Funded by the European Union

DISCUSSION PAPER No. 379

Cross-border data flows in Africa: Continental ambitions and political realities

By Melody Musoni, Poorva Karkare and Chloe Teevan

October 2024

Africa must prioritise data usage and cross-border data sharing to realise the goals of the African Continental Free Trade Area and to drive innovation and AI development. Accessible and shareable data is essential for the growth and success of the digital economy, enabling innovations and economic opportunities, especially in a rapidly evolving landscape.

African countries, through the African Union (AU), have a common vision of sharing data across borders to boost economic growth. However, the adopted continental digital policies are often inconsistently applied at the national level, where some member states implement restrictive measures like data localisation that limit the free flow of data.

The paper looks at national policies that often prioritise domestic interests and how those conflict with continental goals. This is due to differences in political ideologies, socio-economic conditions, security concerns and economic priorities. This misalignment between national agendas and the broader AU strategy is shaped by each country's unique context, as seen in the examples of Senegal, Nigeria and Mozambique, which face distinct challenges in implementing the continental vision.

The paper concludes with actionable recommendations for the AU, member states and the partnership with the European Union. It suggests that the AU enhances support for data-sharing initiatives and urges member states to focus on policy alignment, address data deficiencies, build data infrastructure and find new ways to use data. It also highlights how the EU can strengthen its support for Africa's data-sharing goals.

Table of contents

List of tables

Glossary

Data:	Information in both digital and non-digital form which can be a collective of different types (confidential, personal, non-personal, big data) from different sectors (healthcare, education, meteorology) found at different levels (e.g. economic data could be at macro, industry, firm or individual level).
Personal data:	Any information that relates to an identified or identifiable living individual directly or indirectly (e.g. names, addresses, bank accounts, online identifier, genetic data, physiological data, location data etc.).
Non-personal data:	Any information that does not refer to an identified or identifiable natural person or data that was initially personal but subsequently anonymised.
Digital sovereignty:	The authority or powers exercised by governments, usually through policies and laws, over digital infrastructure, data, activities in cyberspace including control over their citizens' activities in cyberspace.
Data localisation:	No single definition but it consists of the laws and measures put in place by governments which encumber the movement of data across national borders or limit where and by whom data is stored and the restrictions vary from strict, conditional to open transfers.
Cross border data flow:	The movement or transfer of data (personal and non-personal) across country borders usually through electronic means. Also referred to as transborder data flows.
Data value creation:	Using data to develop solutions which can solve real world problems and promote sustainable development (e.g. analysing big data to inform resource allocation needs to enhance service delivery.

Acknowledgements

This project was funded by the European Commission. The core team also consisted of Sérgio Luis Cossa and Talla Ndiaye who provided valuable insights and details into the policy frameworks in Mozambique and Senegal respectively. ECDPM's Sara Gianesello accompanied the field visit to Senegal and Nneka Okechukwu assisted in preparing the infographic to show the state of play of cross border data policies in African countries. Bruce Byiers provided helpful comments on previous drafts of this report to bring the theme of digital policies closer to the regional integration agenda in Africa. The report also benefited from layout and other editorial assistance by several other ECDPM colleagues. The authors would like to thank the numerous experts and policymakers who shared their insights throughout the research process. The authors take responsibility for any factual errors. For any feedback or suggestions regarding future work, please contact mmu@ecdpm.org, pk@ecdpm.org and cte@ecdpm.org.

Acronyms

ADE	National Agency for Geospatial Development
AfCFTA	African Continental Free Trade Area
AGM	Annual General Meeting
AI	Artificial Intelligence
ANSD	National Agency of Statistics and Demography
AU	African Union
AUC	African Union Commission
AUDA NEPAD	African Union Development Agency - New Partnership for Africa's Development
BMZ	Bundesministerium für Wirtschaftliche Zusammenarbeit (German Federal Ministry of Economic Cooperation and Development)
CBN	Central Bank of Nigeria
CBDFs	Cross Border Data Flows
CDP	Personal Data Protection Commission
CDPB	Continental Data Protection Body
CEMAC	Central African Economic and Monetary Community
CGIAR	Consultative Group for International Agricultural Research
CNBB	National Centre for Biotechnology and Biological Sciences
CoE	Council of Europe
COVID-19	Coronavirus Disease 2019
CPLP	Community of Lusophone Countries
CSIRT	Computer Security Incident Response Teams
DFFT	Data Free Flow with Trust
DGA	Data Governance Act
DGIFA	Data Governance & Innovation Forum for Africa
DIF	Digital Investment Facility
DPA	Data Protection Authority
DPF	Data Policy Framework
DRC	Democratic Republic of the Congo
DSM	Digital Single Market

DTP	Digital Trade Protocol
DTS	Digital Transformation Strategy
EAC	East African Community
ECCAS	Economic Community of Central African States
ECDPM	European Centre for Development Policy Management
ECOWAS	Economic Community of West African States
EU	European Union
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
ICT	Information and Communication Technology
ID	Identification Data
INAGE	National e-Government Institute
INAM	National Institute of Meteorology
INCM	National Institute of Communications of Mozambique (Instituto Nacional das Comunicações de Moçambique)
INTIC	National Institute of Information and Communication Technologies
MDAs	Ministries, Departments, and Agencies
NADPA	Network of African Data Protection Authorities
NDPA	Nigerian Data Protection Act
NDPC	Nigerian Data Protection Commission
NDPR	Nigerian Data Protection Regulation
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
NSO	National Statistics Office
OECD	Organisation for Economic Co-operation and Development
OFESA	Eastern Africa Forest Observatory
OPG	Open Government Partnership
PAENS	Digital Economy Acceleration Program Portuguese-speaking African countries (Países Africanos de Língua Oficial Portuguesa)
RECs	Regional Economic Community
SADC	Southern Africa Development Community
SDBA	Safe Digital Boost with Africa
SSA	Sub-Saharan Africa
UEMOA	West African Economic and Monetary union. (Union Économique et Monétaire Ouest Africaine)
UN	United Nations
UNECA	United Nations Economic Commission for Africa
US	United States
USMCA	US-Mexico-Canada Agreement
WARDIP	West Africa Regional Digital Integration Project

Executive summary

Data is key to the digital economy as a whole, and the backbone of the evolving Artificial Intelligence (AI) industry. It exists at various levels (e.g. economic data could be at macro, industry, firm or individual level), in different sectors (e.g. healthcare, education, agriculture, meteorology etc.), and in multiple forms (e.g. confidential, personal, non-personal, big data, open data etc.). Data sharing and use promotes economic growth, competition, research and scientific advancements (especially AI innovations which heavily depend on data to build algorithms), and transparency.

Cross-border data flows (CBDFs) within Africa are essential for the newly established African Continental Free Trade Area (AfCFTA) and the digital single market (DSM). They could also be the key to developing sufficiently large data sets to feed African built sectoral AI models that cater to African needs. Restrictive measures such as strict data localisation could hinder economic growth, negatively impacting trade and investment.

The African Union (AU) has developed a diverse set of legal and policy instruments aimed at promoting digital transformation and an integrated digital economy in Africa. Continental and regional instruments reflect diverse values (such as democracy, rule of law, transparency, social justice, peace, and security), goals (including economic growth, geopolitical interests, and political stability), and mechanisms (like regulatory convergence, capacity building, trade agreements, and multilateral partnerships), leading to varied approaches to data sharing.

While each instrument targets specific policy objectives, they complement each other, collectively presenting a coherent approach to intra-African cross-border data sharing with a strong emphasis on data protection and security. These instruments advocate for free data flow and intra-continental transfers, discourage strict data localisation (which completely restricts data transfers outside a country or mandates local storage), and support conditional localisation that permits data transfers under clearly defined conditions. This reflects a recognition that Africa can potentially achieve much more if its countries work together to develop digital trade under the AfCFTA, and to develop a dynamic and innovative data economy that can in turn provide the data sets to develop African-built AI.

There is no single continental policy on cross-border data flows (CBDFs), but there are evident synergies across the various digital policy and legal frameworks at the AU level. Continental frameworks emphasise the necessity of cross border data sharing (e.g. AU Data Policy Framework) and provide guiding rules to facilitate it with an emphasis on trust and security especially of personal data (e.g. Malabo Convention). They also promote the harmonisation of national frameworks. Many of these instruments have been adopted or formulated only recently (e.g. AfCFTA Digital Trade Protocol and the Continental AI Strategy), and a comprehensive assessment of their coherence and consistency is still pending.

Within the regional economic communities (RECs), policies have primarily concentrated on regulating personal data and protecting the rights of data subjects.

While a common criticism of policy frameworks in Africa is that, despite having many well-crafted policies, implementation is often lacking, these instruments face shortcomings that have impeded their adoption at the national level. They can be overly broad, lack clear implementation guidance, and impose burdens on Member States. Conversely, broad definitions elaborated so as to accommodate the diverse contexts of Member States can grant excessive flexibility. Without clear data-sharing mechanisms and frameworks, the crucial link between policy and practice is missing, making enforcement a significant challenge. The paper highlights these shortcomings, which may inadvertently inhibit cross-border data flows (CBDFs).

There are also challenges of implementation. This may include lack of incorporation of continental instruments into national laws (e.g. Malabo Convention) or developing national strategies aligned with continental guidelines (e.g. Data Policy Framework, Continental AI Strategy). National policies often prioritise local interests, which can overshadow the continental vision. Our research suggests that varying ideologies, socioeconomic contexts, security concerns, and economic priorities influence national data-sharing policies, leading to differences across countries by looking at the case of Mozambique, Nigeria, and Senegal. Implementation also relies on the socio-political capacity at the national level to coordinate across state agencies, which varies significantly among countries and is often subject to administrative delays and disputes. Ineffective coordination, competing mandates and perverse incentives may further hinder effective implementation.

All these factors together help explain the gap between policy and practice on the one hand, and between national and continental processes on the other.

Developing a comprehensive data economy in Africa will require efforts at both continental and national levels. The paper offers recommendations to strengthen the guidance and implementation frameworks at the continental level, as well as to address policy differences and implementation challenges at the national level to avoid fragmentation and enable interoperability.

The EU is an important trade, investment and development partner for African countries, and can play a role in supporting CBDFs in Africa. This might include sharing some of the EU’s own experiences as it implements its own European Data Strategy, and leveraging the digital pillar of Global Gateway to support the African data economy. Supporting Africa's efforts to develop CBDFs is in line with the EU's goal of leading international cooperation on data and shaping global standards. Indeed, the EU is already supporting the AU and its member states in developing data policies through the Data Governance in Africa initiative.

1. Introduction

Data plays an important role in the broader digital economy and is the backbone of the Artificial Intelligence (AI) economy. It exist at various levels (e.g. economic data could be at macro, industry, firm or individual level), in different sectors (e.g. healthcare, education, agriculture, meteorology etc.), and in multiple forms (e.g. confidential, personal, non-personal, big data, open data etc.) (Beyleveld and Sucker 2022). Data sharing and use promotes economic growth, competition, research and scientific advancements (especially AI innovations which heavily depend on data to build algorithms), and transparency (Mwaya 2022, The Economist 2018).1 Depending on the extent to which it is allowed, public and private sector data access and sharing can generate social and economic benefits worth between 1 - 2.5.% of GDP, while restrictions can cut trade output by up to 7% and increase prices (Mwaya 2022). Cross-border data flows (CBDFs) are an important enabler in Africa's digital economy, which is estimated at US$115 billion in 2022 (Endeavor Nigeria 2022) and could grow by 57% within 5 years (CSEA 2021). Even though most digital infrastructure and trade in African countries takes place with partners outside of Africa, smooth CBDFs within Africa are essential for the newly established African continental free trade area (AfCFTA) and the digital single market (DSM).[2] They could also be the key to developing sufficiently large data sets to feed African built AI models, particularly in specific sectors. Restrictive measures such as strict data localisation could hinder economic growth, negatively impacting trade and investment (Beyleveld 2021, GSMA report 2021, Oloni 2024).

On paper, African countries agree that intra-Africa CBDFs are essential to achieve the continental vision outlined in key policy documents like the Agenda 2063, the Digital Transformation Strategy and the AfCFTA Agreement. These documents advocate for free continental CBDFs to boost the DSM while ensuring privacy, data protection and national security. Recent instruments such as the AfCFTA Digital Trade Protocol, the Malabo Convention, the Data Policy Framework and the Continental AI Strategy demonstrate ongoing efforts to improve data sharing across the continent.

In practice, however, Member States approach CBDFs in Africa differently, with varying capabilities to implement the continental vision. Limited digital infrastructure, inconsistent policy frameworks hindering intelligible data sharing and efforts to combat foreign dominance in Africa's digital economy which also impacts digital sovereignty, all lead to restrictions on CBDFs (Soule interview series 2023). This raises data sovereignty concerns and prompts data localisation measures to regulate data flows. Leaders fear that losing control over data could lead to intellectual monopoly and data colonialism, stifling African entrepreneurship with unsuitable non-African tools and generating profits elsewhere using African data while

[1] In the data value chain: data producers generate data from the internet of things and traditional big data sources; data aggregators extract, format and collate it; data presenters simplify complex datasets for users; insight providers generate value from advanced analytics such as machine learning algorithms and statistical models (Naidoo 2020).

[2] According to the AU, the Digital Single Market across Africa would entail enhanced (broadband) connectivity across countries and regions in the continent, elimination of roaming charges, harmonised regulation and digital innovation for greater economic integration in line with the AfCFTA (Digital Transformation Strategy).

depriving countries of revenue opportunities (Sampath and Tregenna 2022). As a result, CBDFs in Africa remain limited, with only five countries counting among the top hundred countries that are digitally connected and open to sharing data (Global Competitiveness Index for 2020).

This paper examines the extent to which the continental vision on data sharing and data flows is implemented at the national level. We identify and discuss the discrepancies between policy and practice by first analysing the extent to which continental policies promote CBDFs in Africa and then looking at how the continental and national policy and legal frameworks relate to each other. We explore why national policies diverge from continental commitments by looking at the factors shaping the current digital policy landscape in selected countries. Finally, we provide actionable policy recommendations at the continental, national and EU level to bridge the gap between policy and practice to promote continental data sharing and regional integration.

To illustrate the varying data policy landscapes or 'data contexts', we selected three countries as case studies, Senegal, Nigeria and Mozambique. Senegal is one of the first countries to adopt a data strategy inspired by the AU Data Policy Framework (DPF) and shows how the DPF is reflected in national policy. Nigeria, despite being one of Africa's vibrant digital economies, has been slow in developing a clear data strategy and only recently adopted a personal data protection law. Mozambique, one of Africa's least digitally prepared countries, does not have a data strategy and lacks other regulatory framework for data governance.

This work draws on a literature review, an extensive analysis of African policies and strategies and over 60 interviews with officials, experts and private sector representatives working on data governance in Africa. Interviews were conducted in person in Nigeria, Senegal and Mozambique, as well as online with officials and experts in Africa and Europe.

The paper is organised as follows: Section 2 discusses the continental and regional vision on CBDFs and their shortfalls. Section 3 synthesises the main characteristics of national policies observed in the three case study countries. Section 4 identifies factors that explain the gap between national and continental frameworks and vision. Section 5 provides recommendations for the AU and relevant organs, national governments, and for the EU given its critical role in Africa's data governance ecosystem.

2. Continental vision on CBDFs

The African Union (AU) has a wide range of legal and policy instruments to promote digital transformation and regional (data) integration in Africa. While each instrument may have a specific policy objective, overall, there is complementarity across them all with coherence in their approach to data-sharing while particularly highlighting the importance of data protection and security. In particular, the Malabo Convention is prominently featured across these frameworks, emphasising trust and security when processing personal data. These instruments promote free data flow and intra-continental transfers, discourage strict data localisation (measures that completely restrict data transfers outside a country or mandate local storage), and favour conditional localisation that allows data transfers under clearly defined conditions (Musoni et al. 2023). This section highlights the different continental and regional policies that indicate the AU's approach to governing continental CBDFs, and identifies some of their shortcomings.

2.1. AU policy instruments promoting CBDFs

There is no one continental policy on CBDFs. Instead, several continental instruments indicate the vision highlighted above. Though many of these instruments were only recently adopted/formulated, and there is yet to be a more robust assessment in terms of coherence and consistency between them, at first glance, there are synergies on CBDFs across the various digital policy and legal frameworks at the AU level. They highlight the need for transborder data sharing (DPF, Continental AI Strategy) and provide the guiding rules to facilitate them (Malabo Convention, DTP). They also encourage the harmonisation of national frameworks.

Table 1: Overview of the continental digital policies

Policy	Purpose	Position on CBDFs
AU Digital Transformation Strategy 2020 - 2030	Comprehensive plan to leverage digital technologies for transforming African economies and societies, focusing on four key pillars: digital infrastructure, digital skills, digital innovation and entrepreneurship, and enabling environment and regulations.	Supports the AfCFTA by promoting intra-African digital trade, e-commerce, data sharing, and the development of data standards and interoperability frameworks. Advocates for harmonised policy, legal, and regulatory frameworks, including data protection in line with the Malabo Convention. Pioneering for regulations enabling the free flow of *non-personal* data. Following its endorsement, several policies, frameworks, and initiatives have focused on elaborating or enabling its foundational pillars.
AU Data Policy Framework 2022	Data governance framework covering both personal and non-personal data. Outlines a vision,	Advocates for balanced policies on data localisation, emphasising the benefits of data sharing over data hoarding. Encourages Member States to weigh the costs and

	principles, strategic priorities and recommendations for developing *national* data systems to derive value from data of citizens, government entities and industries.	benefits of localisation, considering human rights and broader economic development priorities. Invites African countries to shift focus from data localisation to promoting the free and secure data flows while safeguarding human-rights, upholding security and ensuring equitable access and sharing of benefits (Musoni 2024).
AU Interoperability Framework on Digital ID 2023	Establishes interoperability rules for digital ID data to enable citizen participation in the digital economy, facilitate digital payments and digital financial services. Provides standards and processes for trusted, secure sharing of personal data.	Introduced in December 2023, though the framework's adoption status remains unclear. Potential interest among Smart Africa[3] countries to develop interoperable digital ID systems with the ability to exchange information securely and seamlessly (Smart Africa Digital ID Blueprint) under the leadership of Benin.
AU Continental AI Strategy 2024	Outlines continental approach to building the AI economy through AI development and use, emphasising infrastructural capabilities such as data centres, cloud computing and quality data for Member States' AI development.	Adopted following extensive multi stakeholder discussions including on the AUDA NEPAD White Paper on AI. Recommends Member States to develop data policies and strategies enabling access and sharing of non-personal data. Urges the establishment of data governance frameworks with standards for ethical, responsible and secure data-sharing. Highlights the need for intra-Africa coordination on AI, advocating for regional cooperation in open data and proposing a regional instrument to guide data sharing and cross border data transfers.
AUDA NEPAD White Paper on Responsible AI 2024	Identifies areas that African countries need to prioritise in order to effectively leverage AI. These areas being human capital development, infrastructure and data, creating an enabling environment, boosting the AI economy and building sustainable partnerships.	Encourages African countries to develop robust data storage capabilities to reduce foreign dependence, stimulate local innovation, attract investments, and drive economic growth. Supports investments in local data centres, fostering data governance frameworks, and promoting data sovereignty to unlock the full potential of data-driven initiatives for economic development and innovation. Recommends laws and regulations promoting data storage and

[3] Smart Africa is an initiative by some African leaders to drive sustainable socio-economic development through digitalisation. It started with 7 African governments but today it consists of 39 countries.

		transfer within Africa, encouraging the development of robust data infrastructure to reduce reliance on non-African data storage facilities. Proposes measures for CBDFs to address challenges and opportunities associated with data governance and sovereignty, specifically in the AI context in Africa.
AU Convention on Cyber Security and Personal Data Protection 2014	Legally binding instrument addressing electronic commerce, personal data protection, and cybersecurity. Establishes rules for electronic transactions to promote continental e-commerce. Mandates Member States to adopt policies and strategies on cybersecurity and promote international cooperation. Provides guidance on personal data processing.	Permits conditional transfer of data (Oloni 2024). Requires Member States to enact data protection laws safeguarding individual rights and obliging data controllers[4] to ensure adequate protection when sharing with non-Member States of the AU (Article 14(6)(a)). In essence, the Malabo Convention promotes free CBDFs while protecting rights through established safeguards.
AfCFTA Digital Trade Protocol 2024[5]	Seeks to regulate and facilitate digital transactions through common continental rules, overcoming fragmentation challenges, to achieve the objective of the AfCFTA. Shapes CBDFs in Africa beyond the Malabo Convention as it focuses on both personal and non-personal data within the context of digital trade.	Encourages State Parties to facilitate data transfers while ensuring data protection and privacy, remove barriers like local data storage requirements and promote data innovation through the establishment of policies and standards on data mobility and data portability. Consists of exceptions allowing Member States to diverge from the general rule of unrestricted data flows as long as the adopted measures serve 'legitimate public policy objectives' or 'protect essential security interests.

[4] A data controller is any person (natural, legal, public, private, organisation, association, etc) that decides to collect and process personal data and determines the purposes.

[5] This analysis is based on the leaked version of the DTP.

2.2. Policy instruments at the regional level promoting CBDFs

Within the regional economic communities (RECs), policies on CBDFs have exclusively focused on regulating personal data and safeguarding the rights of data subjects. Table 2 summarises policies in four RECs in Africa namely the Economic Community of West African States (ECOWAS), the Southern African Development Community (SADC), The Economic Community of Central African States (ECCAS) and the East Africa Community (EAC) and their respective approaches to transfer of personal data.

Table 2: Overview of RECs policies on CBDFs

Policy	**Purpose**	**Position on CBDFs**
2010 ECOWAS Supplementary Act on Personal Data Protection	Binding treaty regulating personal data processing among Member States, inspired by the Malabo Convention.	Establishes adequacy requirements allowing transfers to non-Member States with adequate protection of privacy, freedoms and individual rights in data processing.[6] Except for the Gambia, Guinea-Bissau, and Liberia, all members have adopted domestic data protection laws (Musoni, Domingo, Ogah 2023), with Guinea, Mali, Niger and Togo reportedly copy-pasting provisions of Supplementary Act (Abdulfauf 2024).
2013 SADC Model Law on Personal Data	Non-binding model law setting out data protection principles, rights and obligations for Member States to consider when developing national laws.	Provides specific conditions (separately for SADC and non-SADC Member States) for personal data transfer.[7] Mozambique and Comoros are the only countries with no domestic data protection law in place.
2013 ECCAS Model Law and the Economic and Monetary Community of Central Africa (CEMAC) Consumer Protection Directive	Similar in scope to the SADC Model Law (King'ori 2024).	Three articles on cross-border data transfers; restricts personal data transfers to non-ECCAS members unless the recipient jurisdiction can ensure an adequate level of protection compared to the ECCAS model law, or when the data controller offers sufficient guarantees for protection.[8] Burundi, Cameroon and the Central African Republic have not yet adopted national data protection laws.

[6] Article 36 of the ECOWAS Supplementary Act.

[7] Articles 43 and 44.

[8] Also see King'ori 2024.

2008 EAC Legal Framework for Cyber Laws	Provisions on a range of issues from data protection, to consumer protection, electronic transactions, intellectual property and taxation.	No explicit provisions on CBDFs. Recent adoption of data protection laws in the DRC, Kenya, Rwanda, Uganda and Tanzania is said to be the result of pressure from Europe[9] rather than pressure or urgency to comply with the Malabo Convention (Fidler 2024).

2.3. Shortcomings of continental instruments

Continental and regional instruments embody different values (e.g. democracy, rule of law, transparency, social justice, peace and security), aims (e.g. economic growth, geopolitical interest, political stability), and instruments (e.g. regulatory convergence, capacity building, trade agreements, multilateral partnerships) resulting in different approaches to data-sharing (Shahin et al. 2024). Shortcomings to these instruments have hindered their adoption at the national level. They can be overly broad, lack implementation guidance, and be burdensome to Member States. In other cases, rather broad definitions give Member States excessive flexibility. This section highlights these shortcomings which may inadvertently inhibit CBDFs.

2.3.1. Broad scope

AU instruments can be very broad in scope. The Malabo Convention covers “data protection, e-commerce, cybersecurity and cyber-crime”, aggregating “human rights, criminal and trade and commercial law issues in a single instrument” (Ayalew 2022). Its slow adoption - taking nine years for only 15 countries to ratify, and excluding major players like Egypt, Nigeria, South Africa and Ethiopia (where the AU sits) - also affects its credibility (Ifeanyi-Ajufo 2024).

Other instruments are comprehensive to the extent that they become vague or impose onerous conditions on Member States. The AfCFTA DTP with its numerous unfinished annexes risks obscuring its precise provisions. While it encourages free flow of data, the DTP allows exceptions for 'legitimate public policy objectives', but defining and proving legitimacy is challenging. Some have raised concerns that exceptions will be frequently used without sufficient recourse to challenge decisions or obtain a verdict (CIPIT 2024). Others highlight that frameworks like the DPF put pressure on Member States to do too much (Saturday and Nyamwire 2023).

2.3.2. Focus on personal data

Most discussions until recently have focused on personal data protection through enforceable instruments, with limited attention on governance and sharing of other data types to promote intra-African CBDFs. For instance, despite its delayed adoption, the Malabo Convention is a legally binding instrument designed to protect personal data. Several countries are adopting

[9] The EU’s General Data Protection Regulation 2016/679. The Council of Europe data protection convention (Convention 108 and 108+). Companies found it cost-effective to adopt GDPR compliance in Africa and lobbied for similar laws to ease compliance. The GDPR, as seen as a global gold standard, influenced African regulations - a phenomenon known as the Brussels effect.

personal data protection laws with data regulators for monitoring and enforcing compliance. The AU DPF was groundbreaking for expanding its focus to include detailed guidelines on the use of non-personal data. However, it is not a legally-binding instrument. The AfCFTA DTP shows more promise by also regulating both personal and non-personal data and is intended to be legally-binding, but still has issues to be ironed out (see below).

Non-personal data sharing among African countries under specific sectoral arrangements/agreements may not be framed under continental frameworks. African countries share climate and environment-related data for better preparation against natural disasters or to conserve biodiversity.[10] The focus of such arrangements is usually on specific policy objectives like public health during the COVID-19 pandemic rather than economic development, which now drives CBDF discussions (Koch 2022).

2.3.3. Insufficient guidance

Some AU instruments lack guidance to Member States and RECs. The Malabo Convention in particular offers limited guidance on data localisation and precise data transfer rules or mechanisms (Beyleveld and Sucker 2024; King'ori 2024). Similarly, the ECOWAS Supplementary Act lacks crucial terminologies such as cross-border transfer, and rights regarding complaints to regulators or data portability (Saturday and Nyamwire 2023). Further, the DTS also lacks an implementation framework/s for its different pillars affecting its credibility. The DPF is promising, providing Member States with a clear roadmap for policy domestication. Some African countries, including Benin, Burundi, Egypt, The Gambia, Madagascar, Mozambique, Ghana, Rwanda, Tanzania, Uganda and Zambia, sought AU support on national implementation, and GIZ, supported by a wider Team Europe Initiative, is supporting the AU in providing technical support to selected countries.

2.3.4. Not reflecting African interests or contexts

AU instruments tend to emulate best practices from other regimes, but this emulation can have unintended consequences. For instance, the Malabo Convention was inspired by the EU's Data Protection Directive (now replaced by the General Data Protection Regulation (GDPR)) (Ayalew 2022) while the AfCFTA DTP draws on the US-Mexico-Canada Agreement (USMCA) (Gathii 2024; Whittle 2024). Some interviewees raised concerns that adopting frameworks developed in different contexts may not be suitable for, or overlook, African realities. Other studies have also alluded to this risk (Beyleveld and Sucker 2024; Saturday and Nyamwire 2023).

With Africa's data and AI economy dominated by foreign companies, there is concern that certain provisions in the AfCFTA DTP may have been influenced by these companies to protect their own interests. For instance, the AfCFTA DTP grants near absolute secrecy rights to (usually foreign) software firms, potentially hindering technology and skills transfer by inadvertently limiting access by African developers and governments to essential software and algorithms

[10] The Eastern Africa Forest Observatory (OFESA) is a regional initiative to monitor and manage forest resources which involves CBDFs among member states of OFESA. See https://ofesa.rcmrd.org/en/.

(CIPIT 2024). The USMCA-inspired approach of unfettered CBDFs poses potential risks for citizens' privacy, shaping the future of the internet. Indeed, this approach is being reconsidered in the US due to the risk of power abuses by big tech firms and national security concerns (Gathii 2024, Kilic 2024). Yet, these provisions are included in the AfCFTA DTP.

Critics also highlight external influence in many of these policy processes. Some interviewees believe that the favourable terms for big tech firms in the AfCFTA DTP result from the USAID's support to the AfCFTA Secretariat through the 2020 Digital Transformation with Africa Initiative, while others argue that the process was led by African experts ensuring African agency. The DPF, developed with the support of AU institutions, Team Europe and Research ICT Africa, also exemplifies this issue. Germany, through GIZ, supported the development of the DPF, while the European Union and several Member States are also supporting its implementation.[11] While GIZ emphasises AU ownership, some interviewees have expressed doubts about the level of genuine involvement that AU Member States and other stakeholders have.

Finally, these instruments aim to facilitate CBDFs *within* Africa, but much of its digital infrastructure and services are imported from *outside* the continent. As such, policies governing extra-African transactions are more relevant for 'digitally-driven development' in Africa (Stuart 2024a). These differ across countries and lack uniform governance.[12]

3. From continental vision to national implementation

There are also challenges at the level of national implementation (CSEA 2021). Implementation may involve adoption into law (e.g. Malabo Convention, DTP) or adoption of national strategies following continental guidelines (e.g. DPF, Continental AI Strategy), compliance requiring monitoring, and enforcement against breaches. Yet, national policies often prioritise national interests that may contradict or overshadow the continental vision. Implementation depends on the socio-political capabilities at the national level to coordinate across state agencies, which vary widely across countries, and are subject to administrative delays and contestation (Jaïdi et al. 2024). Without the necessary foundational capabilities (e.g. institutional capabilities and governance structures, regulatory frameworks, administrative capacity in terms of trained personnel, financial resources etc.) to support the implementation of these instruments there is a widening gap between policy and practice. This attempt to do "too much, too soon and with too little" is described by some experts as premature load bearing (Pritchett 2019).

[11] GIZ is leading the implementation of the programme. It has developed an implementation framework, hosted the first Data Innovation Forum in November 2023, and is rolling out a framework at the national level.

[12] The AfCFTA is a Free Trade Agreement and not a Custom Union which means that Member States cannot govern extra-African digital trade as a collective, unless through regional economic communities that cover this area specifically.

3.1. National approaches to data flows

Varying ideologies, socioeconomic contexts, security concerns and economic priorities shape data-sharing policies, resulting in differences across countries. This section examines the factors that shape the national policies of three African countries, namely Mozambique, Nigeria, and Senegal. This is important to understand in order to draw policy recommendations to bridge the gap between continental and national processes.

Table 3: Overview of national policies in selected country studies

Nigeria	2011 Central Bank of Nigeria (CBN) guidelines for the banking sector[13] 2013 National Information Technology Development Agency (NITDA) Guidelines for Nigerian Content Development in ICT (NITDA ICT Guidelines),[14] amended in 2019 2019 National Cloud Computing Policy 2019 Nigeria Data Protection Regulation (NDPR) under NITDA, followed by Nigerian Data Protection Act (NDPA) operationalised in 2023. The Nigeria Data Protection Commission (NDPC) monitors and enforces the NDPA with whitelist to facilitate CBDFs	Not signed or ratified the Malabo Convention Signatory of the ECOWAS Supplementary Act on Personal Data Considered the AU DPF when developing its draft National Data Strategy NDPC a Member of the African Network of Personal Data Protection Authorities (NADPA/RAPDP)	Evolving approach - previous focus on local data processing (e.g. NITDA ICT Guidelines, or CBN Guidelines). Without a clear vision like the later National Data Strategy, or NDPA to protect personal data (Nigeria deemed a latecomer compared to other countries), effectiveness was assumed by focusing on promoting local innovation through strict measures on data flows. Now emphasis on governing data within Nigeria and of data transfer. National Digital Economy Policy and Strategy, and draft National Data Strategy balance data privacy and CBDFs. The NDPA permits personal data transfer; along with National Cloud Computing Policy challenges earlier policy positions on local data storage by allowing transfers outside Nigeria if stipulated provisions are met.[15]

[13] Guideline 4.4.8 mandates all domestic transactions to be processed using the services of a local switch and not routed outside the country Central Bank of Nigeria Guidelines on Point of Sale Card Acceptance Services 2011).

[14] Guideline 12.1(4) and 14.2(3) mandates ICT companies to host customer and subscriber data within Nigeria and all government data to be hosted locally (NITDA Guidelines for Nigerian Content Development in ICT).

[15] Data transfer is permitted if the recipient of the data is subjected to law, binding corporate rules, contractual clauses, code of conduct, certification mechanism that affords an adequate level of protection with respect to personal data. CBDFs are also permitted under the NDPA if the data subject provides their consent, transfer is necessary for the performance of a contract, for public interest reasons, for the protection of vital interests of data subjects or other persons etc.

	including countries that ratified the Malabo Convention and others (Nigerian Implementation Framework Annex C) 2020 National Digital Economy Policy and Strategy Draft National Data Strategy		2020 Significant Economic Presence Order under Companies Income Tax sets out conditions under which non-resident companies are liable to taxes without insisting on local data storage. [16] Motivation for building local data centers evolved from a focus on data localisation, equated with data sovereignty, to building national capabilities to position Nigeria as a hub for African data market, serving the regional/continental cloud-computing needs (Africa Data Center Map; Smart Africa, du Couëdic 2014). Extensive stakeholder workshops to shape its AI and data strategies
Mozambique	Personal data protection law currently being drafted 2021 National Cybersecurity Policy and Strategy following the ratification of the Malabo Convention Sectoral laws e.g. strict conditions by Central Bank covering the banking sector	Signed and ratified the Malabo Convention The SADC Model Law on Data Protection is being considered in drafting the national law on data protection	Emphasis on cybersecurity, covering sectors such as banking and conservation, with a view to avoid EU blacklist (Chevalier and Sciales 2023). Strong support for Malabo Convention as an opportunity to 'control the rules of the game' and achieve governance autonomy (Fidler 2024). Also joined the Council of Europe Convention on Cybercrime (Budapest Convention). View of data sovereignty as data localisation - development of national data centres in an effort to store data locally.

[16] The National Cloud Computing Policy mandates that Federal Public Institutions use cloud service providers that store data in jurisdictions with data protection levels equivalent to Nigeria's, with guidance from NITDA on acceptable data storage locations. Additionally, the policy enforces localisation for certain government data, requiring confidential, sensitive, and classified information to be stored on-premises or within Nigerian territory (Oloni 2024).

Senegal	2008 Data Protection Act, which also established the Personal Data Protection Commission (CDP) Senegal Digital Strategy 2025 (SN2025) 2023 draft new Data Protection Act 2023 National Data Strategy 2023 National AI Strategy	Ratified the Malabo Convention Signatory of the ECOWAS Supplementary Act National Data Strategy adopted in line with the AU DPF CDP a Member of the African Network of Personal Data Protection Authorities (NADPA/RAPDP) CDP a Member of the French-speaking Association of Personal Data Protection Authorities (AFAPDP) 2014	Requirement to localise data to control collection, storage, processing of Senegalese data in accordance with Senegalese law following directions of the former President. National Data Strategy seeks to harness data as a catalyst for inclusive socioeconomic development based on privacy, transparency, fairness and security (Houeto 2023). Also acceded to Convention 108 and its Additional Protocol, reinforcing commitment to data protection. Personal data protection is a key priority, with stringent requirements on transborder data flows. Ongoing discussions to amend and update the 2008 Data Protection Act as it didn't consider data evolution induced by social networks and to align with other technological advancements.

3.2. How national data policy priorities are shaped

At the national level, policy development is influenced by various motivations such as public discourse, expert opinion, media influence, political and business interests among others. These not only interact and evolve over time, but also vary across countries resulting in different national vision and perspectives on data-sharing. Siloed discussions add another layer of complexity in harmonising these visions.

3.2.1. National vision shaped by economic and political interests

National data policies often prioritise economic and political interests. In all three countries, discussions primarily focus on national frameworks, with intra-continental CBDFs not being a current priority despite their recognised economic value.

In Nigeria, the policy priority is to foster local innovation and economic development. Certain sectors have restrictions on CBDFs in order to create more opportunities for local businesses, including requirements for data localisation.[17] However, experts criticise these measures for their weak economic logic given inadequate infrastructure and cybersecurity, which increase costs and diminish benefits (Adeleke 2021, Abdulrauf and Abe 2021).[18] Moreover, Nigeria's whitelist of countries considered safe for data-sharing, motivated by economic and political interests, includes countries like Bahrain and the US, which lack robust national data protection laws.

In some other cases, economic consideration is not the key factor guiding local data storage. Mozambique's National Centre for Biotechnology and Biological Sciences (CNBB) stores data locally, irrespective of the costs involved, to protect confidentiality and intellectual property. Nevertheless, the government is making efforts to increase the currently low utilisation (of around 50%) of its national data centre by way of mandate e.g. national decree,[19] and persuasion e.g. by the National e-Government Institute (INAGE), for public institutions to store their data in this public infrastructure. The National Agency for Geospatial Development (ADE) was set up at an impressive pace driven by the political interest in building state capabilities to assess the country's natural resource wealth, although the agency's focus is much broader than that. This shows that political and economic interests can align with the objective of CBDFs, and do not always capture this agenda.

On the other hand, despite ratifying the Malabo Convention, Mozambique is not included in Botswana's white list, which instead favours trade partners like South Africa and Kenya (Musoni 2022).

3.2.2. External influence and path dependence

Senegal provides yet another context. In 2021, the country inaugurated a national data centre with Chinese financing and equipment from Huawei. According to some analysts, this move demonstrated the attractiveness of the Chinese data governance model that "requires all servers to be located within a country's borders, providing the state with full access to the

[17] Previously, the protection of privacy rights, building of local ICT and banking sectors, tax benefits and protecting Nigeria's sovereignty were often cited as justifications for local processing, and local storage of data (Adeleke 2021; Beyleveld and Sucker 2022).

[18] According to Stuart (2024b) "a key characteristic of the internet and one of its most misunderstood is the fact that it is essentially borderless. The internet, even websites that are local to a country or city, do not necessarily 'exist' on that locality. In fact, they are more than likely to exist in multiple places and multiple countries, even if their web host is a local business. This means that any attempts to limit cross-border data flows, to localise data or to force the location of data centres will encounter important practical challenges and certainly lead to efficiency losses/cost increases".

[19] Regulation of the Electronic Government Framework.

information" (Olander 2021). However, there has been limited progress in repatriating and storing public sector data at the national facility despite the push by former President Macky Sall. Private and certified data centres are instead widely used.[20] The data centre reflects China's maturing relations with African countries, shifting from trade and loans to more politically-driven engagements, drawing inspiration in the sphere of governance which traditionally was the EU's niche (Karkare et al. 2020). At the same time, Senegal also worked closely with GIZ and the EU on its National Data Strategy,[21] emphasising personal data protection and data security, demonstrating that cooperation with China in one area does not preclude cooperation with Team Europe in another area.

Path dependence, where current outcomes are shaped by past events and decisions, also influences how policy frameworks and institutional setups look in a given country. Mozambique's data-sharing rules in the banking sector are influenced by Portuguese practices, reflecting its colonial past and current economic/trade relations. Collaboration around data, just as in many other policy areas, are more commonly sought in the Community of Lusophone Countries (CPLP) or its African sub-group (PALOP).[22] Similarly, Senegal's regulatory frameworks somewhat mirror the French system.

The US-China-EU geopolitical competition influences national policies indirectly. Strong trade ties with the EU incentivise the adoption of European data protection approaches (Fidler 2024). Nigeria accelerated its data protection law due to European loan stipulations (Musoni, Domingo, and Ogah, 2023). Mozambique's National Strategy for Cybersecurity, driven by the need to avoid EU blacklisting, aligns with the Malabo Convention and draws from Portuguese laws (Chevalier and Sciales 2023).

3.2.3. Siloed discussions and fragmented sectoral agreements

Most government Ministries, Departments, and Agencies (MDAs) do not use data for decision-making and operate independently with limited cooperation and communication due to a culture of secrecy and lack of trust. Accessing data from another public entity often involves lengthy, hierarchical procedures, delaying decision-making. Siloed discussions and fragmented approaches by institutions and regulators on intra-continental CBDFs risks missing critical cross-sectoral insights.[23] This is seen in the conflation of data sovereignty with data localisation recently explored by Soulé (2024).

Policymakers tend to treat the digital economy the same way as the (physical) goods economy which has an impact on CBDFs. Unlike traditional industrial resources like oil, data is inexhaustible and non-rivalrous, meaning its value grows with increased access and usage.

[20] https://uptimeinstitute.com/uptime-institute-awards/country/id/SN

[21] https://smartafrica.org/senegal-unveils-its-national-data-strategy/

[22] Mozambique's National Personal Data Protection Law, currently being discussed, draws from existing laws in other Lusophone countries including Portugal, even as it aligns with the Malabo Convention.

[23] Data is discussed in various thematic areas like digital trade, cybersecurity, and AI within separate expert committees, often with limited inter-committee communication.

However, policies, particularly the interpretation of digital sovereignty, tend to prioritise resource monopolisation over sharing.

In practice, and despite the above challenges, data-sharing takes place in all three countries. In many cases, it is governed by sectoral, multilateral or firm-level agreements. These agreements overcome the shortcomings in national frameworks by defining sector rules for actors across borders. For instance, data-sharing in the banking sector is governed by mandatory rules and regulations (of the central bank), whereas meteorology or trade data are governed by multilateral agreements, and in yet other sectors such as conservation data-sharing is guided by international (voluntary) best practices.

3.3. Implementation challenges

A recurring criticism of policy frameworks in Africa is that while there are many good policies, implementation is lacking, with common challenges observed across countries. Ineffective national coordination leads to competing mandates and perverse incentives which distract from implementation. Without clear data-sharing mechanisms and frameworks, an important bridge between policy and practice is missing, and enforcement remains a challenge.

3.3.1. Poor national coordination creates competing mandates and perverse incentives

Given the cross-cutting nature of data-sharing, several entities are involved in making it work. This can create friction. In Mozambique, policies related to information technology fall under the mandate of the Ministry of Science and Higher Education, while the Ministry of Transport and Communications oversees telecommunications. This overlap creates confusion between the telecommunications regulator (INCM) and the ITC regulator (INTIC), with a lack of clarity on who does what exactly. A similar situation is observed in Nigeria as well. The National Data Protection Act overseen by the Nigeria Data Protection Commission did not repeal the National Data Protection Regulation under National Information Technology Development Agency (see table 3 above), leading to overlapping mandates, even though both agencies fall under the Federal Ministry of Communication, Innovation, and Digital Economy.

In some cases, policy decisions can also create perverse incentives that negatively impact data-sharing. For instance, entities like Nigeria's National Identity Management Commission (NIMC) and Senegal's National Agency of Statistics and Demography (ANSD) charge access fees for data due to limited central government funding, discouraging stakeholders from accessing data and undermining their initial data-sharing objectives.

3.3.2. Poor data governance and unclear mechanisms

Effective policy implementation requires clear frameworks and mechanisms, which are often lacking. Most countries have not adopted robust data governance frameworks to ensure effective data use and CBDFs. Moreover, limited capacity to collect quality data is a widespread issue. Government data is often outdated or unreliable.[24] For instance, Nigeria's statistical information is still based on the 2006 census which was beset with political sensitivities (Akinyemi 2020; Eromosele 2023; Ndemo et al. 2023). Weak rule of law and enforcement further discourage citizens from sharing data due to fears of misuse (Abebe et al. 2021).

Lack of interoperability in vital statistics such as income taxes, financial transactions or health data also limits public service delivery (Ndemo et al. 2023). This is observed in Mozambique where numerous systems are put in place through development partner-partner supported initiatives without sufficient consideration to interoperability. This can result in delays, administrative burdens and increased costs in the case of customs and trade agencies (White Paper on AI). The situation is further compounded in many countries by the fact that there are no clear national data access and data sharing frameworks (Ndemo et al. 2023). Currently, only 12 African countries have developed national data and / or AI strategies. Unclear frameworks also hinder data sharing in non-politically sensitive but strategically important areas, such as scientific and geospatial data, leading to unnecessary expenses for acquiring existing data while it already exists locally or could be reused (Waruru 2023).

3.3.3. Limited enforcement

Implementation of continental frameworks is incomplete without enforcement though this is often hindered by the absence of independent regulators. In practice, enforcement powers of data regulators are tested especially when influential actors, including other government agencies or big tech companies are involved.

The Malabo Convention leaves it to individual Member States to establish data protection authorities and laws that these authorities would enforce without providing sufficient mechanisms for coordination and harmonisation across countries. Many countries are yet to domesticate the Convention into national law, or establish operational national authorities (King'ori 2024).

Both Nigeria and Senegal have established their regulators, the NDPC and CDP respectively but enforcement is inconsistent. The NDPC was recently criticised for leniency in handling the data breach at NIMC, given it is 'a sister' agency (interviewee). Nigeria's whitelist was recently invalidated by the High Court due to inadequate personal data protection in listed countries like Mozambique, Comoros, and Guinea Bissau. Despite being signatories of the Malabo Convention, these countries lack data protection laws or authorities, contradicting Nigeria's policy aims of ensuring adequate protection for its citizens' data.[25]

[24] Economic activity is inadequately measured due to conflict and political unrest in countries the DRC, Eritrea and South Sudan, or due to the lack of a clear methodology and understanding of the informal sector (Koch 2019). Only about three out of four countries in Africa update their budget data, national laws and procurement information in a timely manner while only half publish updated elections records, or keep their company registers up-to-date (Lämmerhirt 2019).

[25] The Incorporated Trustees of Ikigai Innovation Institute v. National Information Technology Development Agency FHC/ABJ /CS/1246/2022.

In Mozambique law enforcement has generally proven difficult due to the lack of state capacity – technical, human, and financial. On the other hand, in Senegal, the stringent application of the law by the CDP makes it difficult to share even non-personal data, which is subject to authorisation by the CDP. Previous studies suggest that stringent cybersecurity requirements significantly increase compliance costs, especially for small and medium firms (e.g. Ryle et al. 2021 cited in Lemma 2024) which constitute a significant part of African economies.

4. Key takeaways on discrepancies between continental and national perspectives on data flows

National approaches to CBDFs balance different objectives like free data movement, data localisation for sovereignty, personal data protection, cybersecurity with more practical considerations such as economic and political interests, external influence, and trust. As countries prioritise these objectives differently (e.g. Nigeria emphasises the role for economic growth, Senegal highlights personal data protection, Mozambique is focusing on cybersecurity), achieving a cohesive data economy in Africa will require avoiding fragmentation. But the relation of national policies with the regional/continental ones is a function of not just how these countries perceive continental frameworks, but also how relation between different countries, in other words regional integration, empowers continental frameworks to guide national processes.

4.1.1. Competing national interests and continental commitments

A key lesson from regional integration studies is that national interests often overshadow continental commitments (Byiers et al. 2021). This is evident in CBDFs, where national frameworks take precedence over intra-continental data flows (see 3.2.1). Governments prioritise immediate national needs, driven by political leaders seeking legitimacy and influenced by business lobbying (Vanheukelom et al. 2016). For example, Nigeria's whitelist includes trade partners with less-protective data regimes, reflecting economic interests over data protection (see 3.2.1.). The lack of enforcement of continental rules also means that loopholes are often used to pursue national interests. This reflects a more fundamental dilemma at the national level - "why implement [continental] agreements when the sense of ownership is limited and priorities lie elsewhere?" - reflecting 'a crisis of implementation' and thereby hindering collective action (Miyandazi 2020).

Intra-continental CBDFs are also hindered by other factors such as political tensions within (e.g. coups or insurgencies) as well as between countries (e.g. commercial or other forms of competition or rivalry), colonial legacies which create path dependence in terms of language and administrative processes (see 3.2.2.) or varying development trajectory and institutional robustness of systems (Brand et al. 2022). To illustrate, a programme to facilitate data-sharing for a regional ID in West Africa was hindered as data-sharing, especially on cross-border movement of people, was considered sensitive due to national security concerns arising from political instability in the region (interview).[26]

4.1.2. External influence

Additionally, most data-sharing and trade of African countries is with partners outside the continent (Stuart 2024a) creating incentives to align with (stringent) external requirements. Countries with robust cybersecurity mechanisms, in line with international frameworks such as the Budapest Convention, may hesitate to share data with other African states lacking similar policies. An important implication from this is that while some countries have put in place robust mechanisms to enable CBDFs with external partners, these same mechanisms may make CBDFs within the continent more difficult. Many countries have modelled their laws on the EU's GDPR and received EU training and support (e.g. Nigeria, Kenya). This may lead these countries to prioritise alignment with the EU over regional neighbours that have not adopted regulation modelled on GDPR, thereby resulting in a lack of regional harmonisation (Fidler 2024).

4.1.3. Long continental negotiations leading to lack of alignment

Negotiations at the continental level usually take place alongside policy discussions and developments at the national level. The longer timeframes to conclude continental discussions and the fact that the continental position is inherently a compromise between differing positions of member states partly explain the gaps in continental and national frameworks around CBDFs. For instance, the Malabo Convention only came into force 9 years after it was adopted. Not only are there discussions of updating provisions of the Convention given that the landscape in terms of digital advancements has significantly evolved during this time (Ifeanyi-Ajufo 2023; Carnegie 2023), but at least 34 countries already had data protection laws in place, while 22 had data protection authorities, before the Malabo Convention was adopted.[27] Countries like South Africa had less urgency to ratify the Malabo Convention as it had already passed its law on data protection, the Protection of Personal Information Act. This creates discrepancies between national and continental frameworks.

4.1.4. Ineffective coordination

Poor communication between continental and national entities exacerbates the gap. The official formal consultation procedure for continental policies starts with an official memo that first goes to the Ministry of Foreign Affairs before being sent to the responsible Ministry. Delays in passing memos to the responsible agency, further compounded by competing mandates at the national level (see 3.3.1.), leads to misalignment especially when discussions are siloed (see 3.2.3.).

[26] The West Africa Unique Identification for Regional Integration and Inclusion (WURI) programme in ECOWAS was funded by the World Bank to facilitate easier data sharing, data exchange and cross border digital payments through the development of a regional ID.

[27] See https://dataprotection.africa/which-african-countries-have-a-data-protection-law/

In other cases, national processes could be inadvertently undermined due to these bureaucratic delays even if data is being shared. For instance, Mozambique's National Institute of Meteorology (INAM) produces weather forecasts to be distributed in the country, but because of delays in receiving parallel continental forecasts, there are two (sometimes unmatching) sets.

4.1.5. Lack of serious repercussions for AU Member States

Typically, there are no serious consequences when AU Member States deviate from the continental objective or vision and Member States therefore view continental bodies as toothless. The AU and its organs do not have the power to enforce continental agreements unless they are ratified by Member States. Even when they are, they do not impose punitive measures on countries that do not comply with agreed provisions e.g. Malabo Convention. As a result, the focus is towards political declarations rather than effective implementation.

4.1.6. Data deficiencies and low demand for CBDFs

Even as frameworks are put in place to facilitate CBDFs, it is important to consider the input which is data. Many African governments operate with outdated, incomplete, or unreliable data (Chege and Wanjohi 2023, Lämmerhirt 2019; Glassman and Ezeh 2014) leading to ineffective policy-making. Limited data sharing with the wider public is a missed opportunity for data-based analysis and policy advice, for instance by the civil society. As a result, the demand for data-sharing, including intra-continental CBDFs ultimately remains low (Lämmerhirt 2019). Similarly, there is a lack of understanding of concepts such as data value creation, data justice and data stewardship.

5. Strategic steps to enhance CBDFs in Africa

Ensuring seamless and secure data flows across Africa requires concerted efforts at both continental and national levels, with policy alignment and harmonisation to support the vision of the AfCFTA and the DSM. This can be achieved with a bottom-up approach that ensures buy-in from Member States. This paper outlines strategic steps, both in the short term and medium-to-long term, that can be taken to enhance CBDFs in Africa, focusing on recommendations for the AU and its Member States. Some of the proposed policy recommendations are based on the DPF and aim to reinforce or highlight key principles for the AU and its Member States.

5.1. Policy recommendations for the AU

5.1.1. Establish a Data Categorisation and Data Sharing Framework for CBDFs

A one size fits all approach to data sharing is limiting given the nature of data types. Personal data (health, children's or financial data) needs strict guardrails, while non-personal data (climate or agricultural data) may not. The AU and its Member States should work together to develop corresponding data sharing mechanisms that respect these distinctions and needs.

This might involve engaging to develop sector specific mechanisms on CBDFs. For instance, within the agricultural sector, different data types may be mapped out and categorised in terms of which non-personal data may be transferred outside the country and under what conditions.

5.1.2. Strengthen implementation and enforcement capacity

To address the challenge of lacking implementation and enforcement, the AU should consider establishing a Continental Data Protection Body (CDPB). Similar to the European Union Data Protection Board, the CDPB would oversee the implementation of the Malabo Convention and enforce data protection across the continent (Abdulrauf 2021). This body would provide guidance to Member States on interpreting CBDF provisions in the different continental instruments like the Malabo Convention, the AfCFTA DTP and the DPF, consult with national Data Protection Authorities, and enhance regulatory consistency. As the AU revises the Malabo Convention, it should include provisions for the establishment of the CDPB. The AU can also seek guidance from the African Network of Data Protection Regulators (see 5.2.6.) on issues such as the composition, establishment, functions, mandate and jurisdiction of the CDPB.

5.1.3. Establish a Task Force or Working Group on CBDF

Given Africa's rapid digital transformation, dedicated continental task forces or working groups, similar to the OECD's approach on data free flow with trust, focused on different aspects of CBDFs are essential. These include mechanisms on data categorisation and transfer standards. Such engagement ensures expertise continuity and consistency in policy making amid changes in governments or technical teams among Member States.

5.1.4. Facilitate peer to peer learning among Member States

Peer to peer learning and sharing of success stories can motivate other countries to align with the continental vision. For instance, a study tour to Rwanda in December 2023 supported Senegal's national Data and AI strategy implementation. This tour was led by Senegal's Ministry of Communication, Telecommunications and Digital, supported by Team Europe, GIZ and the AU-EU D4D Hub. Similarly, Benin's Ministry of Digitalisation attended a validation workshop in Accra to learn from Ghana's National Data Strategy and inclusive development process.

5.2. Policy recommendations for AU Member States

5.2.1. Governance

Harmonise policy perspectives: Member States should align national policies with the AU's continental vision on CBDFs. This entails developing or updating laws on data protection, e-commerce, cybersecurity, and artificial intelligence to align with continental policies. Countries like Mozambique, without digital policies, should develop comprehensive frameworks, while others with existing policies, like Nigeria and Senegal, should revise and update them to align with the continental vision. To understand the impact of CBDFs, sector-specific policies need to be re-evaluated to identify priorities, areas of alignment or lack thereof.

Wider digital policy alignment: Member States should explore how internationally recognised best practice on data protection such as the Convention 108+ and GDPR can be adapted to their local contexts and develop domestic policies that also align with broader data sharing frameworks. Digital policy alignment should extend to other policy areas such as competition, trade, intellectual property and taxation. This would require strong cross-sector coordination and multi-stakeholder engagement to avoid siloed approaches. Further, collaboration between data protection authorities and competition regulators could help address challenges of cross border data flows and develop consistent regulatory practices.

Implement measures to address data deficiencies: African countries need to improve data governance practices to ensure data accessibility, promote data integration and interoperability. By developing internal data strategies and governance frameworks, government institutions can generate reliable, up-to-date data while maximising effective data utilisation and compliance with relevant regulations and policies (Saturday and Nyamwire 2023). Non-traditional data sources are increasingly being used to resolve national challenges. During Covid-19, Nigeria used satellite and geospatial big data to generate poverty estimates in urban areas and identify eligible beneficiaries of Covid-19 relief funds and social security with collaborative efforts between the National Social Safety Nets Coordinating office, an AI developer and telecommunications companies (GPAI 2021). There is a need to include new forms of data through remote sensing, satellite imaging, sensors, social media, communication devices, etc. into policy (Ndemo et al. 2023). South Africa is a leading example in this regard.[28] Focus should be on improving data quality as well as increasing the demand for data use by incorporating principles of digital equality and data justice, in line with state capabilities.

5.2.2. Enabling factors

Build / use data infrastructure on the continent: Developing local data infrastructure is critical for economic growth and digital sovereignty (AUDA NEPAD White Paper on AI; Musoni and Snail 2023).[29] African countries should invest in data centres and improve energy efficiency, cybersecurity measures, and digital literacy to support data infrastructure development. Efforts should focus on emerging hubs in South Africa, Nigeria, Ghana, Egypt, Algeria, and Morocco (AUDA NEPAD White Paper on AI), and include accompanying measures to address structural impediments like providing reliable power supply, improving energy efficiency, increasing internet connectivity, improving digital literacy skills, and ensuring strong cybersecurity. The Smart Africa Alliance recommends promoting ease of business, facilitating land acquisition for data centres, mobilisation of funds and enacting appropriate data governance and data protection laws (Smart Africa 2022).

[28] South Africa's NSO strategic plan for 2020/21–2024/25 emphasises integrating data from different sources, seeking collaborations with other data producers in the analysis of existing data, and exploring the use of alternative sources of data (Statistics South Africa 2020).

[29] Africa currently has the least number of data centres globally. Within the African continent, some countries like South Africa have a significant data centre market, about two thirds of the continent's total capacity while West Africa contributes less than 10% of the total data centre capacity (Augustine 2022).

Strengthen cybersecurity: Enhancing cybersecurity capabilities is crucial for protecting Africa's digital economy from threats. While risks of privacy violations, misuse and exploitation increase, only a fifth of African countries meet standard requirements for combating cybercrime (CSEA 2021), due to lack of expertise, resources, and technological dependence (Diorio-Toth 2023). Member States should adopt comprehensive cybersecurity strategies and establish national cybercrime laws in line with the Guideline for Model Cybersecurity Law and adopt the Lome Declaration on fighting cybercrime. They should also develop cybersecurity incident response teams (CSIRTs) and align efforts with the ongoing UN process to develop a global treaty on cybercrime. Collaboration with countries with mature cybersecurity frameworks like Mauritius, Morocco, Egypt and Ghana can provide a guide to others (Ifeanyi-Ajufo n.d.).

5.2.3. Capacity and Skills

Conduct stakeholder awareness training: Promoting a data culture requires continuous advocacy and capacity building among stakeholders to raise awareness on how data can be leveraged as the 'new oil' (Boateng 2022), existing opportunities and benefits from CBDFs. Governments should provide training on data analytics, governance, and the digital economy for small businesses, regulators, and youth. Collaboration with civil society groups can enhance awareness of data rights and the benefits of cross-border data sharing.[30]

Build institutional capacity: Establishing independent Data Protection Authorities is essential for upholding robust data protection laws and safeguarding data privacy. Consulting the national authority is crucial when developing a whitelist of countries for data sharing, creating cross border data transfer mechanisms or formulating data policies and strategies.

These bodies need to be adequately resourced and empowered to monitor compliance and address data protection issues effectively - Nigeria, Senegal, South Africa, Kenya, Ghana, Zimbabwe, Mauritius have established their data protection agencies, but they are often under-resourced and lack financial independence. This affects their ability to enforce rules and address sensitive data protection issues effectively (Boateng 2022, ALT Advisory, King'ori and Dorwart 2022).

Joining the Network of African Data Protection Authorities can facilitate regional cooperation on data protection and CBDFs as highlighted at a recent AGM. Bilateral agreements, like those between South Africa and eSwatini enhance regulatory cooperation, leading to greater benefits from multilateral agreements (South Africa Information Regulator and eSwatini Communications Commission).

[30] Paradigm Initiative. KictaNET, Pollicy, MISA, etc.
African Data Leadership Initiative was launched by Smart Africa, Economic Commission for Africa and Digital Impact Alliance https://dial.global/work/adli/. Open Knowledge International https://okfn.org/en/. Open Data Institute https://theodi.org/. World Wide Web Foundation. Open Data Day https://opendataday.org/.

5.2.4. Data Usage

Support open data initiatives: Open data initiatives can enhance transparency, public service delivery, and innovation (The African Open Data Report 2017; World Bank, CSEA 2021). Governments should create enabling environments for open data platforms (Data 4 Development) and ensure that data is up to date (GPAI November 2023 Report) while experimenting with data in sectors like health, agriculture, and climate. For instance, in Senegal, Orange-Sonatel leveraged customer data, including mobile phone records and social media data, to gain insights into climate-induced migration (Data Pop Alliance). The John Hopkins Covid-19 dashboard facilitated the sharing of critical health information during COVID-19. Initiatives like Kenya's Open Data Initiative, South Africa's Open Data Portal, and Uganda National Statistical Office Open Data Portal exemplify efforts to promote transparent data access, yet they often struggle with irregular updates. Non-governmental platforms such as CGIAR and Masakhane which focus respectively on agriculture and African language preservation also show the value of open data.

Experimenting with innovative structures: African countries can also explore innovative approaches like developing data trusts, which enable communities to collectively utilise data for mutual benefit and assert collective power (Olorunju and Adams 2022). As seen in Kenya, these structures empowered rural communities to access vital information on available water sources, social amenities, perceptions of water scarcity and farmers-herders' relations through community data stewards. The data generated was subsequently used to identify non-functional water infrastructure and attract more investment in borehole repairs (Data to Policy). However, it is crucial to find ways to share proprietary data for social and public purposes without compromising commercial viability or intellectual property interests (Tshuma 2024). Further research into new data sharing models, including data trusts and stewardship, is essential to assess associated risks and opportunities (GPAI 2023). Collaboration with development partners such as the World Bank, African Development Bank, UNECA, and successful African counterparts leading open data initiatives can enhance knowledge sharing and accelerate the adoption of best practices in open data governance across the continent.

6. What role can the EU play in supporting cross border data flows in Africa?

The EU is a major trade partner for African countries and has significant investments in Africa's digital economy, encompassing both hard and soft infrastructure, including data systems. To enhance this partnership and support CBDFs in Africa, the EU can leverage the digital pillar of Global Gateway via its Team Europe Initiatives (TEIs) and share insights from its European data-sharing efforts.

Supporting Africa's data-sharing initiatives aligns with the EU's goal of leading international cooperation on data, shaping global standards, and fostering economic and technological development in compliance with EU law (EC 2020). Indeed, the EU is already supporting the AU and its member states in developing data policies through the Data Governance in Africa initiative (D4D Hub n.d.). This support aims to create an African data economy that benefits its citizens and businesses (EC 2020).

6.1. Background: The EU Data Strategy

The EU Data Strategy aims to facilitate free data flows within the EU based on harmonised protection of personal data and common standards for all data, progressing toward a Digital Single Market which is still a work in progress. It proposes measures to boost the use and demand for data and data-enabled services across the Single Market (EC 2020).

The Data Strategy has been followed by the Data Governance Act (DGA), the Data Act and the Free flow of non-personal data regulation. Together with the GDPR, these provide the legal framework for the development of the evolving EU data market.

- DGA establishes mechanisms for trustworthy data sharing and data intermediaries, for a secure and transparent environment for cross-border and cross-sectoral data flows (EU 2022).
- Data Act promotes innovation and competition, by enabling access to data generated by devices and services for businesses, consumers, and public entities (EU 2023).
- Free flow of non-personal data regulation (EU 2018).

For a unified data market, the EU is also developing data spaces - secure environments for data sharing across sectors like health, finance, energy, and agriculture. These spaces ensure high levels of privacy, security, data availability, interoperability, and innovation. They focus on a number of different sectors, including health, finance, energy, and agriculture (EC 2024).

Globally, the EU Data Strategy represents a comprehensive approach to CBDFs. The Japanese G20 initiative "Data Free Flow with Trust" shares similar goals, though at a more international level, but lacks the robust legal frameworks and implementation structures of the EU, relying instead on policy coordination among G7 members (Digital Agency Japan n.d.).

6.2. The Action on Data Governance in SSA

The EU's "Action on Data Governance in Sub-Saharan Africa" aims to support the AU in developing a data market comparable to the EU's, potentially enabling free data flow between the regions. This initiative focuses on governance (at both continental and national level), infrastructure (notably data centres), and data use cases, with a budget of over €50 million from the EU (€30m), Germany's BMZ (€20m), and the French Ministry for Europe and Foreign Affairs (just under €0.5m), for January 2023 - July 2026.

The overall objective is to foster a development-oriented, human-centric data economy in Africa, aligned with the AU DPF. This involves strengthening policies and regulations for personal and non-personal data, leveraging data to inform sector-specific regulations, and developing bankable investment proposals for secure, sustainable data infrastructure through the Digital Investment Facility for European financiers.

The Action builds on a BMZ-funded project, where GIZ's Datacipation project supported the development of the DPF. GIZ continues to offer technical assistance to the AU and its member states in developing policies and regulations. GIZ also supports the AU in delivering technical assistance to member states through its network of Digital Transformation Centres across Africa. For instance, GIZ helped Senegal's Ministry for ICT, alongside Smart Africa and Data Pop Alliance, to develop Senegal's national data strategy, while Expertise France and D4D Hub supported the country's AI strategy. Similar support is provided to Ghana, while other states like Zambia or Benin have also applied for such assistance.

Other Team Europe and member state programs complement this, Action. GIZ's FAIR Forward initiative, which focuses on AI, is working with South Africa's Department of Forestry, Fisheries, and Environment to use data for climate action and support the country's Just Transition. Similarly, BMZ's Data4Policy is identifying data gaps in policy making and developing training for political leaders. The forthcoming Team Europe Initiative, Safe Digital Boost with Africa (SDBA), will support African regions in e-governance, e-commerce, and cybersecurity, likely aligning with the Action on Data Governance.

6.3. Recommendations for the EU

The EU's governance model is a key strength, successfully promoting a strong regulatory approach to digital governance through the 'Brussels Effect'. Many African states have adopted European regulations, such as the GDPR, for their data protection laws rather than developing their own approaches. However, it is crucial for the EU and its member states to recognise the unique functioning of African institutions and support their digital development.

Under the digital pillar of the Global Gateway, Team Europe has committed to increasing investments in digital connectivity, including data centres. Fulfilling this promise will be essential to show that the EU can offer much needed infrastructure alongside the support it provides on digital governance and regulatory environment. The EU's experience in developing data spaces serves as a valuable example for regions aiming to establish their CBDFs.

6.3.1. Governance

Team Europe is already supporting the AU DPF and building links with the AfCFTA DTP. Continued efforts should focus on better coordination between African continental actors to facilitate policy coherence on CBDFs. This includes facilitating information exchange among the AU, AfCFTA Secretariat, Smart Africa, RECs, and member states. Supporting events like the Data Governance & Innovation Forum for Africa can play a crucial role.

At the member state level, Team Europe should adopt a **holistic approach to implementation** by supporting inclusive processes that align with continental strategies, build on local ecosystems, and address local priorities, challenges, and opportunities. Ensuring **local**

ownership through a multi-stakeholder approach is essential, as demonstrated by the EU's own digital regulations developed through consultations with private sector, civil society, and citizen groups. There is real potential for the EU-AU partnership to support human-centric and inclusive digital policymaking processes (Abah et al. 2022).

While sharing experiences can be vital to peer-learning, the EU's model might not be directly applicable to other regions due to differing capacities and interests, and it is **important to take cultural and legal differences into account**. Other countries may advocate for a more collective approach to data protection, and in the case of the AU DPF for a stronger focus on the concept of data justice, which aims to prevent further discrimination and injustice through datafication.

Capacity building can strengthen local authorities' abilities to implement regulations and policies, ensuring sustainable governance at both continental and national levels.

6.3.2. Infrastructure

Under the Global Gateway, Team Europe already aims to scale up financing for Africa's data infrastructure to address significant inequalities, with the Digital Investment Facility developing bankable projects for European financial institutions. This effort requires a deep understanding of the local ecosystems and a bottom-up approach to coalition building (Bilal, Teevan and Tilmes 2024).

Investments in data infrastructure need to be **complemented by measures ensuring its utility to the local economy**. This includes addressing affordability and security issues through regulatory interventions, cybersecurity measures, and capacity building. Team Europe should **increase support for African governments to adopt safe and secure data-sharing infrastructure**. Developing a meaningful data market in Africa requires investments in making government data usable and shareable, as governments remain the most significant data producers. Investments should facilitate secure sharing of citizens' data across government departments and beyond.

6.3.3. Use cases

Under the data governance action, Team Europe supports developing use cases in Africa and aims to scale local initiatives. Key actions include

- **Experience Sharing** of implementing data spaces within the EU, which can serve as a model for developing CBDFs in other regions and advancing international initiatives like Data Free Flow with Trust.
- **Targeted Funding** for specific projects, such as digitising National Statistical Offices to produce accurate, updated, and reliable data and funding data value creation use cases, open data initiatives, and the establishment and operation of Data Protection Authorities and AI offices in African countries.

References

Abah, J., Baptista, K., MacKenzie, C., Varghese, A. 2022. *Putting People at the Centre of Digital Policy. Mechanisms for Citizen Engagement in Nigeria*. Chapter in Daniels, C., Erforth, B., & Teevan, C. (Eds.). Africa–Europe Cooperation and Digital Transformation (1st ed.). Routledge. https://doi.org/10.4324/9781003274322.

Abdulrauf, L. 2021. *Giving "teeth" to the African Union towards advancing compliance with data privacy norms.* Article, Department of Public Law, University of Ilorin, Nigeria and Institute for International and Comparative Law in Africa (ICLA), Faculty of Law, University of Pretoria, South Africa.

Abdulrauf, L. 2024. *African Approach(es) to Data Protection Law*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), African Data Protection Laws: Regulation, Policy, and Practice (pp. 31-54). Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909-005*.

Abdulrauf, L. and Abe, O. 2021. *The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations*. Johannesburg: Mandela Institute.

Abebe, R., Kingsley, S., Aruleba, K., Obaido, G., Sadagopan, S., Birhane, A., Remy, S. L. 2021. *Narratives and Counternarratives on Data Sharing in Africa*. FAccT '21, March 3–10, Virtual Event, Canada.

Adeleke, F. 2021. *Exploring Policy Trade-Offs for Data Localisation In South Africa, Kenya And Nigeria.* Johannesburg: Mandela Institute.

Akinyemi, A. 2020. *Nigeria's census has always been tricky: why this must change*. The Conversation

Arnold, S. 2024. *Africa needs China for its digital development – but at what price?* Article, The Conversation.

Atuguba Akongburo, R., Boshe, P., Dei-Tutu, S. and Hennemann, M. 2024. *African Data Protection Laws: Regulation, Policy, and Practice*. Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909*.

Augustine, A. 2022. *The Next Wave: A data centre roadmap for Africa*, Article, Techcabal.

Ayalew, Y. E. 2022. *The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* Blog of the European Journal of International Law, EJIL Talk.

Beyleveld, A. 2021. *Data Localisation In Kenya, Nigeria And South Africa: Regulatory Frameworks, Economic Implications And Foreign Direct Investment*. Policy Brief 07, Johannesburg: Mandela Institute.

Beyleveld, A. and Sucker, F. 2022. *Cross-Border Data Flows in Africa: Policy Considerations for the AFCFTA Protocol on Digital Trade. Report,* Johannesburg: Mandela Institute.

Beyleveld, A. and Sucker, F. 2024. *African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol's potential contribution*. *http://dx.doi.org/10.2139/ssrn.4741632*.

Bilal, S., Teevan, C. and Tilmes, K. 2024. *Financing inclusive digital transformation under the EU Global Gateway*. ECDPM Discussion Paper 370. Maastricht: ECDPM.

Boateng, R. 2022. *Data-Driven Enterprises in Africa: An Evaluation of Winners and Losers*. Abuja: CSEA AFRICA - CENTRE FOR THE STUDY OF THE ECONOMIES OF AFRICA.

Brand, D., Singh, J. A., McKay, A. G. N., Cengiz, N. and Moodley, K. 2022. *Data sharing governance in sub-Saharan Africa during public health emergencies*: *Gaps and guidance*. South African Journal of Science, 118(11-12), 1-6. *https://dx.doi.org/10.17159/sajs.2022/13892*.

Byiers, B., Apiko, P. and Karkare, P. 2021. *The AfCFTA and industrialisation*: *from policy to practice*. ECDPM Discussion Paper 314. Maastricht: ECDPM.

Carnegie. 2023. *Continental Cyber Security Policymaking*: *Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa*. Event, Washington, DC: Carnegie Endowment for International Peace.

Chege, Z. M. and Wanjohi, P. M. 2023. *A Value Chain Approach to Data Production, Use, and Governance for Sound Policymaking in Africa.* Chapter 3 in B. Ndemo et al. (eds.), Data Governance and Policy in Africa, Information Technology and Global Governance, *https://doi.org/10.1007/978-3-031-24498-8_3.*

Chevalier and Sciales. 2023. *EU updates AML/CFT blacklist and adds five countries*. Article, Luxembourg: Chevalier and Sciales.

CIPIT. 2024. *Commentary on the AfCFTA Digital Trade Protocol*. Youtube video, Centre for Intellectual Property and Information Technology Law.

CSEA. 2021. *Strengthening Data Governance In Africa.* Project Inception Report, Abuja: Centre for the Study of the Economies of Africa.

D4DHub. n. d. *Data Governance in Africa*. Website page.

Diorio-Toth, H. 2023. *Five unique cybersecurity challenges in Africa.* Article, Kigali: Carnegie Mellon University Africa.

du Couëdic, T. 2014. *Djibouti wants to be a global digital hub*. Article, African Business.

EC. n.d. *European data strategy. Making the EU a role model for a society empowered by data.* European Commission.

EC. 2020. *A European Strategy for Data*. Communication From the Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. COM/2020/66 final, European Commission.

EC. 2024. *Shaping Europe's digital future.*

Endeavor Nigeria. 2022. *The Inflection Point*: *Africa's Digital Economy is Poised to Take Off*. Blog.

Eromosele, F. 2023. *It's disappointing Nigeria hasn't conducted census in 17 years — Sen Ningi*. Vanguard.

EU. 2018. Regulation (EU) *2018/1807 of the European Parliament and of the council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*.

EU. 2022. *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022* on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union.

EU. 2023. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023* on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union.

Fidler, M. 2024. *African Data Protection Laws*: *Politics, But as Usual*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), African Data Protection Laws: Regulation, Policy, and Practice (pp. 55-74). Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909-006*.

Gathii, J. T. 2024. *The AfCFTA's Digital Trade Rules are Not Fit for Africa*. Analysis, Afronomicslaw.org.

Glassman, A. and Ezeh, A. 2014. *Delivering on a Data Revolution in Sub-Saharan Africa*. Brief, Washington, DC: Center for Global Development.

GPAI. 2023. *The Role of Government as a Provider of Data for Artificial Intelligence: Interim Report*. November 2023, Global Partnership on AI.

GSMA. 2021. *Cross-Border Data Flows The impact of data localisation on IoT*. Report, London: GSMA.

Houeto, C. 2023. *Protection des données et transparence: Le Sénégal lance sa Stratégie nationale des données*. Article, Africa Cybersecurity Magazine.

Ifeanyi-Ajufo, N. N.d. *"The current state of cybersecurity in Africa is the tendency towards a cyber-militarisation approach"*. Interview, Oxford: Global Economic Governance Programme, Blavatnik School of Government.

Ifeanyi-Ajufo, N. 2023. *Africa's Cybersecurity Treaty enters into force*. Commentary, Directions.

Ifeanyi-Ajufo, N. 2024. *The AU took important action on cybersecurity at its 2024 summit – but more is needed*. Article, Chatham House.

Jaïdi, L., Byiers, B. and El Yamani, S. 2024. *Fostering investment and inclusivity in the African Continental Free Trade Area*. ECDPM Briefing Note 182. Maastricht: ECDPM.

Kilic, B. 2024. *AfCFTA and digital governance*. Centre for International Governance Innovation.

King'ori, M. 2024. *RECs: Towards a Continental Approach to Data Protection in Africa Perspectives from Privacy and Data Protection Harmonization Efforts in Africa*. Global report, Washington, DC: Future of Privacy Forum.

King'ori, M. and Dorwart, H. 2022. *A Look into DPA Strategies in the African Continent*. Washington, DC: The Future of Privacy Forum (FPF).

Koch, T. 2022. *Better data is the key to unlocking major investment in Africa.* Article, Atlantic Council's Africa Center.

Lämmerhirt, D. 2019. *How open is government data in Africa?* Blog, Open Knowledge.

Miyandazi, L. 2020. *The African Union should work on policy implementation to realise its ambitions.* Blog, London: LSE.

Musoni, M. 2022a. *Eswatini: An overview of the Data Protection Act*. Article, OneTrust DataGuidance.

Musoni, M. 2022b. *Africa: The state of cross-border transfer of personal data in the SADC region.* Article, OneTrust DataGuidance.

Musoni, M. 2024. *The Role of Data Localisation in Cybercrime Investigations*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu and M. Hennemann (Ed.), African Data Protection Laws: Regulation, Policy, and Practice (pp. 177-202). Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909-011*.

Musoni, M., Domingo, E. and Ogah, E. 2023. *Digital ID systems in Africa: Challenges, risks and opportunities*. ECDPM Discussion Paper 360. Maastricht: ECDPM.

Musoni, M., Karkare, P., Teevan, C. and Domingo, E. 2023. *Global approaches to digital sovereignty: Competing definitions and contrasting policy.* ECDPM Discussion Paper 344. Maastricht: ECDPM.

Mwaya, J. 2022. *Dare to Share: Unleashing the Power of Data in Africa*. Commentary, Tony Blair Institute for Global Change.

Naidoo, R. 2020. *Building a vibrant data economy in Africa*. Article, ITWeb.

Ndemo, B., Ndung'u, N., Odhiambo, S., Shimeles, A. 2023. *Data Governance and Policy in Africa*. Information Technology and Global Governance.

OECD. 2019. *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. Paris: OECD Publishing, *https://doi.org/10.1787/276aaca8-en*.

Oloni, V. 2024. *Cross-Border Data Flows: Oiling the Wheel of the African Digital Economy*. In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu and M. Hennemann (Ed.), African Data Protection Laws: Regulation, Policy, and Practice (pp. 157-176). Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909-010*.

Olorunju, N. and Adams, R. 2022. *Research ICT Africa (RIA) Working Paper. African Data Trusts: New Tools Towards Collective Data Governance?* Research ICT Africa.

Pritchett, L. 2019. *The Big Stuck in State Capability and Premature Load Bearing, Some New Evidence*. Article, Cambridge: Harvard Kennedy School.

Sampath, P. and Tregenna, F. 2022. *Digital Sovereignty: African Perspectives*. Johannesburg: DSI/NRF South African Research Chair in Industrial Development. DOI: 10.5281/zenodo.5851685.

Saturday, B. and Nyamwire, B., 2023. *Towards Effective Data Governance in Africa: Progress, Initiatives and Challenges*.

Shahin, J., Hoogenboom, S., Morais, C., and Santaniello, M. 2024. *Chapter 4: Regional digital governance*. In Handbook of Regional Cooperation and Integration. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jul 5, 2024, from *https://doi.org/10.4337/9781800373747.00012*.

Soule, F. 2023. *Mandira Bagwandeen: The domination of foreign companies in Africa's digital landscape could impact a country's digital sovereignty*. Negotiating Africa's digital partnerships: interview series.

Soule, F. 2024. *Digital Sovereignty in Africa: moving beyond local data ownership*. CIGI Policy Brief no. 185.

Stuart, J. 2024a. *The Digital Trade Protocol of the AfCFTA and Digitally-Driven Development in Africa*. Blog, Tralac.

Stuart, J. 2024b. *The AfCFTA Digital Trade Protocol – clarification of key issues*. Blog, Tralac.

Teevan, C. 2023. *Building a digital single market: From the EU to Africa*. ECDPM Briefing note 155. Maastricht: ECDPM.

The Economist. 2018. *How regulators can prevent excessive concentration online*. Special Report, The Economist.

Tshuma, B. 2024. *Data Imaginaries and the Emergence of Data Institutions in sub-Saharan Africa.* In R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), African Data Protection Laws: Regulation, Policy, and Practice (pp. 205-214). Berlin, Boston: De Gruyter. *https://doi.org/10.1515/9783110797909-012*.

Vanheukelom, J., Byiers, B., Bilal, S. and Woolfrey, S. 2016. *Political Economy of Regional Integration in Africa. What Drives and Constrains Regional Organisations?* ECDPM Synthesis Report, Maastricht: ECDPM.

Waruru, M. 2023. *'Culture of secrecy' thwarting data sharing in Africa*. SciDev.Net, PsyhOrg.

Whittle, D. 2024. *Digital: Some Initial Thoughts on AfCFTA's Leaked Digital Trade Protocol*. Blog, Trade Notes.

World Bank. 2022. *A Digital Stack For Transforming Service Delivery: ID, Payments, and Data Sharing.* Practitioner's note, ID4D AND G2PX, Washington, DC: World Bank.

About ECDPM

ECDPM is an independent 'think and do tank' working on international cooperation and development policy.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union. This publication also benefits from the structural support by ECDPM's institutional partners: Austria, Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, The Netherlands and Sweden.

ISSN1571-7577

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Avenue des Arts 44, 1040
Brussels *Bruxelles*
Belgium *Belgique*
Tel +32 (0)2 882 50 08

info@ecdpm.org
www.ecdpm.org
KvK 41077447