AFRICAN CONTINENTAL FREE TRADE AREA - DIGITAL TRADE & E-COMMERCE PROTOCOL (DATA GOVERNANCE & DATA PROTECTION) GUIDE

Africa Digital Rights Hub

JUNE 2023

africadigitalrightshub.org

AFRICAN CONTINENTAL FREE TRADE AREA - DIGITAL TRADE & E-COMMERCE PROTOCOL (DATA GOVERNANCE & DATA PROTECTION) GUIDE

June 2023

Acknowledgement

This research was conducted and written up under the auspices of the Africa Digital Rights Hub with support and contributions from:

- Ms. Stella Nalwoga (International trade law and digital trade consultant – Kampala, Uganda and Brussels, Belgium).

- Ms. Teki Akuetteh Falconer (Founder and Executive Director – ADRH)

The research was funded by the Bill & Melinda Gates Foundation. The views, however, expressed within this report do not necessarily reflect the grantor's official policies or opinion. We express gratitude to the Bill & Melinda Gates Foundation, the Africa Digital Rights Hub Board of Directors, the staff, and all who contributed in various ways to making this report possible.

Executive Summary

This guide report deals with the question of how Micro, Small and Medium Enterprises (MSMEs) in Africa can better exploit the opportunities presented by the digital economy in a safe and secure way that promotes data governance and personal data protection, in order to take advantage of the liberalised trade under the African Continental Free Trade Area (AfCFTA). The report also explores how the negotiators of the AfCFTA digital rules can effectively support MSMEs in taking advantage of Africa's digital economy. For this, the report proposes rules, standards, and practices that have been established within and outside Africa. In Africa, MSMEs are *the backbone of the* economy. However, the majority of them are informal and unregistered. The growing use of digital technologies in Africa presents an unprecedented opportunity for MSMEs to scale up and formalise. Through the digital economy, MSMEs can utilise digital platforms to access a wide market through digitally enabled services to improve the efficiency of their operations. For instance, by using new tools to market and sell, simplify payments, access finance (fintech), communicate with customers and other businesses (social networks and platforms), and reduce trade costs (digital solutions in trade processes and logistics).

However, for those benefits to be realised, a series of factors must be established to promote the digitalisation of MSMEs. These factors include ICT infrastructure (access, usage and affordability), an enabling legal and regulatory landscape, and relevant skills to enable the use of digital technologies and hence close the digital divide. In the context of a legal and regulatory framework, it is necessary to promote digital trust. The latter is essential for both MSMEs and their customers to adopt and participate in the digital economy. Digital trust includes, but is not limited to, personal data protection and cybersecurity.

Promoting simplified data governance frameworks could allow MSMEs to establish robust systems to create value from data through safe and secure means. Currently, few African countries have established data governance frameworks. Where personal data protection laws have been established, there are inconsistencies, gaps, and divergences between countries, the technical terms used are also off-putting for most MSMEs. Data localisation requirements restrict cross-border data transfers which are the lifeblood of the digital economy. Solving these issues will require well-coordinated, inclusive, and targeted approaches at the national, regional, and continental levels. Harmonisation of the legal and regulatory environment is one of the objectives of the ongoing negotiations under the AfCFTA digital trade rules. Those negotiating the continental digital trade rules could use the lessons learned from the policies and commitments established in some African countries and digital trade agreements in other regions.

This report is organised in seven main sections. The first section provides a summary of ADRH's report on ***Africa's Digital Economy: The Case of the African Continental Free Trade Area and the Readiness of Five Countries – Kenya, Nigeria, Rwanda, South Africa, and Ghana*** which forms the background for this paper. Section 2 offers an overview of Africa's digital economy, and is followed by Section 3, which deals with the opportunities presented by the AfCFTA for MSMEs. Section 4 presents a situational analysis of the challenges and opportunities in establishing an inclusive data governance framework in general, and in specific for MSMEs in Africa. Section 5 provides approaches to address challenges to inclusive data governance frameworks, while Section 6 complements Section 5 in highlighting factors that support inclusion, innovation and cohesion. Section 7 concludes the report.

Contents

1. Background

In December 2021, the ADRH published a report entitled "*Africa's Digital Economy: The Case of the African Continental Free Trade Area and the Readiness of Five Countries – Kenya, Nigeria, Rwanda, South Africa, and Ghana*". The report contextualised the legal, regulatory and policy frameworks of the digital economy landscapes in said countries by examining their legal, regulatory and policy frameworks with regard to their readiness for economic transformation to digital economy through the lens of the African Continental Free Trade Area (AfCFTA). Essentially, the report analysed the selected countries' digital economy ecosystem in terms of the environment that enables the development and growth of digital businesses and innovation, which includes the infrastructure, policies, regulations, and institutions that support digital technologies and their adoption, such as internet access, digital skills training programmes, supportive policies for start-ups and entrepreneurs, and regulations that protect personal data, privacy and security.

The report demonstrated an inclination towards embracing the digital economic revolution – powered by a young population keen on digital technologies, and an increasingly conducive legal and institutional environment aimed at creating spaces for digital and technological innovations. On the downside, the report found that limited capacities and gaps in policy and legal frameworks, as well as weaknesses in the regulatory infrastructures, posed a significant risk to the countries' ambitious journeys to digital economic evolution.

Beyond the examination of the legal, regulatory and policy frameworks, the report also investigated the impact of the digital economy in the selected countries. This analysis was intended to denote the potential of the digital economy to transform the economy of African countries. The report noted that the transformative economic benefits of the digital economy had propelled it to the centre of policy discussions in the selected countries. To that end, the report pointed out several legal and institutional frameworks established to regulate the digital economy in the selected countries. The review of the countries' legal, regulatory and policy frameworks was two-pronged: 1) Within the broader context of the AfCFTA; and 2) The consistency of the countries' regulatory infrastructures, which the report found substantially incoherent. Inconsistent national regulatory infrastructures make the digital economy regulatory environment cumbersome to navigate and ripe for reform. The report emphasised reform of digital economy-related policies and laws to make them coherent and thus reflective of an environment that enables the development and growth of digital businesses and innovation.
The role of African governments in the digital economy and the digital revolution was another central theme of the report. It pointed to several government-led initiatives in the selected countries intended to oversee and manage the digital transition, e.g. developments in e-government for delivering public services, investment in digital infrastructures, and

government policies in support of start-ups in various sectors of the economy. The report underscored the critical role of the private sector in the development of the digital economy, given the private sector's increasing adoption and innovation of digital technologies in Africa, such as Fintech including mobile money, which has revolutionised financial inclusion in Africa.[1] To further stimulate and maintain private sector investment in the digital economy, the report called for public-private sector partnerships in leveraging the digital economy in Africa. Financial and technical support to digital entrepreneurs and innovators, is noted as one of the means to enable them to scale their businesses.

The selected countries' readiness for economic transformation through digital economies, was assessed based on the capacity of ordinary citizens to utilise the digital technologies. The report found that exponential growth in the information and communications technology (ICT) sector over the past three decades in Africa does not correspond to the citizens' digital literacy. That created a glaring gap in basic and technical digital skills, and therefore, cast a shadow over possibilities for economic transformation through digital economies. The report recommended an increase in government investment in digital literacy and capacity building. Digital trust was another major concern. The report noted that data protection was still in its infancy in the selected countries, which posed a grave danger in terms of unlawful processing and access of personal data. Inadequate regulation of personal data processing could derail the steady growth of the digital economy, particularly if the already fragile market loses trust in digital technologies. Additionally, the vast and unregulated informal sector in many African countries compounds the challenges of regulating digital tools and business set-ups in the digital economy. That necessitated immediate action to establish legal and institutional frameworks for personal data protection and to set requirements for cybersecurity as well as inclusive implementation strategies that are cognisant of the largely informal and unregulated businesses in Africa's digital economy.

In terms of the AfCFTA, the report called for harmonisation of national policies and laws as well as implementation strategies to reduce operational barriers and inconsistencies in enforcement of digital-related laws. The Report noted concerns that trouble the interface between the digital economy in Africa and the AfCFTA, such as disparities between middle-income African countries and poorer African countries in terms of technological advancement, and the digital divide within countries between urban and rural communities. That could jeopardise the distribution of benefits of the liberalised digital economy under the AfCFTA.

As a follow-up to that report, this Project was conceptualised to guide the ongoing negotiations for AfCFTA rules on digital trade and e-commerce, particularly on aspects of data governance and data protection. The report aims to facilitate the design of an effective data governance and data protection framework in the context of AfCFTA rules on digital trade and e-commerce.

1 https://www.un.org/africarenewal/magazine/august-2022/fintech-other-knowledge-intensive-services-could-drive-africa%E2%80%99s-prosperity

The report considers an effective data governance and data protection framework as one which facilitates inclusive development of all enterprises, especially the micro, small and medium-sized enterprises (MSMEs) that make up the majority of Africa's digital economy.[2] In that context, the report focuses on the following aspects of the digital trade regulation, about which there has been until now limited literature and clarity on how to address them under the AfCFTA:

- data governance;
- data protection implementation;
- cross-border data flows underpinning Africa's digital economy;
- rules and regulations to ensure certainty in the digital marketplace;
- rules and regulations to facilitate harmonisation of the digital marketplace; and factors for fostering inclusion, innovation, and cohesion.

Methodology

This guide report is a follow up of the ADRH report entitled "Africa's Digital Economy: The Case of the African Continental Free Trade Area and the Readiness of Five Countries – Kenya, Nigeria, Rwanda, South Africa, and Ghana" of December 2021. The report is based on desktop research which involved analysis of the main challenges to effective data governance and data protection in the digital economy in Africa at a macro level. The report sets out recommendations to establish effective common rules on data governance and data protection under the AfCFTA. The recommendations were enriched by stakeholder engagements which include contributions from government officials, policymakers, business, civil society, and academia.

The Process

The report was set out in the inception report of May 2023.

The first draft of the report was discussed in the stakeholder engagement workshop on 10th August 2023 via a virtual workshop that brought together numerous stakeholders from various public and private sector organisations in Africa. Comments from the discussion were integrated into a revised draft which was in turn discussed in December 2023 during the 2023 Edition of the Data Protection Africa Summit under the topic the "Role of Data Protection in the Implementation of the AFCFTA Digital trade and E-commerce Protocol".

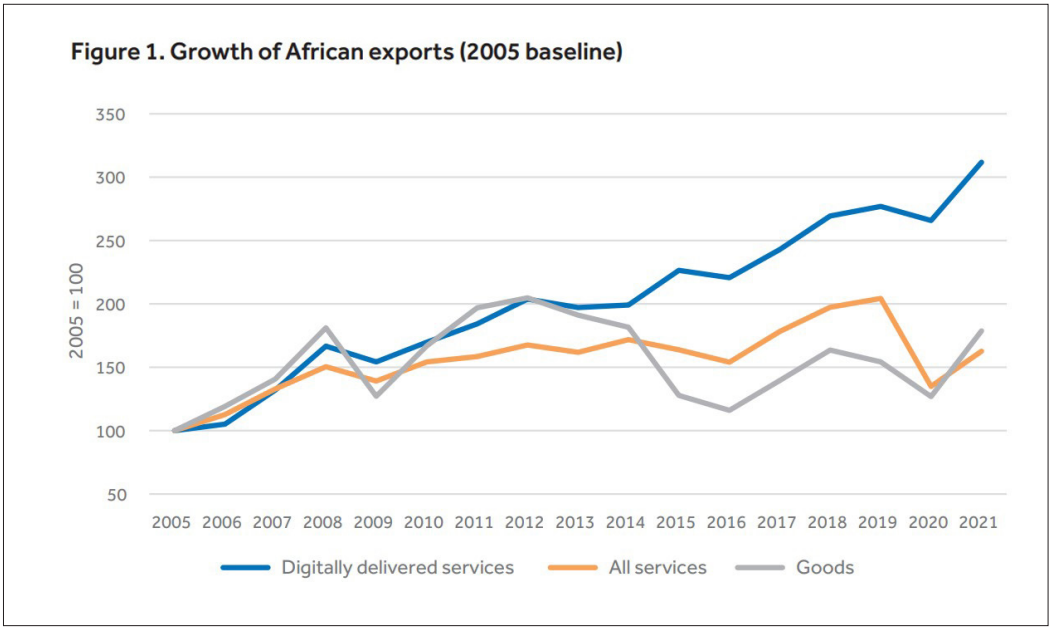
2 https://msme-resurgence-uat.unctad.org/sites/smesurge/files/2021-08/11%20MSME%20formalization%20good%20practices%20in%20Africa_final.pdf

2. Africa's Digital Economy

There is no globally agreed definition of the term 'digital economy' or a methodology to measure it. Digital economy can be loosely defined as the use of digital technologies to perform economic activities.[3] Africa's digital economy is projected to reach USD $180 billion by 2030 (ECDPM, 2022). The growth rate for online purchases or payments across Africa is significantly higher than in other regions. Between 2014 and 2017, online payments or purchases in Africa grew by 240.4%, compared to 97.6% in Asia, 42.2% in Europe and 69.2% in North America (WTO, 2020). In terms of cross-border trade in Africa, digitalisation is expected to facilitate trade in goods through technologies deployed in delivery of border and customs administration such as single window schemes and One Stop Border Posts (World Economic Forum, 2022).

Support for the digital economy in Africa is motivated by political, economic, and socio-cultural factors. From a political perspective, the digital economy can foster transparency, accountability, and good governance through interactions between the government, businesses, and individuals, while socio-cultural benefits include enhanced quality of life via internet access, facilitating activities like ICT-enabled education, digital payments, and skill development. Economically, digital economy spurs growth, job creation, and government revenue through taxation. Additionally, digital trade shows great potential to diversify from predominantly goods-based trade to services trade with a high potential for investment in innovations geared towards solving both longstanding and new challenges to development. Figure 1 below shows that trade in digitally delivered services significantly surpasses trade in goods and services and is growing exponentially.

3 (UNCTAD 2019b, 49).



Source: CommonWealth Secretariat, 2023.

The Digital Economy Blueprint for Africa developed by Kenya offers an instructive description of five pillars that make up the digital economy, namely: 1) Digital government – public service delivery enabled by digital services and platforms; 2) Digital business – a marketplace for digital trade, digital finance services, and digital content; 3) Digital infrastructure that is affordable, reliable, resilient, and accessible; 4) Digital innovation – support for innovation-driven entrepreneurship to deepen digital economic transformation; 5) Digital skills and values based on ethical values and socio-cultural values.[4] These are integrated into a digital ecosystem comprising the government, the citizens, and the private sector.

Africa's nascent digital economy faces several cross-cutting and emerging issues. The digital divide is evident in terms of access and capacity to use digital technologies, the nature of businesses in the digital economy, competition issues, taxation, and digital trust, among others. Africa's digital divide is a key hindrance to the growth of the digital economy. In terms of human capital, the level of digital literacy is significantly low, measured at an average of 31% based on an analysis of 34 African countries (Afrobarometer, 2020). That is aggravated by low internet usage measured at 43.1% compared to the global average of 66.2% (Statista, 2022), as well as disparities in the technological advancement between middle-income and poor African countries, and between rural and urban communities.

In terms of the nature of businesses in Africa's digital economy, the majority are informal and unregulated, which creates challenges in regulating digital tools and business set-ups. Nevertheless, the informal and unregulated sector in Africa is the main source of employment outside agriculture and the backbone of economic activity contributing between 25% and 65% of GDP, (IMF, 2017). The existing digital divide and the informal establishment of MSMEs

4 https://smartafrica.org/knowledge/digital-economy/#:~:text=The%20Blueprint%20identifies%20the%20five,explored%2C%20complete%20with%20illustrative%20tables.

affects their ability to utilise digital platforms for e-commerce, and/or analyse terms of access and control over data which may be unfavourable, as well as the ability to establish digital trust due to high risk of non-compliance with privacy and data protection laws and cybersecurity requirements.[5] Regarding digital trust, concerns about cybersecurity hinder the adoption of digital tools especially with the prevalence of internet fraud. In the same vein, lack of and/or inconsistencies in digital legal regimes constrain effective personal data protection and data governance. Finally, the existing gaps and variations in policies, legal, and regulatory frameworks among the African countries are unfavourable to the interconnected nature of the digital economy and the integration agenda of AfCFTA.

5 Martin Luther Munu, "e-Commerce and MSMEs: what trade rules could improve the business climate in Africa?", 2019, https://ourworldisnotforsale.net/2019/Munu_Africa.pdf

3. MSMEs in the Digital Economy and Opportunities Presented by the AfCFTA

The AfCFTA is a flagship programme of the African Union's Agenda 2063, which in terms of digitalisation in Africa, aims at creating a single digital market.[6] The expanded market is likely to lead to a reduction in transaction costs and increased returns from economies of scale, as well as opportunities for MSMEs to access new markets. Such liberalised trade could reduce the informality of MSMEs by increasing opportunities in the competitive part of the economy and, consequently, shift resources from the informal sector (IMF, 2027).

In terms of the informal and unregulated nature of businesses in the digital economy in Africa, trade liberalisation could reduce informality by increasing opportunities in the competitive part of the economy and, consequently, shift resources from the informal sector (IMF, 2027). The AfCFTA presents a significant platform for coordinating MSME integration into Africa's digital single market. However, specific policy objectives and actions are needed to integrate MSMEs into the regional and continental digital value chains.

Domestic legislation classifies MSMEs based on different factors including the number of employees, assets, sales turnover, value of investment (capital), sector (either providing goods or services) and legal framework. An example is Table 1 below, which shows MSME classification in Uganda's MSME policy. [7]

Table 1: Classification of MSMEs in Uganda

Enterprise	**Number of employees**	**Total assets**	
		UGX	USD
Micro enterprises	Up to 4	10 million or less	2700

6 https://au.int/en/agenda2063/flagship-projects

7 Uganda Micro, Small and Medium Enterprise (MSME) Policy, June 2015, https://www.ugandainvest.go.ug/wp-content/uploads/2016/02/Final-MSME-Policy-July-2015.pdf

Small enterprises	5 and 49	10 million to 100 million	2700 to 27,000
Medium enterprises	50 and 100	100 million to 360 million	27,000 to 99,000

Source: Uganda MSME Policy, 2015.

MSMEs represent 90% of businesses and employ 60% of workers, especially women and youth (African Union, 2022)[8]. The African Union highlights the crucial role of MSMEs in achieving Agenda 2063, which includes fostering innovation, creativity, and quality employment. The AU encourages the formalisation of MSMEs and their active engagement in international, regional, and national markets. This includes providing inclusive access to capacity-building opportunities and financial ser ices, like affordable micro-finance and credit, to support MSME growth.[9] In that context, the African Union Small and Medium Enterprises Strategy was developed and adopted in 2019; it aims to develop "competitive, diversified, and sustainable economies underpinned by dynamic, entrepreneurial, and industrial sectors that generate employment, reduce poverty, and foster social inclusion."[10] Whilst these developments deserve applause, they must be effectuated to derive utility for MSMEs. Clear and comprehensive strategies are needed to assist MSMEs utilise the digital space while maintaining the digital trust of their customers. The AfCFTA digital trade rules provide an opportunity to coordinate and cooperate on such strategies.

8 https://au.int/en/pressreleases/20220628/first-au-sme-annual-forum-realize-africas-industrialization

9 https://au.int/en/newsevents/20230627/micro-small-and-medium-sized-enterprises-day

10 https://au.int/en/newsevents/20230627/micro-small-and-medium-sized-enterprises-day

4. Establishing Inclusive Data Governance Frameworks

Digital technologies are poised to transform African economies, with data representing a fundamental element of that transformation.[11] For the purposes of the present context, data refers to information in digital form that can be transmitted or processed, and it takes various forms based on quantity, transmission method, accessibility, purpose, or the nature of the subjects to which it refers.[12] The specific context determines the type of data, ranging from "big data" which refers to volume, to "open data" which emphasises accessibility, to "personal data" which pertains to individual subjects.[13]

Africa faces data challenges across sectors, ranging from timely availability of data for evidence-based policymaking, accessibility of data for various stakeholders including the private sector, and the quality of data collected.[14] Several barriers exist that prevent data sharing, such as isolated ICT investments, lack of inter-ministerial cooperation, absence of advanced data analysis technology, regulatory differences regarding personal data sharing, and insufficient capacity in anonymising personal data. Moreover, the lack of data standardisation, harmonisation, and integration complicates data comparison, efficient use, and potential misinterpretations, thereby hindering data sharing and international collaboration.[15]

4.1. Data Protection Implementation in Africa

There is no globally agreed definition of personal data, but the definition provided in the EU's General Data Protection Regulation is commonly referenced. It defines personal data as any information that can directly or indirectly identify an individual, including identifiers such as name, identification number, location data, online identifiers, or attributes specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.[16] Data protection and data governance are interlinked, as effective data protection within a data governance ecosystem can boost economic activities, attract investments, safeguard citizens'

11 https://unctad.org/news/blog-digitalization-driver-structural-transformation-african-ldcs (accessed 06/06/2023).

12 Data Definition & Meaning - Merriam-Webster

13 https://cseaafrica.org/wp-content/uploads/2022/10/2022-10-28-CSEA__MI__Report-on-Cross-Border-Data-Flows-in-Africa__Policy-Considerations-for-the-AfCFTA-Protocol-on-Digital-Trade.pdf

14 https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

15 https://www.scielo.org.za/scielo.php?pid=S0038-23532022000800014&script=sci_arttext

16 Article 4(1) GDPR.

data, enhance public service delivery, and promote privacy interoperability for smoother international cooperation.

The protection of personal data is crucial to the digital economy, as it builds consumer trust, and encourages investment and innovation. On the flip side, divergences in data protection laws pose challenges for digital trade. That has created a pressing need for international cooperation and the development of privacy and data protection frameworks that can seamlessly work together, commonly known as "privacy interoperability."[17]

African countries are at varying stages of establishing legal and institutional frameworks for data protection. To date, thirty-six out of fifty-four African countries have data protection laws and/or regulations. Less than twenty-eight of them have established National Data Protection Authorities to enforce compliance with the laws and/or regulations. Data protection frameworks have also been established at the regional level such as the 2008 East African Community Framework for cyberlaws, the 2010 Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS), and the 2013 Southern African Development Community model law harmonising policies for the ICT Market in sub-Saharan Africa. So far, the ECOWAS Supplementary Act on Personal Data Protection is the only binding regional data protection agreement in force in Africa. It is clear that control over the use of personal data in the digital economy in Africa is impeded by lack of legislative and enforcement frameworks. At the continental level, the African Union developed the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) in 2014, which came into force in June 2023.

4.2. Data Governance and Data Protection Implementation Concerns for MSMEs

The challenges faced by MSMEs in relation to data governance and data protection are influenced by various factors including the informal and unregulated nature of their business operations.

4.2.1. Lack of Focus on Data Governance for MSMEs

MSMEs face distinct challenges in navigating data governance, an area traditionally directed towards larger businesses. Developments relating to data governance frameworks in Africa ignore the unique position of MSMEs. While larger enterprises typically have the resources to handle the demands of data governance frameworks, MSMEs find investing in data governance more challenging.[18] However, given the increasing participation in digital economy and their significant economic contribution, it is crucial that MSMEs also prioritise and implement data governance strategies.

17 https://www.oecd.org/en/publications/interoperability-of-privacy-and-data-protection-frameworks_64923d53-en.html

18 Carolyn Begg and Tom Caira, 2012

Moreover, their increasing engagement with personal data through digital marketplaces and payment platforms make them crucial stakeholders in data governance. In terms of building a data economy[19] and data-driven innovation, efforts are needed to build the capacity of MSMEs to recognise the intrinsic value of their data and perceive it as separable from their digital tools.[20] Those aspects could encourage adoption of data governance practices. The significance of MSMEs in terms of contribution to the economy and employment across Africa should inform the digital strategies and rules at the national, regional, and continental levels. Currently, most interventions concerned with integrating MSMEs are focused on investment in ICT infrastructure, access to finance, and digital skills development. There is a pressing need to explore and validate data governance approaches tailored specifically to the unique requirements and characteristics of MSMEs.

4.2.2. Regulatory Gaps and Inconsistencies

Apart from the low adoption rate of the African Union Malabo Convention which hinders its enforcement, effective protection of data in Africa is impeded by regulatory gaps and inconsistencies that contribute to potential challenges in its uniform application and compliance across the continent. These discrepancies manifest in a number of areas: the rationale and objectives for rules relating to cross-border data flows; the regulatory structures influencing compliance, which might prioritise 'consent-first' or 'adequacy-first' approaches; the various legal mechanisms available for cross-border data transfers, including consent, adequacy decisions, contracts, binding corporate rules, certification, and codes of conduct, which vary between jurisdictions; differing approaches to implementation and enforcement, with some jurisdictions being more prescriptive and others facing constraints in terms of resources and expertise, or a lack of independent privacy enforcement authorities. That state of affairs creates uncertainties and increases costs for MSMEs interested in cross-border digital trade.

4.2.3. Inability to Comply

High legal risk of non-compliance with data protection laws. Apart from gaps, inconsistencies, and inadequacies in the legal and enforcement frameworks, there is minimal awareness of the right to privacy and protection of personal data in the digital ecosystem in Africa. That is the case especially for most of the consumers of the digital technologies and digital services and the informal and unregistered MSMEs which feature prominently in Africa's digital economy. This poses three challenges for data protection: 1) Lack of awareness of obligations under the law or lack of legislation; 2) Inability to comply; 3) Inability to enforce compliance with law.

The inability to comply and enforce the law is exacerbated by lack of infrastructures and contextualised implementation processes to support the safeguarding of data protection and privacy rights. That inability to comply could be due to the failure to *comprehend the specificities of risks associated with personal data processing, and to assess and manage risks following a formal methodology*. Data protection laws originate to a large extent in digitally advanced

19 Generally speaking, the production, distribution and consumption of digital data. More precisely, the data economy represents the financial and economic value created by the storage, retrieval and analysis of detailed business and organisational data at high speeds. It is usually associated with data generated through the Internet of Things, (ISEAL, Data rights governance, 2020).

20 Carolyn Begg and Tom Caira, 2012

economies. Careful consideration should be given to the needs of the informal unregulated businesses processing data in the digital economy and data subjects largely unaware of their data protection rights and means to enforce them. Mobilising all stakeholders in the public and private sector including informal enterprises, the media, learning institutions, community leaders, youth, women, and all other minority groups in society to promote data protection is seminal to effective data protection implementation. Data protection laws should not be a preserve of the elite, rather the right to data protection should be embodied by ordinary people as well.

4.4.4. Restrictions on Cross-Border Data Transfers from a Trade Policy Perspective

Cross-border data flows play a crucial role in digitally enabled trade by facilitating communications, supply chains, logistic channels, and globally supplied communications services such as data transmission networks and online distribution platforms, making them essential resources for entities producing goods and providing services, and with emerging technologies like the Internet of Things (IoT), 5G, and AI algorithms, the significance of data flows for digital trade is expected to further increase.[21] Cross-border transfer of data plays a vital role in enabling digital trade, benefiting not only large corporations but also MSMEs. These MSMEs have the potential to leverage emerging and disruptive technologies, global e-commerce marketplaces, and data-driven trade logistics, which can greatly enhance their participation in digital trade. Moreover, Africa's growing trade in digital services relies heavily on the movement of data.[22]

Cross-border data flows are taking centre stage in policymaking as governments seek to address the challenge of harnessing the value of data while managing risks and avoiding abuses. These challenges relate to social well-being, competition concerns, and curbing illicit online activities such as fraud, money laundering, data hacking, ransomware and critical infrastructure attacks.[23] In that regard, various policy responses are being considered, with many centred on balancing commercial interests and privacy objectives, concerns around economic imbalances and of claims for a more inclusive digital economy.[24] The challenge of balancing these diverging interests has resulted in an increase in cross-border data restrictions through measures that impose data localisation requirements.

Policies restricting cross-border data flows not only impact international trade opportunities but also determine the extent to which digital connectivity and technological advancements can be leveraged to unlock the developmental potential of data[25], for instance, in solving

21 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

22 Shamira, Ahmed, "Leveraging the potential of digitalisation, disruptive technologies, and cross-border data flows to facilitate aspirations of a Pan-African Digital Single Market", https://researchictafrica.net/2022/01/25/leveraging-the-potential-of-digitalisation-disruptive-technologies-and-cross-border-data-flows-to-facilitate-aspirations-of-a-pan-african-digital-single-market/

23 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

24 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

25 Shamira, Ahmed, "Leveraging the potential of digitalisation, disruptive technologies, and cross-border data flows to facilitate aspirations of a Pan-African Digital Single Market", https://researchictafrica.net/2022/01/25/leveraging-the-potential-of-digitalisation-disruptive-technologies-and-cross-border-data-flows-to-facilitate-aspirations-of-a-pan-african-digital-single-market/

Africa's glaring digital divide. Restrictions to cross-border data flows can distort the competitive conditions of digital trade exchanges by providing *de jure* or *de facto* domestic economic actors with a competitive advantage over foreign competitors in digitally enabled trade. Moreover, "for digital products, data flow restrictions would hinder trade altogether, as much as a border measure would impede the import of traditional goods".[26] The legitimacy of these distortive restrictions varies across jurisdictions, reflecting differences in public policy goals and rules.[27]

4.4.5. Challenges Associated with Data Localisation Requirements

Data localisation restricts the movement of data to a specific geographic area for public policy and economic development objectives such as attracting foreign investment, maximising domestic firms' gains, protecting citizen privacy, and ensuring regulatory oversight. It can take various forms, either requiring data to be stored in a specific jurisdiction or prohibiting the transfer of certain types of data.[28] In case of privacy and data protection, although the primary aim is to protect individual privacy when data crosses borders, unintended consequences may include data localisation due to differences in privacy protection levels between countries or the inability to provide sufficient privacy assurances. Data localisation requirements are prevalent in Africa with varying degrees of strictness - see Table 1 below. Examples of data subject to data localisation requirements in Africa include government data in Kenya, all government data, subscriber and consumer data in Nigeria, "personal information" in Zimbabwe, Malawi, and Tunisia, telecommunications subscribers' registration information in Sierra Leone, "critical information" and "sensitive personal data" in Zambia, data deemed sensitive in sectors of vital importance in Morocco, and data for public cloud computing services and e-commerce operators in Algeria.[29] This situation poses a significant challenge when it comes to negotiating the AfCFTA rules on digital trade regarding liberalisation of cross-border data transfers.

26 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

27 pg. 18. https://cseaafrica.org/wp-content/uploads/2022/10/2022-10-28-CSEA__MI__Report-on-Cross-Border-Data-Flows-in-Africa__Policy-Considerations-for-the-AfCFTA-Protocol-on-Digital-Trade.pdf

28 https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-07/Trade%20Hot%20Topic%20-%20Energising%20Africa%E2%80%99s%20Digital%20Economy%20Cross-Border%20Data%20Flows%20and%20the%20African%20Continental%20FTA.pdf?VersionId=EcDZrtFAs1_99.BsnL_Njs3slbYMyXeE

29 https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf

Table 1. Typology of data localisation measures

Conditional transfers	Hard	Data transfers are contingent upon explicit approval by a public authority.
	Soft	Data transfers are contingent upon the self-assessment of compliance with a given condition, such as user consent.
Limited transfers	Strict	The absolute prohibition of data transfers, requiring that data must be stored and processed domestically.
	Partial	Data transfers are allowed if a copy of the data is stored domestically.

Source: CommonWealth Secretariat, 2023.

a. The Impact of Competition and Internationalisation

Data localisation laws disrupt the smooth flow of data, causing delays and complications for firms that need continuous data flow. These restrictions can affect competition in the digital economy and hinder businesses looking to expand internationally or those that cannot afford their own IT infrastructure. Data localisation requirements disproportionately affect start-ups and MSMEs as they are less financially equipped to handle the additional costs associated with compliance, such as higher prices for data storage and processing services, along with the burden of verifying their adherence to regulations across multiple jurisdictions.[30] Moreover, access to cost-saving and efficient options like cloud-enabled services and distributed networks, which larger businesses can more easily afford, may not be feasible for start-ups and MSMEs.[31]

b. Reinforce Digital Infrastructure Inefficiencies

Data localisation requirements in Africa could exacerbate digital infrastructure inefficiencies and weaken cybersecurity. These regulations may increase government surveillance, compromise data privacy, democracy, and human rights, and decrease personal information protection due to underdeveloped domestic cybersecurity infrastructure.[32]

30 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

31 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

32 https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf

c. Economic and Trade Implications

Evidence-based studies indicate that data localisation requirements can significantly impact the economy and trade in African countries (Badran and Tufail 2019). Cross-border data transfer restrictions could result in GDP decline, an increase in production costs, a decrease in income due to price hikes, and negative impacts on sectoral production. Trade impacts include a decline in imports across almost all sectors and countries with the most impact felt by import-dependent economies. Data localisation requirements can significantly affect economic performance and trade dynamics in African nations.[33]

4.4.6. Challenges Associated with Digital Marketplaces

A digital marketplace is an online platform that facilitates direct transactions between buyers and sellers.[34] Digital marketplaces play a vital intermediary role matching potential buyers of a service or a product with providers of that service or product, thereby creating an accessible and efficient digital commerce system.[35] Given Africa's small and fragmented markets, digital marketplaces established either by vendors or third-party facilitators could provide access and visibility to previously unreachable clients, thereby unlocking new markets for businesses. Thus, for Africa, digital marketplaces provide great potential for transformative disruption.[36]

E-commerce platforms are growing in Africa. There are a number of country-based and successful intra-African e-commerce platforms such as 'Jumia'[37],and 'Burundi shop', which have international reach.[38] Digital platforms can operate at sectoral level and can act as market-led solutions to socio-economic challenges in Africa, for example, connecting farmers directly to markets, thus eliminating middlemen, and in the financial sector, the Mobile Money Interoperability platform was established by the government of Ghana to promote digital financial inclusion and facilitate cashless transactions for Ghanaian citizens, thereby laying the groundwork for a digital economy (Smart Africa, 2020). The platform results from collaboration between Ghana Interbank Payment and Settlement Systems Limited, the Bank of Ghana, FinTech firms, and telecommunication companies with the aim of enhancing access to, and efficiency of, financial services. It eases the transfer of funds across different networks and allows businesses to accept payments from various accounts, which has increased mobile transaction volume in Ghana.[39]

Legal and regulatory frameworks are required to establish certainty and promote consumer trust in digital marketplaces, within and across borders. Through regulation, the government can provide legal validity for electronic contracts, clarify rights and obligations of the multiple actors involved in digital transactions, ensure digital trust through consumer rights and data

33 https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf

34 https://www.lawinsider.com/clause/digital-marketplace

35 https://www.eib.org/en/stories/what-is-a-digital-marketplace

36 https://www.eib.org/en/stories/what-is-a-digital-marketplace

37 https://www.jumia.com.ng/

38 http://www.burundishop.com/

39 https://dial.global/wp-content/uploads/2020/10/SmartAfrica-DIAL_DigitalEconomyInAfrica2020-v7_ENG.pdf

privacy protection, and a mechanism for dispute settlement, and establish a framework that promotes consumer trust in digital markets.[40]

Generally, MSMEs plug into the digital economy via digital marketplaces or digital platforms. Platforms enable MSMEs to reach a broader range of customers, minimise expenses since numerous services are consolidated within platforms, and enhance the productivity in their businesses. In an interconnected digital economy, consumers of products and services provided via digital platforms are both domestic and international. Digital trust is critical due to the long-distance nature of the transactions. Establishing e-commerce rules that ensure trust in e-commerce transactions is key. For instance, regarding digital payment systems, most MSMEs are predominantly cash-based businesses. With more MSMEs joining digital platforms, convincing their consumers to source from digital marketplaces requires trust built on safe and secure consumer experiences. Digital trust is therefore critical for the success of digital platforms and the MSMEs utilising them. [41]

Digital marketplace enablement varies significantly across African countries, presenting distinct challenges and variation in regulating the above-mentioned aspects. Additionally, the heterogeneity of existing legal frameworks creates legal uncertainties for digital platforms and businesses interested in expanding across borders. Existing regulatory measures restricting cross-border data flows and online purchases can further segment digital markets impacting the availability of goods and services across national boundaries.[42] Therefore, regulations introduce restrictions that limit the types of goods and services available online, impose burdensome conditions on online platforms and services, and hinder the transfer of data necessary for transactions. A discussed in the previous section, data localisation requirements on digital marketplaces demonstrate that restrictions on data flows could potentially undermine the ability of businesses in Africa to capitalise on e-commerce opportunities which rely heavily on real-time data connectivity across borders. That underscores the crucial role of unrestricted data exchange in the successful expansion of digital marketplaces.

In terms of data governance, e-commerce platforms need and generate a wide range of information including on clients, sales, and logistics. Data analytic skills are needed to analyse such information to maximise sales. Unfortunately, data scarcity and data management are major challenges for MSMEs in leveraging the digital platforms to connect to markets.[43] Regarding personal data protection, with the ever-increasing adoption of digital technologies in Africa, MSMEs are increasingly handling customers' personal data. This status as data controllers entails significant legal responsibilities which, if mismanaged, could be detrimental to the relevant consumers and could expose the MSMEs to hefty penalties and potential financial hardship. Yet compliance with data protection laws presents substantial challenges. This raises data management concerns regarding processing of such data and its adequate protection,

40 https://documents1.worldbank.org/curated/en/998881578289921641/pdf/The-Regulation-of-Digital-Trade-Key-Policies-and-International-Trends.pdf

41 https://www.cgap.org/blog/super-platforms-connecting-farmers-to-markets-in-africa

42 https://documents1.worldbank.org/curated/en/998881578289921641/pdf/The-Regulation-of-Digital-Trade-Key-Policies-and-International-Trends.pdf

43 https://www.cgap.org/blog/super-platforms-connecting-farmers-to-markets-in-africa

for instance, against data breaches. Moreover, to access cross-border markets, MSMEs would have to navigate intricate data protection laws and compliance requirements. This situation underscores the vital role of government in delivering contextualised compliance support to MSMEs and the need for continental harmonisation of regulatory regimes. At the same time, recognising the diversity of MSMEs and their varied capacities to handle such responsibilities is vital.

5. Addressing the Challenges

Africa's specific digital landscape marked by informality and unregulated business environments calls for bespoke, nuanced, and multifaceted approaches that balance global best practices with local needs and requirements. That means innovative approaches to support the inclusive growth of all enterprises, especially MSMEs, which form the bulk of Africa's digital economy. Addressing the complex challenges faced by these enterprises, including regulatory intricacies and limited resources, the AfCFTA digital rules should bridge the gap between MSMEs' existing capabilities and stringent data governance and protection requirements, thus facilitating their effective participation in digital trade without compromising on robust data governance and protection. The AfCFTA digital rules should address the challenges that current data governance and data protection frameworks could pose for MSMEs. The following selection of best practices is presented as a possible solution to that data governance and data protection implementation challenges facing, in particular, MSMEs in Africa.

5.1. Simplifying Data Governance for MSMEs

The AfCFTA rules should avoid a 'one size fits all approach' by contextualising data governance and data protection implementation and compliance requirements to meet the needs of MSMEs. To this end, State Parties under the AfCFTA digital rules should commit to exploring and establishing simplified data governance models to address MSMEs compliance constraints and ensure digital trust in the digital economy. The complexity of legal and administrative processes and procedures is one of the reasons for the ongoing lack of formalisation of the majority of businesses in Africa. Important policy changes have been implemented regarding, inter alia, the ease of doing business. In terms of support for cross-border trade, African countries have committed at the multilateral level to providing simplified trade processes and procedures under the WTO Trade Facilitation Agreement (*an instrument designed to facilitate and reduce the cost of trade across borders, which contains a variety of measures that involve the use of digital solutions*).[44]

That model could be instructive in assisting MSMEs to start using data easily and responsibly for business development. Such technical assistance relating to information management and data protection should be incorporated in national, regional and continental MSME strategies with an emphasis on effective and inclusive communication methods. Guidelines are a viable method for simplifying data governance for MSMEs. Guidelines could be developed to equip MSMEs with basic knowledge of data protection and security practices. The general framework

44 https://www.unescap.org/sites/default/d8files/event-documents/MSMEs%20and%20the%20Digital%20Economy.pdf

of the guidelines should be established at the continental level through the AfCFTA digital rules to ensure harmonisation across Africa. This is due to the heterogeneity of MSMEs in terms of business activities, internal capacity, and resources. Therefore, their challenges are varied and could entail different support measures according to their level of digitalisation and size.[45] State Parties should be encouraged to establish other methods to simplify data governance for MSMEs, such as developing App(s) for self-assessment of digital maturity. Such initiatives could offer free easy-to-use and holistic one-stop professional guidance, Apps, and online tools to MSMEs which do not have the resources to consult professional advisory services on issues involving privacy and data protection. Whilst some African countries have embarked on similar initiatives, there is still a need for holistic and comprehensive methods so that MSMEs do not get lost due to the scattered nature of information. The AfCFTA could encourage State Parties to provide such tools via a government platform dedicated to the digital transformation of MSMEs.

45 https://smeunited.eu/admin/storage/smeunited/smeunited-digital-brochure.pdf

Guidelines on the law including compliance requirements, processes and procedures:

- provide for a simplified definition of data protection, examples of personal data, application (scope), objective, compliance requirements e.g., registration, how to protect the rights of citizens including in relation to communicating, obtaining consent, access and portability, warnings on data breaches, erasing of data, profiling, marketing, safeguarding sensitive data, children's data, data transfer within Africa and outside Africa, a checklist when it comes to appointing a data protection officer, record keeping, the requirement for impact assessment reports, the cost of non-compliance, and who to contact for additional assistance;
- Accountability practices such as leadership and oversight, policies and procedures, training and awareness, individuals' rights, transparency, processing records and legal precedents, contracts and data sharing, risks and data protection impact assessments.
- Clarity on the obligations that do not apply to MSMEs is also desirable. Due to the nature of risks involved regarding individuals' rights and freedoms in the digital economy, particularly data privacy, security and ethical considerations, data governance rules including data protection apply to the nature of activities and not to the size of enterprise or organisation. However, MSMEs could be exempted from certain obligations such as appointing a Data Protection Officer based on unified criteria, for instance where processing of personal data is not a regulatory activity of the MSME, and the processed data does not contain sensitive data;
- since MSMEs are a heterogenous group, guidelines should be adapted to sectors with respect to categories of personal data that is commonly collected from consumers in that sector, such as a guide to data protection practices for ICT systems, and a checklist to guard against common types of data breaches in each sector;
- information on the prevalence of digital fraud is matched with communication of data security measures, e.g., encryption and backup solutions, and incident management;
- examples of countries with guidelines that can be replicated across Africa and that are subject to capability in terms of resources and national context include Singapore, which has developed various guidelines on data governance and data protection for small businesses including a 'Guide on building websites for SMEs' which collect, use, disclose, or store personal data,[46] and a 'Configuration Guide to Minimise Common Data Breach Issues for Microsoft 365', which is intended to support businesses in minimising common breach issues through good security practices using Microsoft 365, via simple configuration steps that include a screenshot for further clarity. Contents include:[47]
    - Strong Password Settings;
    - How to turn on 'Bitlocker Disk Encryption';
    - Microsoft 365 SETTINGS relating to: 1. Enable Multi-Factor Authentication (MFA) for Administrators; 2. Review of User Accounts; 3. Disable Email Auto Forwarding; 4. Configure Folder Permissions for OneDrive; 5. Manual Back-Up of Local Files (back-up from local device to OneDrive and restore from OneDrive to local device); 6. Restoring the entire OneDrive; 7. Restoring a Selected File in OneDrive; and
    - How to Securely Zip a File.

An App and / or online tool which could provide MSMEs information on data governance and data protection could include the above information as well as:

- a free online self-assessment of the digital maturity of the business, for instance in terms of using digital technologies for customer relationships, marketing and selling of products and services, business management, and value creation.

46 This Guide could empower businesses in their discussions with IT vendors whom they engage to build their websites. https://www.pdpc.gov.sg/help-and-resources/2017/10/guide-on-building-websites-for-smes

47 https://www.imda.gov.sg/-/media/imda/files/programme/dpe/dpe-configuration-guide.pdf

5.2. AfCFTA Digital Rules to Ensure Harmonised Regulations in the Digital Economy

The digital single market envisaged under Agenda 2063 and the African Union Digital Transformation Strategy is expected to function within a harmonised legal and regulatory environment.[48] That is currently the focus of the ongoing negotiations for AfCFTA rules on digital trade and e-commerce as an additional Protocol to the AfCFTA. The AfCFTA negotiations on digital rules offer an opportunity to devise coordinated responses to the above-mentioned cross-cutting and emerging challenges facing the digital economy in Africa. Essentially, the negotiations should establish a harmonised, open, fair, trustworthy, ethical, people-centred, inclusive and sustainable digital economy in Africa. That will require targeted approaches to empowering people and businesses to access, utilise, and innovate in the digital economy. A harmonised digital regulatory environment is expected to propel Africa's readiness for the changing economic paradigms fostered by digital transformation. The expected benefits of integration under the AfCFTA should incentivise political will in the negotiation and implementation of harmonised digital rules, as well as public and private-sector investment and cooperation on programmes such as the rapid ICT infrastructure development needed to resolve the digital divide.

Literature on digital trade integration speaks to its holistic nature, which consists of five interconnected and supportive pillars, namely: 1) lowering digital trade barriers, 2) facilitating digital trade, 3) developing regulatory frameworks and digital trust policies, 4) promoting digital development and inclusion, and 5) institutional coordination.[49] These pillars are considered interdependent and the process of digital integration is deemed multidimensional and multilevel.[50] Therefore, a nuanced and multifaceted approach is essential in harmonising these pillars for successful digital trade integration. [51]

This report advocates for a similar approach in establishing the AfCFTA rules on digital trade and e-commerce. Adopting a nuanced and multifaceted approach to integrating the five pillars of digital trade integration in Africa could address the disparities in regulatory capabilities, digital development stages, and policy inclinations among African countries. Whereas seamless integration in the face of divergent interests and differences in resources is virtually impossible, the mutual benefits of a unified digital economy within a globalised context should incentivise African countries to strategically overcome hurdles within the five pillars of digital trade integration. The negotiation of the AfCFTA rules on digital trade should aim for a comprehensive digital trade governance framework containing binding substantive provisions on certain critical aspects of digital economy such as data protection and cross-border data transfer. Additionally, the negotiations should consider a mix of time-bound regulatory convergence and progressive regulatory convergence. The latter involves a more gradual and flexible approach to harmonising regulations, while the former requires setting specific deadlines or timeframes within which State Parties must harmonise their regulations.

48 https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

49 Digital trade integration in preferential trade agreements | ESCAP (unescap.org)

50 Digital trade integration in preferential trade agreements | ESCAP (unescap.org)

51 Digital trade integration in preferential trade agreements | ESCAP (unescap.org)

That approach could strike a balance between digital trade integration aligned with each country's resources, policy preferences, and socio-economic objectives, and the immediate action to be taken on certain aspects of digital trade.

Trade agreements on digital trade foster regulatory cooperation on digital economy, facilitating negotiations on liberalisation of cross-border data transfers. Policymakers seek to strike a balance between free data flows and the States' right to pursue public policy interests. It is not uncommon for digital trade agreements to give latitude to States to pursue public policy interests which may interrupt the seamless cross-border flow of data. However, to prevent Parties to digital trade agreements from abusing their policies, the right to pursue legitimate public policy interests is in most cases conditional.

The veracity and impact of public policy objectives is established through the process of weighing and balancing three central issues, namely: 1) The public policy objective (also known as a measure) in terms of its effect on digital trade; 2) Whether such a measure is arbitrary or unjustifiable discrimination; and 3) Whether the measure constitutes a disguised restriction on digital trade. That legal text is considered strict for measures imposed to protect privacy and personal data, which are "fundamentally rights-based" and therefore command a higher level of protection.[52] In that context, it is unlikely that measures restricting liberalised cross-border flows to protect personal data and privacy would be challenged before the dispute settlement body established under the digital trade agreement. That strengthens the need for alternative mechanisms to allow cross-border data flows whilst observing public policy interests.

In the context of establishing harmonised rules on cross-border data flows, the following recommendations could be adopted in designing the AfCFTA digital trade rules (Kyle de Klerk, 2023).

52 Irion and Burri.

- The efficacy of data regulation negotiations hinges on a common understanding of key concepts and terminology such as digital trade, e-commerce, data, trade barriers, cross-border data flows, and data protectionism, as differing interpretations can obstruct effective negotiations;
- Once a shared lexicon is established, State Parties should assess alignment in norms, values, and policy goals related to the five pillars of digital trade integration, considering factors like privacy and consumer protection, socio-economic rights, national security, access to information, freedom of expression, cybersecurity, and bridging digital divides;
- Furthermore, it's crucial for all parties to have a collective theoretical and practical comprehension of the objectives and expected outcomes of potential cross-border data flow rules, including what constitutes an acceptable level of restrictions disruptive to trade. A greater alignment in understanding the legitimacy of data flow controls will likely lead to the development of more effective and legitimate rules through negotiations;
- Reconcile regulatory discrepancies between domestic and regional data protection frameworks by referencing the Malabo Convention, regional models, and international privacy and data protection frameworks; and
- Given the diverse capabilities of member countries, especially as many African countries lack domestic privacy laws, a time-bound exemption for non-compliant and capacity-constrained countries is a critical component for an effective solution.

5.3. Enabling Cross-Border Data Transfer

Digital trust, fostered by robust data protection, is a key driver of competitive digital economies. To ensure legal and safe data sharing, especially among African countries where data protection laws may not exist, alternative binding mechanisms can be implemented in line with the AfCFTA requirements. This strategy not only boosts efficient data sharing but also overcomes the barriers posed by the lack of or disparities in privacy and data protection laws. In lieu of a comprehensive legal framework, sector-specific requirements can be used to safeguard privacy and promote trust in the digital economy. By offering alternative, practical avenues for data transfer, the AfCFTA could address a significant hurdle in digital integration. It underscores that personal data protection is not just a legal requirement but a vital element in building trust within the digital economy. Thus, outlining parameters for businesses operating in countries without established data protection regimes enhances the AfCFTA's relevance and importance to its citizens and businesses.

The AfCFTA digital trade protocol should provide a binding commitment on liberalisation of data flows and on the prohibition of data localisation requirements with a narrow scope of exemptions and criteria upon which their veracity would be tested. On data protection, the continental digital rules should set minimum binding standards with criteria and binding harmonisation requirements referencing regional, continental, and international frameworks. Additionally, the AfCFTA digital rules should provide for time-bound exemptions for capacity-constrained African countries, that could achieve the much-needed balance in digital integration and securing political support. That approach was adopted in the Digital Economy Partnership Agreement between New Zealand, Chile, and Singapore, and could be replicated in the African context.

In the digital era, regulatory measures that impede cross-border data flow are inevitable. As noted above, such measures are adopted for various public policy interests. It is common practice for digital trade integration agreements to provide policies to State Parties to

pursue such interests. That creates a significant task in terms of balancing the objectives of agreement and varying State Parties' public policy interests. Studies recommend that State Parties adopt a risk-based approach to regulation to mitigate the economic and trade impact of such measures, where extremely sensitive data like health records and state security-related data may be restricted, weighing their cross-border transfer risk against economic and trade benefits (Kugler, 2022). Consent and anonymisation could offset risks when economic and trade benefits surpass them (Kugler, 2022). The AfCFTA could prompt State Parties to adopt a risk-based approach to regulate cross-border data flows, centred on security, trust, and equal access (Kugler, 2022).

To facilitate cross-border data flows while protecting legitimate public policy interests, alternative measures are needed. By offering alternative, practical avenues for data transfer, the AfCFTA could address a significant hurdle in digital integration.

5.3.1. Mechanisms for Facilitating Cross-Border Data Flows with Safeguard for Privacy and Data Protections

- By offering alternative, practical avenues for data transfer, the AfCFTA could address a significant hurdle in digital integration.
- Another feasible solution could be to compile a certification system tailored specifically for MSMEs. Drawing parallels from certification systems in the trade of goods, the scheme would simplify the requirements for data governance and data protection. This approach could enable MSMEs to demonstrate their commitment to proper data management and protection without the need for exhaustive resources typically required under standard regulatory compliance. The certification system would offer a dual advantage. For the MSMEs, it provides a feasible way to engage in digital trade by meeting the necessary data governance standards, thereby boosting their market credibility and expanding their potential for growth. For the regulatory authorities, it offers an effective and scalable way to monitor compliance, thereby ensuring the integrity and safety of the digital trade ecosystem. The establishment of such a system should be based on an inclusive and comprehensive stakeholder consultation process.

Those solutions could be further analysed and developed at the continental level to establish AfCFTA digital rules to which State Parties adhere with commitments on data governance and data protection implementation that are directly manageable and are an asset to MSMEs.

Possible Practical Solution to Restrictions on Cross-Border Data Transfers under AfCFTA Digital Trade Rules

International agreements, harmonisation, and mutual recognition, as well as initiatives involving the private sector, are well-recognised mechanisms for promoting interoperability of privacy and data protection frameworks, and therefore facilitate the free flow of cross-data (OECD Going Digital Toolkit Note, No. 21, 2021). Incorporating such mechanisms in the AfCFTA Digital Trade Protocol could guarantee continued cross-border data transfers and protection of citizens' privacy irrespective of regulatory gaps, inconsistencies, and divergences in public policy interests for restricting data flows. That would enable the Protocol to address a significant hurdle in digital integration. This would enhance the AfCFTA's relevance and importance to citizens and businesses. Established private sector mechanisms that the

negotiator of the Protocol could consider include model contract clauses, binding corporate rules (BCRs), certification systems, and codes of conduct.

a. Harmonisation and Mutual Recognition (Adequacy Decisions)

The adoption of adequacy decisions commonly utilised by the European Union (EU) to authorise international data flows whilst maintaining a high degree of privacy and data protection for its citizens has become a common practice globally. Adequacy or equivalence determination is a unilateral recognition certifying that the data protection regime of another country meets certain privacy requirements, and that data can be transferred unimpeded to that country (OECD, Going Digital Toolkit Note, No. 21, 2021). Adequacy recognition can be mutual where similar transfer frameworks exist for both parties involved. Adequacy decisions can be applied on a sectoral basis, such as in the case of digital financial services, digital payment platforms, and systems, for example access to Pan African payment settlement system.

Some African countries, such as Uganda and Kenya have established adequacy as one of the legal precedents for transferring data across borders, but without providing criteria to guide such a finding.[5354] At the regional and continental levels, the concept of adequacy in data protection has been approached with some ambiguity. The Southern African Development Community (SADC) Data Protection Model Law (DPML) states that personal data transfer to non-SADC countries, or SADC members that have not adopted the DPML, requires a prior finding of adequacy by the domestic data protection authority. The Malabo Convention provides for international data transfer from Africa based on reciprocity, without providing clarification with regard to intra-Africa data transfers.[55]

The AfCFTA should provide clarity on intra-Africa data flows and the criteria for adequacy assessments, which is another shortcoming of the Malabo Convention. The criteria for making a finding of an adequate level of data protection are well developed under the EU's General Data Protection Regulation (GDPR) data protection laws. Negotiators of the AfCFTA Protocol can be informed by Article 45 of the GDPR which provides for requirements including the recipient country's rule of law, respect for human rights and fundamental freedoms, pertinent legislation concerning public security, defence, public authorities' access to personal data, the enforcement and implementation of this legislation, data protection rules, professional rules, security measures, and the rules for onward data transfer. Establishing common substantive rules on data protection and the criteria for a finding of adequacy could ensure harmonisation across Africa.

Initiatives Involving the Private Sector

In the absence of an official decision confirming the adequacy of another country's data protection regime, the AfCFTA digital rules should require State Parties to provide for other

53 https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf

54 https://www.odpc.go.ke/download/kenya-gazette-data-protection-act-2019/?wpdmdl=3235&refresh=64d10d4bdd9e51691422027

55 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

means to transfer personal data using proper safeguards. Private sector-led initiatives, such as binding corporate rules, standard data protection clauses adopted by a supervisory authority, approved codes of conduct, or certification mechanisms with binding commitments, have emerged as resourceful alternatives for safeguarding cross-border data transfer.

Model Contractual Clauses

Model Contractual Clauses (MCCs) also known as Standard Contractual Clauses (SCC) can significantly enhance data protection in Africa by fostering the interoperability of privacy and data protection frameworks. MCCs are pre-approved by competent domestic authorities like a data protection authority and provide a legal basis for the transfer of personal data without the requirement for businesses to seek authorisation for each transfer.[56] By establishing a data protection regime at the contractual level, MCCs can bridge existing differences in privacy and data protection standards under respective domestic legal frameworks. As a model with fixed content, MCCs promote transparency and legal certainty for both companies and individuals. Moreover, the low cost of MCCs makes them particularly attractive for MSMEs. MCCs reduce negotiation and compliance costs and time while maintaining safeguards for personal data transferred across borders. SCCs or MCCs are not currently well established in Africa. Negotiators of the continental digital trade can be informed by the ASEAN Model Contractual Clauses for Cross-Border Data Flows.[57] Businesses can incorporate the ASEAN MCCs in their commercial contracts between the parties to the data transfer(s).[58] MCCs can be further developed by State Parties through, inter alia, guidelines and templates and can be applied at the sectoral level.[59]

c. Binding Corporate Rules

Binding Corporate Rules (BCRs), also known as intra-group rules, offer a mechanism for ensuring safe cross-border data transfers within corporate groups.[60] These rules can be highly advantageous for multinational corporations operating in African countries that need to transfer personal data within their group but are impeded by inadequate or varying levels of personal data protection. BCRs are effective intra-group personal data protection policies and procedures that guarantee adequate data protection and compliance with local laws during cross-border transfers.[61] The rules generally encompass data protection principles, data transfer types, data subjects' rights, complaint handling procedures, the role of Data Protection Officers, compliance verification mechanisms, reporting procedures to supervisory authorities, and training. Approval by a supervisory authority is sometimes required for BCRs. [62]

---

56 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

57 https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

58 https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

59 https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

60 (See https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf) (also see Harmonised standard contractual clauses: https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/

61 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

62

Generally, explicit recognition of BCRs is not common in African countries privacy and data protection laws. South Africa's Protection of Personal Information Act recognises BCRs as a cross-border data transfer mechanism.[63] The AfCFTA Protocol should require State Parties to similar action and provide for BCRs as a valid data transfer mechanism.

d. Certification Systems, Codes of Conduct, and International Standards

There are several other mechanisms led by the private sector through which businesses and organisations can transfer data across borders subject to domestic law. These include certification systems, codes of conduct, and international standards. Codes of conduct can be developed by an organisation or industry, applied on a voluntary basis, as a guide to the application of data protection rules including those on cross-border data transfer. In some countries, codes of conduct may be subject to government approval. For example, the EU's GDPR recognises codes of conduct as valid international data transfer mechanisms subject to requirements such as enforceability.[64] When applied at industry level, codes of conduct can be used by the association or representative body to evaluate membership applications and ensure compliance by members. In this context, codes of conduct can assist MSMEs to save costs as they can rely on the association to ensure compliance.[65]

Regarding international standards, the privacy protection ISO (ISO/IEC 27701:2019, developed through international cooperation at the International Standard's Organisation (ISO),[66] is a good example of a privacy standard that can be implemented by businesses, governments, and organisations to demonstrate compliance with privacy and data protection requirements. The standard specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS).[67] Certification systems in the face of diverging policy and regulatory requirements are commonplace in trade agreements, particularly, certification systems relating to compliance with product health and safety requirement, and environment sustainability requirements. Certification systems can be developed by the public or private sector at sector or industry level. Within the private sector, the privacy trust mark or seal is slowly gaining momentum as one way of certifying that an organisation, product or service adheres to privacy and data protection requirements.[68] Privacy trust marks or seals can promote digital trust and international data protection interoperability at an organisation and product/service level.[69] This is an interesting development that negotiators of the AfCFTA Protocol on digital trade rules could consider.

---

63 https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

64 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

65 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

66 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, available at https://www.iso.org/standard/71670.html

67 https://www.iso.org/standard/71670.html

68 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

69 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

At public sector level, the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR)[70], a government-recognised data privacy certification for companies, developed by APEC economies based on the APEC Privacy Framework[71], stands out as the main non-European mechanism to facilitate the cross-border flows of personal data.[72] Interested countries must demonstrate compliance with the CBPR system with respect to enforceable standards to be applied against certified companies and public or private sector entities to act as an accountability agent to certify domestic companies, provide risk-based protections implemented by certified companies, consumer-friendly complaint handling, consumer empowerment including data subject rights, agreement to be bound by the CBPR programme to ensure harmonised implementation across different legal regimes, and cross-border enforcement cooperation.[73]

A key aspect is the CBPR system's recognition of differences among privacy regimes. It does not seek to replace domestic privacy laws. It only establishes a baseline protection for personal data to which participating countries must adhere.[74] In essence, participating countries can still adopt legitimate public policy objectives that could restrict cross-border flows, but the CBPR system can be relied upon as a baseline transfer mechanism. Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply.[75] However, in the absence of privacy laws, the system provides a minimum level of protection that businesses can rely on to transfer personal data. The CBPR System is recognised unilaterally by Japan, South Korea, Australia, and Singapore[76], and via regional trade agreement by the United States, Mexico and Canada under their USMCA[77].

The AfCFTA digital rules could recognise the CBPR System as an available transfer mechanism. African countries have considerable experience in meeting the requirements of certification schemes.[78] [79],[80] Drawing parallels from certification schemes in the trade of goods, through which most agricultural produce is exported outside Africa, an international privacy certification system could be highly feasible to implement at less cost to bridge the regulatory

70 https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf

71 https://www.wto.org/english/res_e/reser_e/5_luis_inai.pdf

72 https://www.wto.org/english/res_e/reser_e/5_luis_inai.pdf

73 https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,internationally%2Drecognized%20data%20privacy%20protections.

74 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

75 https://iapp.org/news/a/why-cbpr-recognition-in-the-usmca-is-a-significant-development-for-privacy/

76 https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

77 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

78 https://standards4sdgs.unece.org/sites/default/files/2019-07/SDG13_Africa.pdf

79 https://www.intra-afrac.com/News%20Attachments/Paper%20on%20development%20of%20accreditation%20in%20Africa.pdf

80 https://unfss.org/2022/04/07/africa-prepares-to-mainstream-voluntary-sustainability-standards-launch-of-the-african-continental-platform-on-voluntary-sustainability-standards%EF%BF%BC/

gaps and inadequacies. The flexibility provided by the CBPR system could prove beneficial for AfCFTA State Partners, as it allows for local adjustments while maintaining a consistent, global standard for cross-border personal data flows.

Rules and Regulations to Ensure Certainty in the Digital Marketplace

As consumers grow more aware of their personal data's value, trust in its management becomes crucial. Inadequate trust can deter consumers from electronic transactions, thus hindering digital market growth. However, stringent regulations on individual data use and transfer can also impose significant costs, especially for MSMEs. Striking a balance is crucial, enabling data transfers to support digital market expansion while ensuring consumers trust the security and control allocated to their private information. Governments have a crucial role in facilitating the participation of MSMEs in the digital economy by acting as both regulators and enablers. To enable MSMEs to thrive in the digital landscape, governments need to support them through a robust legal, regulatory, and business infrastructure. Key aspects of this support include laws promoting digital adoption, such as those related to digital signatures and electronic authentication, ensuring that online contracts have equivalent validity as their paper-based counterparts. African countries without such laws can leverage existing regional and international resources, such as the United Nations Commission on International Trade Law's (UNCITRAL) model law on electronic signatures,[81] to develop their own regulations. This can be referenced in the AfCFTA digital rules. Moreover, governments can also simplify the administrative processes for establishing and operating businesses. One approach to achieving this is by creating one-stop shops, which would provide MSMEs with easy access to necessary information on legal and administrative requirements for operating formal businesses.

Given the variety of players on digital platforms, regulatory frameworks for digital marketplaces could assign responsibilities related to privacy and personal data protection accountability in the digital marketplace ecosystem, such as responsibility for safe and secure payment methods. Such data privacy legal frameworks could provide customers' rights regarding their personal data's collection, use, storage, and disposal, while also outlining obligations for data controllers and processors, as well as structures for data sharing to improve access to data within the ecosystem.

Providing substantive rules on digital marketplaces at the continental level would ensure that harmonised requirements are established for all platforms. Additional requirements could be included at the level of sector-specific requirements. [82]

81 https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf

82 https://www.unescap.org/sites/default/d8files/event-documents/MSMEs%20and%20the%20Digital%20Economy.pdf

6. Factors for Fostering Inclusion, Innovation and Cohesion

The rapid digitalisation of economies requires regulators to establish innovative solutions to keep up with and encourage new and changing business models. The AfCFTA digital trade protocol should aim to fortify innovation capacity in Africa by proposing mechanisms that enhance State Parties' innovation capacity. Such mechanisms should be based on inclusive coordination and cooperation to engender an equitable distribution of the benefits of digitalisation and digital innovation in Africa. Inclusive coordination and cooperation on innovation is critical for creating an innovation culture in Africa, which is necessary to harness the digital transformation. Innovation should be promoted in all sectors and in all businesses including start-ups, MSMEs, technology companies, and traditional businesses using digital technologies. That could yield a positive impact on microeconomic growth, the quality of life, and closing the digital divide.[83]

The AfCFTA digital trade rules should encourage State Parties to create an enabling environment for inclusive and collaborative innovation intended to establish innovation-driven entrepreneurship ecosystems and data-driven innovation ecosystems. These two ecosystems should be inclusive and collaborative and should aid businesses in developing innovative products and services across Africa. Additionally, the enabling environment for innovation should foster collaborative innovation via international partnerships. That could entail lowering barriers to international innovation networks and knowledge flows.[84] Therefore, cross-border data flows within and outside Africa should be promoted based on trust and respect for privacy and personal data and regional, continental, and international interoperability of the underlying law.

The AfCFTA digital rules could propose a non-exhaustive list of tools that State Parties could deploy to enhance their innovative capacity. Regarding data-driven innovation ecosystems, these could include legal frameworks for cross-border data flows and data sharing. Enacting legal frameworks for start-ups and establishing digital free economic zones could facilitate innovation-driven entrepreneurship ecosystems.

83 https://dial.global/wp-content/uploads/2020/10/SmartAfrica-DIAL_DigitalEconomyInAfrica2020-v7_ENG.pdf

84 https://dial.global/wp-content/uploads/2020/10/SmartAfrica-DIAL_DigitalEconomyInAfrica2020-v7_ENG.pdf

Trusted Data Sharing Mechanisms

Cross-border data flows and data sharing enable the creation of data-driven innovation. Data sharing mechanisms such as trusted data sharing frameworks and open licensing agreements[85],[86] can be utilised to promote data-driven innovation in Africa. Such mechanisms help spur innovation and creativity, facilitate the spread of information, knowledge, technology, culture, and arts, and foster competition along with open and efficient markets.[87] It is pertinent that those data sharing mechanisms place humans and their societal values at the centre of the discussion.[88] Data sharing mechanisms should therefore allow insights to be extracted from data held by different people, companies, organisations or governments without compromising issues of data privacy, security, ownership, and trust. The AfCFTA digital rules could be instructive in establishing harmonised rules on data rights and data sharing principles relating to transparency, fairness, and accountability that can foster trust. The continental digital rules should also establish requirements on data controls and ethical considerations to be embedded in data sharing mechanisms.

Regulatory Sandboxes

Regulatory sandboxes are proposed in African Union Data Policy Framework policy recommendations as tools to enhance innovation in Africa.[89] According to the AfDB, a sandbox is a controlled environment set up by a regulatory body where businesses can test their products and services in the real market without all the bureaucracy that normally needs to be negotiated first.[90] Given the rapid technology advancements and associated new business models in the digital economy, regulatory sandboxes could enable policymakers to keep up with the market and regulate accordingly.[91] These have become prevalent in Africa, especially in the financial sector where a growing number of fintechs seek to address Africa's historical financial challenges in innovative ways.[92] Regulatory sandboxes allow for data, including personal information, to be shared among businesses adhering to domestic laws.

In terms of innovative projects involving cross-border data flows, some recent trade agreements, such as the Canada-United States-Mexico trade agreement CUSMA and the DEPA, have included provisions for cross-border regulatory sandboxes to support innovative projects involving cross-border data flows, while also discouraging data localisation and promoting national regimes that protect rights proportionately.[93] Such multi-jurisdictional sandboxes promote cross-border regulatory harmonisation and enable innovators to scale more rapidly on

85 https://opensource.guide/legal/#why-do-people-care-so-much-about-the-legal-side-of-open-source

86 Microsoft, removing barriers to data innovation, https://news.microsoft.com/wp-content/uploads/prod/sites/560/2021/03/Backgrounder-FAQ-Sheet_FINAL.pdf

87 This provision is provided for in the DEPA.

88 https://direct.mit.edu/books/edited-volume/4586/Trusted-DataA-New-Framework-for-Identity-and-Data

89 See the African Union Data Policy Framework, available at https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

90 https://blogs.afdb.org/economic-growth/whats-in-a-sandbox-new-report-highlights-the-regulatory-benefits-for-government

91 https://blogs.afdb.org/economic-growth/whats-in-a-sandbox-new-report-highlights-the-regulatory-benefits-for-government

92 https://www.openbankproject.com/regulatory-sandboxes-in-africa/

93 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

a regional or global basis.[94] Those advantages could be attractive for innovators, given Africa's small and fragmented markets which make delivery of financially sustainable innovative solutions challenging. The inclusion of cross-border regulatory sandboxes in AfCFTA digital trade rules could allow negotiators to explore data policies and practices to address emerging issues in a collaborative manner, rather than committing to binding rules and to adjust policies based on evidence and stakeholder feedback.[95] Regulatory sandboxes are especially beneficial for emerging players such as MSMEs, given their potential to unlock investment and level the playing field with established businesses.[96]

The implementation of regulatory sandboxes in Africa poses challenges and risks, including competition concerns among participants, constraints on regulators' capacity and resources, potential liability issues in the event of failures or damage at, ambiguous transition paths from sandbox to full market operations, inter-agency coordination problems among regulators, and a lack of sufficient regulatory tools and frameworks.[97],[98] In the context of cross-border sandboxes, despite the economies of scale, this could be realised by multiple regulators operating the sandbox, the initial design costs could be significant.[99] Given these challenges and risks, regulatory sandboxes may not be the most feasible, efficient or impactful means of creating an enabling regulatory environment for innovative projects involving cross-border data flows in Africa.

Innovation Offices

Another mechanism that the AfCFTA could propose to assist innovators and businesses in overcoming regulatory barriers to innovations is the innovation office.[100] These would set up by State Parties to provide regulatory clarification through engagements with innovators and businesses seeking to offer innovative products and services in the digital market. The key objective of innovation offices is to facilitate regulator–innovator engagement and mutual learning in a pro-innovation setting.[101] Some African countries have established innovation offices (regulator-business engagement programmes), albeit with different names, forms, and functions. These include national investment promotion agencies for local and foreign direct investment facilitation, trade point centres for cross-border trade facilitation, and digital hubs which offer central meeting points for tech, innovation and creative businesses within the region.[102]

These existing programmes could offer significant reference points for designing innovation offices in Africa. Additionally, innovation offices could serve as inquiry points or one-stop shop centres commonly promoted in trade agreements but should be designed to go beyond

94 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

95 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

96 https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf

97 https://fsdafrica.org/blog/fintech-and-regulation-thinking-outside-the-sandbox/

98 https://www.cgap.org/blog/running-sandbox-may-cost-over-1m-survey-shows

99 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

100 https://fsdafrica.org/blog/fintech-and-regulation-thinking-outside-the-sandbox/

101 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

102 https://ruraldigital.eu/wp-content/uploads/2020/01/CORA_Digital_Hub_Guide_14.01.2020_Executive_Summary.pdf

providing information on regulations and support on regulatory compliance. The interaction between regulators and innovators enabled by innovation offices poses several benefits for regulators and innovators. Regulators identify emerging issues and obtain evidence to inform policy developments, whilst innovators receive information on the current regulatory landscape in a local context and the regulatory direction including at the sectoral level.[103] In Africa's context, innovation offices are considered a compelling option for capacity-constrained regulators, since their establishment in most cases does not involve protracted legislative or regulatory change.[104] Additionally, the services offered can be calibrated according to demand and capacity.

Open Government Data

Open government data is a crucial resource for fostering innovation, competitiveness, and economic development in the digital economy. Open government data relates to making data and information produced by public institutions freely available in a form and based on conditions that allow use, re-use and distribution of the data by anyone.[105] Africa's performance in publishing and using open data is relatively poor at the global level (Open Data Barometer, 2016).[106] Robust data is needed in Africa to drive development goals. That includes public access to government data through safe, accessible, and standardised means. The AfCFTA digital rules should encourage State Parties to facilitate public access to government information and endeavour to make that information available as open data. The increased accessibility and usage of open government data can lead to the creation of new business opportunities, driving competitiveness and innovation. Given that businesses would not have to purchase specific datasets or produce them themselves, access to open government data allows business to save on such costs (OECD 2020a). That could spur investment in new products and services for cross-border markets. The negotiators of the AfCFTA digital rules could be informed by the DEPA, which encourages cooperation on the use of open data licensing models that allow for the free access, usage, modification and sharing of open data within the boundaries of respective laws and regulations to ensure safe and widespread availability. That could entail cooperation and standardisation of public licences made available online. Privacy, legal, financial and technological related issues are cited as major challenges for implementing open government data.[107] By encouraging State Parties to safely democratise access to government information, the AfCFTA digital rules would spark a new era of data-driven innovation. Provisions on open government would give credibility to the Africa Data Consensus which sets out the vision, principles and key actions needed to achieve a data revolution in Africa.[108]

103 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

104 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

105 https://www.undp.org/sites/g/files/zskgke326/files/2023-03/20230317_Open%20Government%20Data_fin.fin_.pdf

106 A global measure of how governments are publishing and using open data for accountability, innovation and social impact. https://opendatabarometer.org/4thedition/?_year=2016&indicator=ODB

107 https://www.frontiersin.org/articles/10.3389/frma.2022.985999/full

108 https://www.cgdev.org/sites/default/files/Africa-Data-Consensus.pdf

Start-up Acts

Start-ups are sources of creativity and excellent for building an innovative culture. Creating an enabling environment for start-ups could promote market-led solutions to socio-economic challenges in Africa. Through legal frameworks for start-ups, countries can provide the targeted incentives to start-ups necessary to address start-up challenges, such as unfavourable regulatory environments, lack of skilled labour, access to finance, lack of business development services, and vulnerability (ICReport, 2021). So far, only Senegal, Tunisia, Nigeria and Congo have enacted Start-up Acts. Rwanda, Ghana, Kenya, Ethiopia and Uganda are in process of adopting similar legislative frameworks. These developments further signal a progressive shift in the continent's approach to fostering entrepreneurial innovation. In terms of incentives, it is most notably Senegal's Start-up Act that provides a three-year tax exemption for start-ups, specialised training programmes for young and female entrepreneurs, and an easily accessible start-up registration platform hosted on a government website.

As Africa demonstrates increasing enthusiasm towards cultivating supportive environments for start-ups, it's crucial that considerations for start-up regulation are integrated within negotiations on continental rules for digital trade. Moreover, continental rules could ensure a harmonised and cohesive approach to start-up regulation, promoting fair competition and fostering cross-border collaboration.

Digital Free Economic Zones

A new generation of free zones called digital free zones (DFZ) is emerging. These seek to utilise digitalisation to offer combined online and business services to business within that ecosystem.[109]The DFZ adopts characteristics of the traditional free economic zones with regard to the objective of facilitating international trade in goods and services by offering certain incentives that attract businesses, especially foreign investors, to the region or country. For traditional free zones, incentives tend to be exclusively provided by the government and include different regulatory frameworks and tax schemes, such as expedited licensing procedures, customs and tax exemptions. On the contrary, DFZs can be established by the private sector or the government. In essence, DFZs offer a technological and operational platform to facilitate trade in goods and services through a variety of digital services such as integrated and connected technology infrastructure, integrated and automated free zone operations, digitally enabled services for DFZ stakeholders, interconnected ecosystems through physical and virtual platforms, and knowledge and experience sharing between DFZs and businesses.[110] DFZs can accommodate a wide variety of businesses from large companies to MSMEs, governments, financial institutions, logistics operators, and e-commerce organisations, providing a range of services including business process outsourcing, supply chain management, computing, storage, transaction validation, databases, and knowledge and information tech.[111] DFZs can enable e-commerce business to create partnerships in technology, analytics, delivery and

109 https://www.worldfzo.org/Portals/0/OpenContent/Files/614/Digital_Free_Zones_.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=world_fzo_weekly_news_march_16&utm_term=2021-03-16

110 https://www.worldfzo.org/Portals/0/OpenContent/Files/614/Digital_Free_Zones_.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=world_fzo_weekly_news_march_16&utm_term=2021-03-16

111 https://bpospanama.com/

payments which could assist them in strengthening their business offering, customer base, and supply chains. By providing access to digital infrastructure, operational flexibility, commercial networking platforms and attractive tax regimes, DFZs can enhance competition in the digital economy.[112]

Negotiators of the AfCFTA digital rules could look into DFZs based on the experience with traditional free zones that are prevalent in African countries. The AfCFTA digital rules could then recommend that State Parties set up rules for DFZs to promote digitalisation and digital trade. DFZs can be a powerful tool for African governments looking to attract foreign investment in digitalisation. The governments could provide targeted incentives, whilst investors in DFZs would bring specialised infrastructure and know-how, which could be utilised for businesses within the DFZ ecosystem. DFZs in Africa could enable data-value chains, thus supporting the larger goal of economic diversification and closing the digital gap with digitally advanced countries. While this concept seems promising, implementing it effectively would require careful consideration. It is crucial to strike a balance between promoting business growth and ensuring that issues like data privacy and cybersecurity are adequately addressed. It would also be essential to ensure equal access and opportunities for all businesses and individuals in the region to avoid exacerbating digital divides.

The foregoing section discussed developing regulatory innovation initiatives proposed or being undertaken by regulators globally, including in Africa, to promote inclusive innovation in the digital economy. Those initiatives could be replicated across Africa. Through the AfCFTA, State Parties could be encouraged to assess the potential impact of such initiatives on developing innovation-driven entrepreneurship ecosystems and data-driven innovation ecosystems. That could entail distilling lessons learned from implementation in other countries, particularly in Africa. Conducting such impact assessments is important for cross-regional knowledge and policy sharing, and especially valuable for regulators with limited resources.[113] That study could benefit African countries by broadening awareness of regulatory innovation options and cost-benefit considerations.[114]

112 https://www.worldfzo.org/Portals/0/OpenContent/Files/614/Digital_Free_Zones_.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=world_fzo_weekly_news_march_16&utm_term=2021-03-16

113 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

114 https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

Conclusions

The rapidly growing digitalisation of African economies propelled by global advancements in digital technologies poses challenges for regulators. New business models, products and services raise questions on whether, and how, they should be regulated. Authorities must strike a delicate balance between the opportunities and risks that the digital economy brings for economic transformation and other public policy objectives. These issues are ever so acute given the informal and unregulated nature of most businesses, and the limited capacity and resources in Africa.

The main challenges of data sharing include difficulties in compiling and organising data, lack of data availability in a suitable digital format, lack of knowledge about data location, data quality issues (accuracy, reliability, and up-to-dateness), and undefined and time-consuming approval processes, all of which can be overcome by implementing good data governance policies and procedures to facilitate effective and value-driven data sharing within and between organisations.

The argument for designing MSME-friendly data protection regimes stems from their unique position and abilities within the digital economy ecosystem. Governments should take on the responsibility of providing comprehensive training and enhancing awareness about these laws among MSMEs. They should also implement supportive mechanisms to help MSMEs meet legal requirements without threatening their operations.

Establishing a data protection framework that acknowledges the unique conditions and capacities of MSMEs is not only beneficial, but also essential. It ensures individual data rights while fostering the growth and sustainability of MSMEs - a win-win for Africa's digital economy. Given the ongoing WTO negotiations on the Joint Statement Initiative on e-Commerce, which contains provisions potentially opposing data localisation requirements, it is crucial for the negotiations of the African Continental Free Trade Area Protocol on Digital Trade to take these developments into account, particularly as some African countries such as Nigeria, Kenya and others are directly involved, and their existing data localisation policies might conflict with the proposed international norms.

Regarding harmonisation of rules regulation for digital marketplaces, negotiators should recognise that harmonisation does not imply uniformity. Instead, it requires agreement on fundamental principles that participating states should respect and implement in their domestic laws, such as the definitions and principles of data protection, to prevent fragmentation and

unpredictability.[115] The AfCFTA should focus on the aspects of the digital marketplace that are the critical in terms of harmonisation for cross-border transactions. An analysis of the digital marketplace value chain would assist in identifying the key aspects on which to focus. The value chain would show the key players, information and activities involved in the supply, distribution and post-sale activities of goods for the market.

The proposed solutions to cross-border data transfers could be further analysed and developed at the continental level to establish AfCFTA digital rules compelling State Parties to make commitments on data governance and data protection implementation that are directly manageable and are an asset to MSMEs.

115 https://www.tralac.org/blog/article/15620-to-cooperate-or-to-harmonise.html