African Union

An Integrated, Prosperous and Peaceful Africa

AU DATA POLICY FRAMEWORK

CONTENTS

FOREWORD ..... **IV**

ACKNOWLEDGEMENTS ..... **V**

EXECUTIVE SUMMARY ..... **VI**

1. INTRODUCTION **1**

2. MANDATE **3**

2.1 Vision 4

3. RISE OF THE DATA ECONOMY - NEED TO RE-THINK POLICY **7**

3.1 Data as the basis for new social contract and innovation economy 7

3.2 Need for data governance - creating value, preventing harms 9

4. CONTEXT **10**

4.1. Overview of international, regional policy and legislation trends 10

4.2 African policy and legislative context 11

4.3 Situational analysis for data economy in Africa 12

4.4. Arising challenges in realising opportunities and mitigating risk 13

5. DATA POLICY FRAMEWORK **18**

5.1. Guiding principles of the framework 19

5.2 Data definition and categorisation 20

5.3 Enablers to drive value in the data economy 21

5.4 Data Governance 46

5.5. International and Regional Governance 57

5.6. Implementation Framework 62

REFERENCES **65**

ANNEX - WORKING DEFINITIONS **69**

FOREWORD

African countries realise the enormous potential of a robust digital economy to create new business opportunities, increase efficiency, contribute to sustainable development and reshape people's lives.

The explosive growth of data as a strategic asset and a key element of contemporary economy and society has played a central role in policymaking, innovation and job creation.

Adopting the Digital Transformation Strategy (DTS) for Africa 2020-2030, along with the operationalisation of the African Continental Free Trade Area (AfCFTA), introduces huge opportunities for more interconnected and interoperable markets and offers avenues for tech start-ups and e-businesses to flourish. Against this background, the Commission developed the AU Data Policy Framework, which was endorsed by the AU Executive Council in February 2022.

Furthermore, the AU Data Policy Framework represents a significant step toward creating a consolidated data environment and harmonised digital data governance systems to enable the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits.

This framework sets out a common vision, principles, strategic priorities and key recommendations to guide African countries in developing their national data systems and capabilities to effectively use and derive value from data.

The endorsement of this continental policy document by African Union Organs shows the commitment and political will of African leaders to invest in data through strengthening cross sector collaboration and developing the related infrastructure to host, self-manage, process and use data being generated by people and industry to inform policy formulation and decision-making processes. Through this framework, African countries agree to put in place the needed mechanisms and regulations to cooperatively enable data to flow across Africa and pave the way to the achievement of the Digital Single Market.

Our approach to data is inclusive, transformational and forward-looking. We aim to harness the potential of the data revolution to empower people, institutions and businesses, boost intra-Africa digital trade, contribute to economic integration efforts, raise citizens' awareness on data protection and privacy issues, promote research and innovation, preserve states' sovereignty and ownership, build trust in the data ecosystem, and reinforce Africa's participation as a united front and a uniform stance in multilateral discussions on various data-based areas.

The domestication of this framework by African countries and the implementation of its key recommendations and proposed policy interventions both at national, regional and continental levels, along with the development of the necessary human and institutional capacity, will position Africa as a strong partner and will enable African youth to participate and thrive in the global digital economy and society.

Dr. Amani Abou-Zeid
AU Commissioner for Infrastructure and Energy

ACKNOWLEDGEMENTS

The AU Data Policy Framework was prepared under the overall guidance of H.E Dr. Amani Abou-Zeid, Commissioner for Infrastructure and Energy, a Taskforce comprising Moses Bayingana, Ag. Head of Information Society Division and Souhila Amazouz, Senior Policy Officer (Team Coordinator), as well as valuable contributions and inputs from:

Towela Nyirenda-Jere, Tichaona Mangwende and Gideon Nimako (AUDA-NEPAD); Jean Pierre Gashami and Omar Elmi Samatar (AfDB); Miriem Slimani (ATU); Aretha Mare and Jan Krewer (Smart Africa); Tunde Fafunwa, Mactar Seck and Linda Bonyo (UNECA); Torbjorn Fredriksson and Pilar Fajarnes Garces (UNCTAD); Amr Farouk Safwat and May Ragab Abdelhamid (STC-CICT Bureau Chair); Philip Sauerbaum (EU); Caroline Gaju (ITU); Seyni Fati (GSMA); Tapiwa Ronald Cheuka (AUC/ETIM); Marguerite Ouedraogo Bonane and Patricia Poku (African Network of Data Protection Authorities); Tania Priscilla Begazo Gomez, Marelize Gorgens and Mark Williams (WB).

The Framework benefited from financial support from GIZ and technical support from Research ICT Africa.

Comments were received at various stages of production of this framework by African experts from AU Member States, Regional Economic Communities and AU Specialized Institutions attending the virtual validation workshop and the Fourth Specialized Technical Committee on Communication and ICT.

The AU Data Policy Framework was endorsed by the Executive Council during its 40th Ordinary Session held on 2 – 3 February 2022 through Decision with reference EX.CL/ Dec.1144(XL).

Addis Ababa, February 2022

EXECUTIVE SUMMARY

Data is increasingly recognised as a strategic asset, integral to policy-making, private and public sector innovation and performance management, and creating new entrepreneurial opportunities for businesses and individuals. When applied to government services, emerging technologies can generate massive amounts of digital data and significantly contribute to social progress and economic growth. The central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives - from unleashing the economic and social potential of data to the prevention of harms associated with mass collection and processing of personal data.

The purpose of this document is to provide the policy framework for African countries to maximise the benefits of a data-driven economy by creating an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation. This enabling environment refers both to the collaboration between in-country sectors, institutions and stakeholders, an alignment of their development priorities, and the harmonisation of policy across the continent in a manner that provides the scale and scope required to create globally competitive markets.

From a policy perspective, the approach adopted is people-centred, locating them in relation to the role of data in contemporary economy and society by identifying the elements and linkages in what can be called the "data ecosystem" in order to identify the exact points of policy intervention. This allows for a systemic assessment of the interrelated challenges arising from global developments that impact emerging national data economies and those arising within the context of nascent data-driven economic activity, uneven institutional endowments, and human development in many African countries. This enables the design of a contextually grounded but forward-looking data policy framework that uses economic regulation to guide policy makers in realising opportunities for data-driven value creation. The framework points to how opportunities can be realised and how associated risks could be mitigated by creating an enabling and trusted environment.

Building a positive data economy national and regional will require unprecedented levels of collaboration between stakeholders to disrupt the economic, political, and policy pressures already being felt from the global data economy. In order to ensure equitable and safe access to data for innovation and competition, Member States should establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. Existing legal instruments and institutions should be revisited where necessary to ensure that they are not in conflict with one another and that they offer complementary levels of protection and obligations.

A comprehensive data strategy will necessarily include the harmonisation between competition, trade, and taxation policies and laws both at the national and regional levels. This is so an optimised data ecosystem for Africa balances revenue mobilisation and the need to avoid distortions to local markets and the global tax system. Intellectual property laws should also be revised to clarify that they do not generally impede the flow of data or data protection. At the same time, governments need to develop transversal digital policies and strategies to coordinate activities across the public sector and between the public and private sectors to meet national objectives.

While there are multiple competing definitions of data, common to all is the recognition that there are many different types of data. There are also numerous ways that data can be categorised that affect the appropriate policy and regulation of that category in order to mitigate any potential risk associated with the processing, transfer or storage of it. A primary distinction is between personal data and non-personal data, with data protection referring to ensuring the privacy of data subjects. Data categorisation guidelines should be one of the first actions of the data information regulator, a key institution for the development of an integrated national data system, which should be established in partnership with all relevant stakeholders. Essential to the development of an enabling environment for the data economy is ensuring the necessary foundational digital infrastructure and the human resources necessary to develop data as a strategic asset. Due consideration needs to be given to developing robust Digital ID systems for the delivery of public and private value to citizens and consumers.

As the framework also emphasises, this can only be properly achieved through instilling a culture of trust in the data ecosystem. This is done through the establishment of safe and secure data systems based on effective cybersecurity and data protection rules and practices, and ethical codes of conduct for those who set data policy, implement it and those who use data – whether in public, private or other sectors. This is not sufficient, however. Trust in data governance, and a national data system is established through legitimacy. This includes systems and standards that guarantee public and private sector compliance, government itself adhering to personal data protection rules, and government sharing public data.

The framework instils the importance of collaborative and evidence-based policy processes for the domestication of the policy proposed. The governance and institutional arrangements should assign clear roles to the government as policy maker and independent, agile and capacitated regulators to implement policy and effectively regulate the data economy to ensure that fair competition produces positive consumer welfare outcomes. The creation of data and information regulators to promote and safeguard the rights of citizens and their participation and fair representation in the data economy and society will need to be a priority for those countries that have not yet established these. Coordination with other regulators to achieve this will be essential. The legal ecosystem must be harmonised and rebalanced.

Access to data is a prerequisite for value creation, entrepreneurialism and innovation. When data is of poor quality or not interoperable, they limit the capacity of firms and the public sector to engage in the sharing and analytics that can provide economic and social value to data. These processing frameworks should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity. Security models also need to be transversal, with specific emphasis on cloud storage and processing of sensitive/proprietary data, API management, and support of equitable data economies.

Attention needs to be paid to access to quality, interoperable and reliable data – primarily from the state but also from the private and other sectors – with a reinvigoration of the principles of open governance across the continent. Capacity-building should be a key national and regional priority, and resources will need to be allocated in this regard in the areas of data

protection, cybersecurity and institutional data governance in relevant agencies. Skills and an understanding of the data ecosystem will also need to be built in state institutions, a mongst other sectors and communities.

The framework is guided by the broad principles of transparency, accountability of institutions and actors, the inclusion of stakeholders, equity among citizens and fair competition amongst market players. The principles guiding the framework include trust, accessibility, interoperability, security, quality and integrity, representivity and non-discrimination.

As the framework emphasises, transversal collaboration needs to be underpinned with mechanisms to stimulate demand for data, which includes incentivising innovative data communities, and, on the supply-side, ensuring the quality, interoperability, and relevance of data in both the public and private sectors and civil society.

As the framework suggests, there are several regional processes, mechanisms and instruments that can and should be leveraged in the continent's efforts to develop a cohesive data policy framework. These include the African Continental Free Trade Agreement (AfCFTA), which provides an opportunity for cooperation on a number of important aspects of the policy framework. Collaboration between national and regional stakeholders is also necessary for African countries to become more competitive in global policy setting forums where regulations for the global data economy are set and where African states have largely been "standard takers".

It is recognised that different African states have different economic, technical, and digital capabilities, and the recommendations and actions need to be read in this light. It is nevertheless envisaged that the different demands of building a data ecosystem will be progressively realised by countries. At the same time, there are several areas that can be attended to independently of economic or technical capabilities, including establishing regulatory independence, promoting a culture of trust and ethics, building collaborative frameworks for relevant sectors, developing transparent, evidence-based and participatory policy and regulations, participating in collaborative regional processes and mechanisms, and ratifying the AU Convention on Cybersecurity and Personal Data Protection.

The Framework presents a set of detailed recommendations and arising actions to guide member states through the formulations of policy in their domestic context, as well as recommendations to strengthen cooperation among countries and promote intra-Africa flows of data. The main high-level overarching recommendations are included here. It is recommended that Member States:

- cooperatively enable data to flow on the continent while safeguarding human rights, data protection, upholding security and ensuring equitable sharing of the benefits;
- cooperate to create the necessary data capabilities to take advantage of data-reliant technologies and services, including the capacity to govern data so that it benefits African countries and citizens and enables development;
- promote transversal data policy and agile regulation to navigate the emergence of new dynamic data-driven business models that can foster intra-Africa digital trade and data-enabled entrepreneurship;
- create co-jurisdictional frameworks for the coordination of autonomous competition, sector, and data regulators to regulate the data society and economy effectively, formulate, implement, and review data policy in a dynamic, forward-looking and experimental way;

- develop national legislations on personal data protection and adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment;
- establish or maintain independent, well-resourced and effective Data Protection Authorities, strengthen cooperation with DPAs from members of the African Union and develop mechanisms at the continental level to develop and share regulatory practices and support institutional development to ensure a high level of protection of personal data;
- promote interoperability, data sharing, and responsiveness to data demand through the setting of open data standards in data creation conform to the general principles of anonymity, privacy, security and any sector-specific data considerations to facilitate non-personal data, and certain categories of personal data are accessible to African researchers, innovators and entrepreneurs;
- promote data portability so that data subjects are not locked into a single provider and, in so doing, promote competition and consumer choice and enable gig workers to move between platforms;
- improve unevenly developed infrastructure across the continent, leveraging existing REC regional efforts to support efficient broadband network coverage, reliable energy supply, and foundational digital (data) infrastructure and systems (FDI) (digital identity (Digital ID)), interoperable trustworthy payments, cloud and data infrastructure, and open data sharing systems, for cross border digital trade, e-commerce;
- establish an integrated national data system to enable data-driven public and private value creation, operating on the basis of harmonised governance frameworks that facilitate the flow of data necessary for a vibrant data economy, but with sufficient safeguards to be trusted, safe and secure;
- govern the integrated national data system according to the principles of access, availability, openness (where anonymity can be preserved), interoperability, safety, security, quality, and integrity;
- integrate sector-specific and specialists data codes or guidelines into national and continental data governance regimes;
- who have not yet ratified the AU Convention on Cyber Security and Personal Data Protection, do so as soon as possible to serve as the foundational step for the harmonisation of data processing;
- in the forthcoming negotiations on Trade in Services and E-commerce protocols, as well as the Competition and Intellectual Property protocols, in the African Continental Free Trade Area provide guidelines to promote access to data to support local innovation, entrepreneurialism and pro-competitive purposes;
- prioritise politically neutral partnerships that take into account individual sovereignty and national ownership to avoid foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States; and
- promote research, development and innovation in various data-based areas, including Big Data Analytics, Artificial Intelligence, Quantum Computing, and Blockchain.

It is further recommended that The African Union Commission, RECs and Regional Institutions:

- facilitate collaboration between the various entities dealing with data across the continent through the establishment of a consultation framework within the digital ecosystem community to safeguard the interest of each actor;
- promote and facilitate data flows within and among AU Member States by developing a Cross Border Data Flows Mechanism that takes into account the different levels of digital readiness, data maturity as well as legal and regulatory environments of countries;
- facilitate data circulation across sectors and cross borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security;
- work in close collaboration with national authorities in charge of personal data protection of AU members, with the support of the African Network of Authorities (RAPDP), to establish a coordination mechanism and body that oversees the transfer of personal data within the continent and ensures compliance with existing laws and rules governing data and information security at national level;
- establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards;
- establish mechanisms and institutions, or empower existing ones, within the African Union to build capacity and render technical assistance to AU Member States for the domestication of this data policy framework;
- support the development of regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and Artificial Intelligence) and the necessary enabling environment and data-sharing mechanism to ensure the circulation across the continent;
- work towards building a secure and resilient cyberspace on the continent that offers new economic opportunities through the development of an AU Cyber Security Strategy and establishment of Operational Cybersecurity Centres to mitigate risks and threats related to cyberattacks, data breaches, and misuse use of sensitive information;
- enable data sharing and enhanced interoperability among AU Member States and other AU mechanisms, including the African Union Mechanism for Police Cooperation (AFRIPOL);
- establish an Annual Data Innovation Forum for Africa to raise awareness amongst policy makers about the power of data as the engine of a digital economy and society so as to facilitate exchanges among countries and enable knowledge sharing on data value-creation and innovation and the implications of data usage on peoples' privacy and security;
- strengthen links with other regions and coordinate Africa's common positions on data related international negotiations to ensure equal opportunities in the global digital economy; and
- develop an implementation plan that takes into consideration the digital sovereignty of states as well as the different levels of development, the vulnerability of populations and digitisation within AU Member States, namely aspects related to ICT infrastructure gap and lack of cybersecurity policies and legislations.

1. INTRODUCTION

Data is at the core of the digital transformation taking place at an unprecedented pace and scale globally. The deployment of data-driven technologies to transform most aspects of our daily lives and work into quantifiable data that can be tracked, monitored, analysed and monetised has become such a phenomenon that the term 'datafication' has been coined to describe it.

These processes - which have accelerated during what has been referred to as the first 'data-driven pandemic' - can turn public and private organisations into data-driven enterprises, improving information flows and efficiencies and creating more competitive economies. Enhanced information flows under the right conditions can also reduce information asymmetries between governments and citizens, ultimately strengthening good governance.

Some of these processes have been incremental and some disruptive, but they have all been highly uneven. Data utilisation is one of the key drivers in accelerating the achievement of Agenda 2063 and the Sustainable Development Goals (SDGs), with the absence of good data being one of the primary challenges to assessing the progress being made toward achieving the underlying targets. Specifically, improved integrated data systems directly contribute to the achievement of several of the goals, such as improved health, education systems identity systems, but without direct policy intervention, the current uneven distribution of opportunities and harms arising from datafication between countries and within them will be exacerbated.

Whether African states can create the conditions for the harnessing of these processes of digitalisation and datafication to create added value, increase efficiency and productivity, improve social services and create new forms of work will depend on the policies adopted and implemented. This calls for a collaborative African response.

Maximising the benefits of a data-driven economy and minimising the risks are highly dependent on enabling policy and regulatory frameworks that increase legitimacy and public trust in the management of data. Data infrastructure that enables an integrated data system is a key strategic asset for countries, but the scale, extent and speed of change brought about by data-driven digital technologies make regulation complex and resource-intensive. As emerging technologies become more central to the data economy, the diversity of stakeholders and plethora of platforms involved in its regulation also expand dramatically, making it increasingly difficult for policymakers to remain involved and informed (African Development Bank, 2019). Emerging advanced technologies like AI are likely to increasingly challenge the efficiency of traditionally disparate legislative approaches to lawmaking.

Data is global in nature, meaning that on the one hand, regulations have cross-border implications and that, on the other, regulatory precedence is most often set by data-rich and data-intensive developed countries. Market pressure is also imposed by oligopoly firms, notably Google, Apple, Facebook, Amazon and Microsoft (or GAFAM). The nature of data allows these firms trading in global data-driven digital markets to leverage their competitive advantage in data and algorithms across the globe. This ultimately affects local competition and inhibits the global competitiveness of domestic data economy participants. There are, therefore, issues of intellectual property and data access, fair trade, competition and consumer rights that impact data policy in a global context and raise the need for global governance and collaboration.

These factors also highlight that much of what drives the development of the local data economy has been outside of the control of African stakeholders, who have been largely 'standard takers' in global governance. They also underscore the need for collaboration and partnerships in many African data ecosystems, regardless of digital maturity and broader economic endowments.

This policy framework, therefore, presents opportunities for countries to ensure that laws proactively enable access to data for developmental, innovative and competitive purposes. At the same time, it demonstrates the need for these to be in harmony with one another to create the scale and scope in the market necessary for data-driven value creation and innovation, which can catalyse the single digital market envisaged in the African Union Digital Transformation Strategy.

2. MANDATE

The central role of data **requires a high-level and strategic policy perspective that is strongly rooted in the local context** and can balance multiple policy objectives. National data strategies and internationally interoperable approaches can help unleash the economic and social potential of data while preventing harm and mitigating risks (OECD, 2019).

This data policy framework derives from the Digital Transformation Strategy (DTS) adopted by the African Union in 2020 to transform African societies and economies in a manner which allows the continent and its member states to harness digital technologies for local innovation that will improve life opportunities, ameliorate poverty, reduce inequality facilitating the delivery of goods and services.[1] Realisation of the objectives of the DTS is critical to the achievement of the African Union Agenda 2063, the pan-African strategic framework for unity, self-determination, freedom, progress, and collective prosperity, and of the United Nations Sustainable Development Goals.

The Data Policy Framework builds on existing instruments and initiatives such as the Digital Transformation Strategy for Africa 2020-2030 (DTS), the African Continental Free Trade Area (AfCFTA) agreement, the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), Smart Africa Vision to Transform Africa into a Single Digital Market by 2030, the Free Movement of Persons (FMP), the Single African Air Transport Market (SAATM), The Single Electricity Market in Africa, the Interoperability framework on Digital ID, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the Declaration on Internet Governance and Development of Africa's Digital Economy of 2018, the Personal Data Protection Guidelines for Africa, regional model laws on data protection and cybersecurity and the African Union Charter on Human and People's Rights.

This Data Policy Framework sets out a common vision, principles, strategic priorities and key recommendations to guide African Union Member States in developing their national data systems and capabilities to effectively derive value from data that is being generated by citizens, government entities and industries. The potential of data-driven solutions to overcome most of Africa's development challenges is made possible by the Member States adopting a common data policy underpinned by a coherent governance approach. Furthermore, the development of integrated data systems is critical to optimise information flows and productivity gains from digitalisation and datafication.

This Data Policy Framework aims to strengthen and harmonise data governance frameworks in Africa and thereby create a shared data space and standards that regulate the intensifying production and use of data across the continent. This by creating a safe and trustworthy digital environment to boost the development of an inclusive and sustainable digital economy that fosters Intra-Africa Digital Trade in line with the ongoing regional economic integration initiatives under the AfCFTA.

1 The Executive Council at the Thirty-Six Ordinary Session held on 6-7 February 2020 endorsed the Digital Transformation Strategy for Africa (2020-2030), referenced in decision [EX.CL/Dec.1074 (XXXVI)], as the master plan that will guide the digital development Agenda of the continent, with Data as one of its cross-cutting themes and as a building block for the establishment of Africa digital economy and society. To enable the creation of Africa's digital economy and society, the Executive Council in its decision [EX.CL/Dec.1074 (XXXVI)], tasked the AU Commission to lead and coordinate the development of a continental framework on data policy and its submission to the STC-CICT 4 in 2021 for consideration and endorsement.

DATA USE CASE FOR VALUE CREATION

Data deserts in many African countries reflect the digital divide, as many people do not have access to the services and systems used to generate the data that are needed to train algorithms or to analyse for decision-making. User-generated data sets, such as social media updates and call detail records (CDR), are a major part of the data revolution, provided they are collected in a responsible manner. These data sets can be combined and repurposed with other data such as anonymised citizen data to reflect the lived experiences of millions of individuals and provide valuable information about many different vulnerable communities that can inform policy making, enhance interventions, and spur economic activity across various use cases. For example, in Senegal, big data was used to map CDR, mobility, and economic activity. In Kenya, big data on M-Pesa mobile money transactions was used to create credit and savings products for subscribers and create credit profiles for small-holder farmers for input and harvest loans, a section of the economy that is typically not able to access formal banking facilities.[2]

2.1 VISION

The Data Policy Framework envisions the transformative potential of data to empower African countries; improve people's lives; safeguard collective interests; protect (digital) rights; and drive equitable socio-economic development.

Practically the process seeks to translate this vision into a framework which will when implemented:

Empower Africans to exercise their rights through the promotion of trusted, safe and secure data systems integrated on the basis of common standards and practices;

Create, coordinate and capacitate governance institutions to regulate, as necessary, the everchanging data landscape and to increase the productive and innovative use of data to provide solutions and create new opportunities while mitigating risk;

Ensure that data can flow across borders as freely as possible while achieving an equitable distribution of benefits and addressing risks related to human rights and national security.

2 See *https://www.developlocal.org/the-big-data-in-africa-report/*

2.2 SCOPE AND OBJECTIVES

Given that data now traverses every aspect of our daily lives, but under very different circumstances across the continent, the **framework provides principle-based guidance** to member states in their domestication of the continental data policy appropriate to their conditions and proposes a continental instrument or mechanism to integrate and coordinate continental efforts. The Africa Data Policy Framework aims to **strengthen national data systems** for effective use of data by creating an enabling environment that **stimulates innovation and entrepreneurialism to drive the development of data value-driven economies** and that facilitates the interoperability of systems and cross border data flows necessary for the realising of the African single digital market. Harmonised across the African markets, this affords the regulatory certainty and the scale and scope conducive to investments required for data-driven public and private value creation with the associated distributional impacts and non-economic multipliers.

With regards to the scope of the framework, it is important to bear in mind that the policy is concerned with **data governance that includes personal, non-personal, industrial and public data**, not only personal data protection that has been the focus of attention internationally and on the continent in recent years.

The specific and overreaching objectives of the African Data Policy Framework are to:

- enable states to cooperate on matters of data governance to achieve common objectives related to the sustainable development of their economies and societies;
- inform and support the domestication of continental policy by African countries;
- ensure that data can flow across borders as freely as possible while promoting an equitable distribution of benefits and addressing risks related to human rights violations and other legitimate interests of states such as the fight against money laundering, tax evasion, online gambling, and national security;
- foster and facilitate cross border data flows and increase business opportunities while ensuring an adequate level of personal data and privacy;
- establish collaborative trust mechanisms to allow for data to circulate as freely as possible between Member States while preserving the sovereignty of Member States and their ability to regulate the digital economy;
- enable states, the private sector, civil society and intergovernmental organisations to coordinate their efforts on data issues across the continent to realise a single digital market and compete more effectively in the global economy;
- enable competitiveness in the global economy through close and sustainable cooperation by African states, the private sector and civil society through restructuring opportunities to optimise the benefits from datafication of the economy and society;
- ensure that data are used in a sustainable manner that benefits society as a whole and does not harm people's privacy, dignity and security;
- ensure that data are widely available within appropriate safeguards for both commercial and non-commercial use; and
- facilitate innovative ways to promote public benefits by using data in new ways that would enable the data in Africa to realise the value of data in public sector decision-making, planning, and monitoring and evaluation.

To enable the continental data policy to meet its envisioned objectives and reflect the interests of all stakeholders, the formulation of the **policy framework is informed by previous initiatives and documents** both from within and outside Africa. The process included an open public consultation. Inputs made through this online consultation, and a public webinar contributed to the development of the draft policy framework.

The AUC coordinated the development of the AU Data Policy Framework in collaboration with Pan African organisations and AU specialised Agencies and Institutions, namely: Regional Economic Communities, AUDA-NEPAD, Smart Africa Secretariat, African Development Bank, Africa Telecommunications Union (ATU), the UN Economic Commission for Africa, International Telecommunication Union (ITU), the UN Council on Trade and Development (UNCTAD), the World Bank as well as other partner institutions.

Data Policy framework

Formulation	Domestication	Monitoring & Evaluation
Identification of policy challenges high level principles, and of recommendations and actions	Implementation of actions (national integrated data systems) Strategies for progressive realisation of enabling conditions	Indicators Targets Measurement
Continental Initiatives, Mechanisms, Instruments		
Global Governance		

3. RISE OF THE DATA ECONOMY - NEED TO RE-THINK POLICY

A shift in approach to data regulation is required for countries to properly benefit from the emerging global data economy. This shift informs this framework. Key elements of this integrated approach to data policy formulation are outlined below.

3.1. DATA AS THE BASIS FOR NEW SOCIAL CONTRACT AND INNOVATION ECONOMY

As data in and of themselves have little value, it is only through the processing, transmission, storage and combination that value is added. In economic terms, data can be understood as a public good in that it is inherently non-rivalrous (at the technical level, it is infinitely usable without detracting from another person's ability to use it). It is naturally non- excludable, which means that there are no natural barriers to multiple people using the same data at once. Although there are attempts to render data excludable through technological and sometimes legal means, these are not inherent features of data. Attempts to limit access, whether for purposes of commercialisation or security, can be regulated to be non-excludable. For example, data that are made open under an internationally recognised licence or public statistics can be regulated to be accessible like free to air public broadcasting, as a classical public good.

Data also does not automatically generate value. Instead, there are different uses of data and different methods to measure the economic and social value of data and data flows (OECD, 2019). In the economic sense, it is what firms do that leads to value creation both internally within the firm and externally across the extended-data network. Theoretically, this value can be quantified by assigning monetary value taking in consideration several cost and income-generating variables, such as how organisations charge for user-generated data or reconciling data management costs such as collecting, maintaining and publishing data. Valuing data from a socio-economic benefits perspective – or non-market-based data value – arises when there are fundamental conditions or enablers that allow governments to deliver more effective public services, offer effective environmental stewardship, and when citizens live healthier and economically secure lives through leveraging data (World Bank, 2021). An example of public data value creation includes using data to inform resource allocation needs to enhance service delivery.

These data characteristics have elsewhere been framed as the **potential of data to provide the basis of a new social contract** (World Bank, 2021). Arising policy directions from this approach emphasise the need for open data, interoperability standards and data-sharing initiatives to harness the potential of data for driving development; ensuring a better distribution of the benefits of data; fostering trust through safeguards that protect people from the harm of data misuse; to create and maintain an integrated national data system that allows the flow of data among a wide array of users in a way that facilitates safe use and reuse of data.

Trust is central to a robust, flourishing data environment. Trust is often equated in the context of digital governance with technical security and confidence in the technical system required for e-commerce to operate. While technical security may be a necessary condition for trust, it is not sufficient. Instead, trust-building permeates the entire data ecosystem, from the people-centred formulation of rights-preserving policies and regulations to ensuring access to and use of data to enable more equitable inclusion in the data economy.

Although the harms associated with the concentration of data and information and asymmetries of power are universal, the impacts are uneven, both between and within countries. Creating policies that mitigate the differential risk for different categories of people, such as children, or categories of data in different sectors, such as health data, or ensuring that the increasing centrality of data does not perpetuate historical injustices and structural inequalities will require far more granular and adaptive regulation. While a right preserving data policy framework will be essential, the individualised notions of privacy, freedom of expression and access to information (first generation rights) in current data protection normative frameworks will not be sufficient to ensure more equitable and just outcomes. Second-generation social and economic rights are also relevant to several areas of data governance in relation to data availability, accessibility, usability, and integrity that require data governance to impact equitable inclusion. This highlights the need to move beyond only negative compliance regulation to positive enabling regulation that will create an environment for African states and citizens to participate effectively in the digital economy. Creating the conditions that allow for the necessary access to data while safeguarding rights will require building institutional capacity within the state and the capabilities to regulate agilely to harness the potential of data to address some of the continent's most intractable problems.

To do so, **policymakers need to balance some of the tensions in the valuing of data** in order to optimise it for these purposes. The transformation of data into useful information to guide decision-making revolves around the data value chain where firms and certain public entities are adequately equipped with enabling frameworks to support a coherent data ecosystem. Generating value from data can enhance private interests, such as improving firm operational efficiency, increasing their customer base, and creating innovative products and services that benefit commercial activities and data subjects. For governments, public value from data is realised by ensuring that the socioeconomic benefits of data accrue to enable the achievement of wider socio-economic goals. While public and private data valuation have different intentions and outcomes, they are not mutually exclusive. In fact, market and non-market value should not be correlated with the private sector and public sector. Non-market value could be linked to research or civil society too. The public sector can also create market value by opening certain data sets and establishing new revenue streams. There are also innovative interplays between public and private actors that can improve the overall data ecosystem to meet socio-economic development needs and enhanced welfare.

With the increasing complexity and adaptiveness of the global communications system, both newer and more traditional forms of governance are arguably proving incapable of providing adequate tools for the governance of global public goods such as data. From a policy point of view, there is a growing distinction being drawn between data value-creation and the value-extracting features of existing data-intensive and platform-oriented industry behaviour and business models (Mazzucato et al., 2020).There has been little restraint either from competition or data regulators on the rise of monopolistic global platforms producing and extracting massive amounts of private data, which has been commodified with seemingly little regard for the social and negative implications for the data subjects (Zuboff, 2018). This may require specific and transversal regulatory responses in order to preserve the positive obligations of data governance.

3.2 NEED FOR DATA GOVERNANCE - CREATING VALUE, PREVENTING HARMS

Data governance at a macro level emerges as an opportunity to use standards, rules, norms and principles as mechanisms for both mitigating against identified data risks and harms while advancing data economy development and digital dividends.

Policy on data governance, therefore, has some practical mechanisms:

- aligning the principles to underscore data governance as a normative function;
- assigning roles and responsibilities for the implementation of policy at a macro and micro level;
- identifying and ensuring legal and policy clarity for mechanisms for implementing data governance;
- identifying and encouraging collaboration across vertical and horizontal stakeholder groups;
- balancing the need for circulation of data to enhance value creation while creating economic incentives for investments in data infrastructure and services and so on; and
- establishing trust mechanisms to support data sharing under terms and conditions agreed upon by all parties on rules for data use and issues of liability (data accuracy, for instance).

This simplification of data governance policy must then be contextualised within the challenges and opportunities described below. In so doing, governance priorities become:

Data definition - Providing specificity and detail on the types of data to be regulated and to what extent to ensure the maximisation of benefit for different role players in the implementation of data policy. This should be done cognisant of the value and nature of data.

Continental coordination - Providing mechanisms and priorities for coordination within the continent to strengthen Africa's position within global governance and provide support for domestication.

Domestic institutional capacity - Assigning obligations, responsibilities and powers for institutional actors at the national level that can help create a consistent domestic environment for data communities (public and private) to institute data activities.

Domestic collaboration - Ensuring policy alignment, identifying multi-stakeholder participants and advancing mechanisms for successful domestication.

Policy support - Providing implementable standards and solutions that focus on the achievement of healthy domestic data quality, control, access and interoperability, processing and protection, and security as the means for growing a data economy.

Clarity - Ensuring clarity, which facilitates compliance, does not have unintended restriction but can also serve as a foundation for cross-border (and cross-silo) coordination.

4. CONTEXT

4.1. OVERVIEW OF INTERNATIONAL, REGIONAL POLICY AND LEGISLATION TRENDS

Many jurisdictions across the world do not have data policy, with about a third having no data legislation in place. UNCTAD found in 2020 that 66% of countries in the world have some sort of legislation, 10% have draft legislation, 19% have no legislation, and 5% have no data at all (UNCTAD, 2020).

Globally, a number of instruments have emerged in this context, such as the EU GDPR 2016/679, the APEC Privacy Framework and the Trans-Pacific Partnership (TPP) Agreement. These agreements take slightly different approaches to data protection and may serve as points of reference for Africa's concerted efforts at data protection.

The EU's GDPR 2016/6 is wide-ranging with an expansive definition of what personal data is. Its broad territorial scope applies within and outside the EU, contains serious penalties for subverting the regulation, requires considerable openness and transparency and, importantly, grants individuals' substantial rights that can be enforced against businesses. This approach to data protection is centred around a human rights agenda in the digital ecosystem.

The APEC Privacy Framework, which has been applied by APEC member states since 2005, is made up of a set of principles which are set up to ensure the free flow of information in support of economic development. APEC's framework takes a different approach to data protection by aligning the framework's mandate with the promotion of trade and investment. An important highlight of the framework is how it emphasises that privacy regulations must take into con- sideration the importance of business and commercial interests in addition to the cultures and other diversities of member states' economies.

The Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) focuses on open trade and regional integration amongst member states. The agreement allows for the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the businesses, but countries can require protection of data that is transferred.

Outside of these multilateral agreements, the public goals of data protection typically centre around protecting the privacy of individuals and communities, safeguarding valuable data from leaks, loss, and theft, and maintaining and increasing public, investor and customer confidence. In a bid to achieve these goals, many countries have included potential barriers to data flow in their domestic laws, such as data localisation requirements and, in some instances, more stringent data processing and collection requirements. These may inadvertently retard or counteract the objects of more far-reaching regional policy frameworks.

In the evolution of domestic policies for the digital economy, several strategies have crystallised globally, such as the government-led approach (as championed by the EU), the private sector-led approach (as promoted in the United States), the top-down policy approach (exemplified by Singapore), and the bottom-up approach (for instance, in Hong Kong, China). These approaches have varying complementary effects on policy implementation, deployment, impact, innovation, agility and stability.

4.2 AFRICAN POLICY AND LEGISLATIVE CONTEXT

In line with international precedents, most efforts in data regulation on the continent have focused on data protection, with the chief aim being to observe and safeguard internet users' privacy rights. While the use and processing of data is a cross-cutting concern, which impacts an array of traditionally siloed areas of policy, there are no examples of umbrella laws that regulate every aspect of data. Instead, data has been regulated across five branches of the law: data protection law, competition law, cyber security law, electronic communications and transactions law and intellectual property law, which potentially conflict in some instances and leave gaps in others.[3]

It is estimated that **32 of Africa's 55 countries have enacted or embraced some form of regulation with the chief aim of protecting personal data.** Regionally, legislative tools such as the 2008 East African Community Framework for Cyberlaws, the 2010 Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS), and the 2013 Southern African Development Community *model law* harmonising policies for the ICT Market in sub-Saharan Africa have been developed. Continentally, the African Union developed the first pan-African framework with the African Union Convention on Cyber Security and Personal Data Protection (*Malabo Convention*) in 2014, which has not come into effect but is currently being ratified.

Regional competition laws and protocols on competition in the established Regional Economic Communities (RECs) apply to businesses that process data, although they mostly do not explicitly refer to data. They include the 2004 COMESA Competition Regulations and Competition Rules, The EAC Competition Act (2006) and The EAC Common Market Protocol and the Protocol on the Establishment of an EAC Customs Union, The ECOWAS Supplementary Act on the "Adoption of Community Competition Rules and the modalities of their application within ECOWAS", The SADC Protocol on Trade (2006), and the SADC Declaration on Regional Cooperation in Competition and Consumer Policies (2009). They address anti-competitive practices, including abuse of dominance and also market structure through regulation of mergers and acquisitions. However, details and approaches differ, which presents challenges for businesses operating in multiple regions.

OTHER MAJOR INITIATIVES ON THE CONTINENT LOOKING AT DATA POLICY

Policy and Regulation Initiative for Digital Africa (PRIDA)[4]: Within the framework of the implementation of this project, The African Union Commission established an Expert Working Group that contributed to the identification of the key harmonisation indicators and the development of a Monitoring and Evaluation (M&E) Model and Tool on Data Protection & Localisation which is ready to use by the AU Member States and Regional Organisation to assess the extent of harmonisation and alignment of national laws and regulations.

Smart Africa is supporting the creation of a harmonised framework for data protection legislations in Africa through the Smart Africa Data Protection Working Group that aims at producing a mapping of legal frameworks, implementation guidelines for Smart Africa Member States, as well as recommendations on enhancing harmonisation and collaboration mechanisms between Data Protection Authorities (DPAs).

3 The continental dimensions of these challenges are addressed through continental digital collaboration.

4 PRIDA is a joint initiative of the African Union (AU), the European Union (EU) and the International Telecommunication Union (ITU) that aims at enabling the African continent to reap the benefits of digitalisation, by addressing various dimensions of broadband demand and supply in Africa and by building the capacities of African stakeholders in the Internet Governance space.

4.3 SITUATIONAL ANALYSIS FOR DATA ECONOMY IN AFRICA

Undertaking a situational analysis of the entire continent with its diverse legal, regulatory and political systems and considering the unevenness of countries' economic development and digital readiness makes it inherently limited and overly generalised. The purpose of the high-level SWOT analysis is to identify broadly applicable strengths and weaknesses of countries at a regional level and to identify the potential opportunities and known risks associated with the global processes of digitalisation and datafication that characterise the development of data economy for all countries but also what these mean specifically for African countries, within their broader developmental context.

Strengths	Weaknesses
• Foundational regional data governance instruments • Regional Economic Communities (RECs) to support economic aspects of data policy initiatives • Regional and continental courts to enable harmonised dispute resolution • Emerging innovation hubs in the region to demonstrate best practices across jurisdictions • Fewer and less developed competition, data and IP laws on data, so there is greater potential for early, rapid continental harmonisation of laws enabling cross border trade	• Sub-optimal data connectivity and usage • Non-harmonised data governance regime • Inconsistencies in the treatment of data in data protection, competition and intellectual property laws within countries • Localisation rules that limit the crossborder flow of information • necessary for local value creation and establishment of the single market • Resource constraints in the evolution and implementation of data governance frameworks • Inadequate data infrastructure • Insufficient open government data to meet data demand • Inadequate provision, or access to, quality data • Uneven development of data standards • Low penetration of foundational Digital ID • Limited number of Data Protection Authorities (DPAs), many of whom • are not well-resourced and/or fully empowered) • Need for cybersecurity capacity

Opportunities	Threats/Risks
• If preconditions are met and enabling environments are created, there are opportunities for both public and private data-driven value creation through improved information flows and efficiencies • Data use for improved public planning and service delivery and public and private sector coordination • With open data and interoperable standards underpinning an integrated national data system, barriers to market entry may be reduced, and opportunities for entrepreneurial development and innovation may increase • Global efforts to develop and harmonise data policy and governance frameworks • Global efforts to coordinate taxation of digital and data services that have largely not contributed to national resource mobilisation efforts • Emerging work opportunities for tech-savvy youth to enhance local entrepreneurialism, local content development and innovation	• Inability of some countries to overcome the challenges of creating enabling environments necessary to realising opportunities • Failure to harmonise policy and regulatory frameworks to enable economies of scale and scope for data value creation and for all countries to enjoy the benefits of a common digital market • Constantly changing data protection and privacy risks • Discriminatory automated (algorithm-based) decision-making risk resulting from invisibility, underrepresentation of categories of people in datasets, and algorithm modelling shortcomings • Concentration in global data markets, preventing fair competition in local markets • Inadequate levels of international policy cooperation required to deal with global data issues - access, integrity, security, equity, rights and ethics

4.4. ARISING CHALLENGES IN REALISING OPPORTUNITIES AND MITIGATING RISK

The uneven distribution of opportunities and risks associated with the development of the data economy correlates largely with the levels of human and economic development of countries and the inequalities between and within countries. These are reflected in the strengths and weaknesses highlighted above. The **ability of countries and regions in Africa to counter these trends is dependent on their ability to create an enabling environment for data-driven value creation that is inclusive and equitable.** The purpose of the data policy framework is to provide a framework for countries to overcome some of the challenges of policy formulation in this dynamic and fast-changing area through common purpose and collective action. Through the creation of a harmonised enabling environment, the strengths of countries can be leveraged and weaknesses mitigated for the development of an integrated continental data economy much more powerful than its individual parts.

The policy challenges that need to be overcome to create an enabling environment to realise the opportunities offered by globalised processes of digitalisation and datafication and to mitigate effectively identified risks for countries across the world should not be underestimated. These are currently the subject of several multilateral organisation reports (UNCTAD 2021, World Bank 2021). While some of the challenges relate to creating conditions for data-driven value creation at the national level that are highlighted in the situational analysis above and discussed below, the international and cross-border nature of data as global public goods requires more than ever before **regional and global cooperation** for them to be realised at the national level and to mitigate associated risks which may arise from the use of data beyond national borders. While the data policy framework provides a high-level framework for countries to develop national policies, these should be based on nationally consultative processes that take into account the local context, needs and institutional endowments of countries.

In creating this enabling environment in African Union member states and in the region, the following considerations arising from the situational analysis that may impact the ability of countries to respond to the needs of a new data economy are flagged.

Digitalisation and datafication cut across the public and private sector, the formal and informal economy, and social and cultural spheres and require a shift from traditional sectoral policies. Policy for the digital and data economy and society needs to be transversal to coordinate activities across the public sector and between the public and private sectors to meet national and regional objectives. It is, at the same time, important to consider the **specific sectoral data policies** to optimise and safeguard the diverse uses of different kinds of data (e.g. health data or climate data). Beyond noting this principle, the actual development of the several sectoral policies that will need to be developed is beyond the remit of this high-level framework. **Effective regulation of increasingly complex globalised markets is essential** to the ubiquitous backbone and seamless services needed for data services and applications to be deployed to meet the diverse economic and social needs, improve competition and promote African innovation. As in countries all over the world, policymakers will need to review and renew institutional arrangements for the governance of the data economy. Specialised regulators such as data or information regulators are required to deal with new issues of data governance, and both new and established regulators will have to engage in high levels of national and regional coordination. To ensure the African single market becomes operational, regulatory harmonisation is also essential for the integration of markets together with common online payment systems and cross-border trade facilitation and standardised cross-border taxation and duties. African states will need to caucus and develop common positions to secure more favourable outcomes in forums of global governance to better serve African interests.

Transversal digital and data policy can manage the important interplay between competition, trade and taxation in a data economy. This presents an opportunity for African states to coordinate sectoral policies to support a flourishing data economy. For many African countries, a risk that needs to be mitigated early on is the tendency towards market concentration and unequal wealth creation due to indirect network effects associated with economies of scale and scope. Data-driven digital markets are prone to 'winner takes all' outcomes. Amongst other factors, hyper-globalisation and digital interdependence contribute to monopolisation. This ultimately affects local competition and inhibits the global competitiveness of domestic data ecosystems. The challenges of market concentration, digital interdependence, and unequal distribution of wealth, particularly from base erosion and profit shifting, create the scope for incentives that encourage greater integration between mutual reinforcing priorities for usually siloed policy strategies in competition, trade and tax.

Because of the increasing importance of regional and global governance, regional economic communities have an important role to play in the implementation of regional data policy through model laws and in supporting institutional- and human- capacity building.

Within the context of the African data ecosystem, **aligning the public policy objectives of taxation and data policy, particularly in the context of enabling the Single Digital Market, has been an intractable policy challenge** for many countries. Recent legislative and policy measures introduced by a number of African countries, within the context of the several multilateral and unilateral efforts at taxing the digital economy, may not be conducive to either the creation of a single market or to accessing international resources to realise global public goods and meet some of the preconditions for a competitive data economy on the continent. Tapping into new sources of tax revenue might allow African countries to eliminate excise duties on social networking and data services, reducing distortions to both the local market and the global tax system. The harmonisation of the tax regime for digital goods and services at the regional level, and alignment at the global level, may mitigate the risks associated with small data economies being unable to generate significant value and compete in global markets. These small data economies are typically unable to contribute to the scale and scope required for data-driven value creation and work with limited tax bases.

Legal clarity and certainty on emerging data issues are necessary for scaffolding a trusted and sustainable digital transformation. A global challenge is that the nature of data flows and digital infrastructure threatens domestic data sovereignty. To exert control of data to safe-guard sovereignty requires both infrastructure and law, but also the technical capacity to do so in a manner that can build trust. Transversal policies provide an opportunity for certainty on issues such as data ownership or custodianship and accompanying rights while establishing a comprehensive system of oversight over accessing and acquiring, and the analysis, storage, and dissemination of both personal and non-personal data. Ensuring consumer protection while enabling innovation is equally key to economic development and inclusion. Moreover, because different sectoral legal approaches serve different interests, countries are afforded the opportunity to re-invent a harmonised legal system that adequately balances corporate interests and relevant digital rights.

Creating **integrated and interoperable national data systems** in response to the emerging challenges enhances efficiencies and enables greater transparency and accountability. A common challenge found across the world is that when **data is of poor quality or not interoperable**, it limits the capacity of firms and the public sector to engage in the sharing and analytics that can provide economic and social value to data. Insufficient avenues for access and limited commitment to open government data, amongst others, also impede an environment that fosters a strong data economy. **The provision of good data requires building demand for data across institutional sites** (i.e. public sector, institutions and firms etc.). Extracting value from data requires not just control but analytical and technical capacity developed in the public, private and other sectors.

SMART AFRICA - DIGITAL IDENTITY

In 2020, Benin championed a Smart Africa flagship project to develop the Digital Identity Blueprint, which was adopted by the Smart Arica Board, including its 32 Member States, the AU and the ITU, with the support of a range of other multilateral organisations and donors. The Blueprint proposes SATA as a platform to facilitate the trusted recognition of digital IDs between a range of actors through federated certification mechanisms. Pilot projects of SATA are anticipated to take place among Benin, Rwanda, Tunisia, and other Smart Africa Member States. SATA will serve as an agile and adaptable solution to enable interoperability between various public and private identity schemes on the continent.

Considering the specific African context and the slow pace of harmonisation efforts, the federated approach of SATA should allow for unilateral recognition of adequate legal frameworks by the African States, with support from a central and trusted certification authority. For this purpose, States need to strengthen their enforcement capacities, in particular, the capacities of data protection authorities in monitoring and approving crossborder data transfers. The proposed framework will embrace state of the art technologies and be respectful of the countries' legislations and regulations. Governments should not be obliged to use specific technologies. The use of open standards and norms should guarantee a large diversity of technological choices by the States.

Despite several countries introducing digital identification systems, pervasive and interoperable digital identification systems remain a major social and economic challenge on the continent. Digital identification systems enable identification for the purpose of transacting and interacting in a trusted data ecosystem. Foundational and functional identity facilitates digital services, but full coverage of foundational identity, in particular, remains both a social and economic challenge. The emerging regional frameworks on digital identity are starting to engage with this challenge directly. There are opportunities for decentralised, functional identity to be embedded in data protection frameworks. These may provide functional identity while reducing the risks associated with personal data.

Another major challenge in this regard is the unevenness of economic and social data and particularly digital indicators in many countries, to inform evidence-based policy formulation and to provide an accurate picture to global public databases such as within the UN statistical system. With the recognition of the strategic value of data, **priority needs to be given to the collection and storage of quality data to realise public value** and reduce existing information and associated power asymmetries within the public sector, between the public and private sector, and between both public and private sectors and citizens and consumers.

African countries face several well-documented and interrelated challenges with respect to their uneven levels of digital readiness (International Telecommunication Union, 2019; World Economic Forum, 2016) that variably impact their ability to respond to national and global challenges. These include the siloed development of policies and legislation, challenges around regional harmonisation of policies, a lack of institutional capacity, the ineffectively regulated competition amongst service providers, low levels of coverage, affordability and quality of broadband connectivity (Gillwald & Mothobi, 2019; Hawthorne, 2020).

Despite the adoption of continental charters, conventions and regional economic community model laws attempting to harmonise **Africa's response to the challenges posed by digitalisation and datafication, the ratification and implementation of them has been varied**. Getting wider adoption of the digital underpinnings for continental initiatives, such as AfCFTA, will be essential to realising the benefits of greater economic cooperation. Standardised rules on cross-border flows are a prerequisite for the anticipated benefits of AfCFTA being realised. This can be done by using the operationalisation of the Agreement to facilitate better crossborder data interoperability and provide a harmonised continental approach to the data-driven digital economy. This can be done in a way that supports the socioeconomic benefits of digital trade and e-commerce while ensuring that sensitive information remains secure and the relevant regulations on personal data protection are respected.

In response to previous waves of technological, and associated economic, regulatory and social innovation, **African countries have tended to be standard takers rather than standard makers**. Multilateral organisations, from the OECD to the World Intellectual Property Organisation and the WorldTrade Organisation, are reacting to the challenges of global data governance. Although Africa and African countries have, with some exceptions, not led global digital policies, there is an opportunity to change this. Multilateral, plurilateral and bilateral trade pressures to enable data flow with few restrictions are matched with pressures to concede intellectual property rights over data so that African countries face the prospect of data being both exploited and appropriated. In the absence of common Policy and commitment to common standards across the continent, it is difficult for most African countries to escape the currents of rapidly changing global dynamics. Therefore, coordinated action by and for Africa is required to collectively release and unlock the huge and transformative potential of data to develop an inclusive and sustainable digital economy and modern society in Africa.

INNOVATION IN DATA COMMUNITIES USE CASE

Typically cited examples of success in open data innovation are the emergence of particular innovation hubs across the region, chiefly in urban areas. Innovation hubs, as advocated elsewhere, can certainly be a site for social and economical open data successes; yet there are examples of open data innovation that can occur more organically just by the provision of quality open government data being made available. These can be driven by the needs of specific sectors – so, for example, in agriculture, iCow was an app launched by a Kenyan entrepreneur that helped improve yields on cows for individual farmers by 100%. Other innovations in agriculture more centrally involving open data include in Ghana, Farmerline and Esoko. Innovative firms can arise from open data, like the South African examples of OpenUp (Cape Town) and Open Cities Lab (Durban), which are socially-focused enterprises both driven by open data. Ushahidi is an organisation (and software-as-a-service company) centred around an opensource platform, which integrates crowd-sourced open data and maps it, and has been used to incredible social and governance effect in elections monitoring and crisis response throughout the region. Open data can have direct public cost savings as a result of innovations which emerge from data initiatives, creating a virtuous cycle: in an early partnership between OpenUp (then Code for South Africa) and the Southern African Programme on Access to Medicines and Diagnostics, a tool developed on open data on medicine prices demonstrated to the Namibian government differentiations between pricing it was receiving on the drug Nifedipine, which after renegotiation led them to a direct cost saving of USD 1 billion a year.

5. DATA POLICY FRAMEWORK

Data is increasingly recognised as a strategic asset, integral to policy-making, private and public sector innovation and performance management, and creating new entrepreneurial opportunities for businesses and individuals. When applied to government services, emerging technologies can generate massive amounts of digital data and significantly contribute to social progress and economic growth. The central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives. To unleash the economic and social potential of data while effectively protecting privacy, intellectual property and other policy goals, national data strategies should be formulated in the context of enhancing inter- national interoperability.

The development of the AU Data Policy Framework is necessary to realise the shared vision and common approach of an integrated African data ecosystem. This data ecosystem should support the establishment of an Africa Digital Single Market (DSM), foster intra-Africa digital trade, and boost the development of inclusive, data-enabled entrepreneurship and businesses. This is envisioned by both the AU Digital Transformation Strategy (DTS) and in the forthcoming Phase II and Phase III negotiations of the AfCFTA, where guidelines on Trade in Services and the E-commerce Protocol are expected to be established.

The Framework provides high-level principle-based guidance to member states in their development of data policy appropriate to their conditions. It identifies the key principles of effective data governance and strategies for implementation at the national, continental and international levels. This includes guidance on the appropriate institutional, administrative and technical procedures and safeguards that need to be implemented. The aim is to ensure national and sub-regional data ecosystems are built on trusted, interoperable digital infrastructure and processes which advance a harmonised continental data system that enables equitable and sustainable economic growth and development for all of Africa's people.

The Framework reaffirms the importance of the AU's commitment to stable, harmonised and predictable regulatory frameworks and contextually relevant policies to facilitate:

- incentives for efficient investment in foundational digital data infrastructure and foundational digital systems;
- institutional arrangements that permit the optimal interplay between state, markets and regulatory institutions to enable public and private value;
- building human and institutional digital capability;
- creating value from responsible data use, fostering sustainable, equitable growth, and enhancing shared prosperity from the data economy;
- improved distribution of opportunities both for the use of data services and for production and data driven-value creation within and between countries; and
- effectively regulated environments that promote fair competition and the resource allocation efficiencies that produce positive consumer welfare outcomes.

5.1. GUIDING PRINCIPLES OF THE FRAMEWORK

The Data Policy Framework needs to align with the AU values and International law to achieve greater unity and solidarity between African countries and their people, ensuring balanced and inclusive economic development, including promoting and protecting peoples' rights through the African Charter on Human and Peoples' Rights and other relevant instruments.

In the spirit of fostering regional prosperity, economic growth and development, social progress and coordinating continental efforts, the following high-level principles guide the framework.

Cooperation: African Union Member States shall cooperate in exchanging data, acknowledging data as a central input of the global economy and the importance of the interoperability of data systems to a flourishing African digital single market.

Integration: the Framework shall promote intra-Africa data flows, remove legal barriers to data flow, subject only to necessary security, human rights and data protection.

Fairness and inclusiveness: in the implementation of the Framework, Member States shall ensure it is inclusive and equitable, offering opportunities and benefits to all Africans, and in so doing, seek to redress national and global inequalities by being responsive to the voices of those marginalised by technological developments.

Trust, safety and accountability: Member States shall promote trustworthy data environments that are safe and secure, accountable to data subjects, and ethical and secure by design.

Sovereignty: Member States, AUC, RECs, African Institutions and International Organisations shall cooperate to create capacity to enable African countries to self-manage their data, take advantage of data flows and govern data appropriately.

Comprehensive and forward-looking: the framework shall enable the creation of an environment that encourages investment and innovation through the development of infrastructure, human capacity and the harmonisation of regulations and legislation.

Integrity and justice: Member States shall ensure data collection, processing and usage are just and lawful, and data should not be used to discriminate unfairly or infringe peoples' rights.

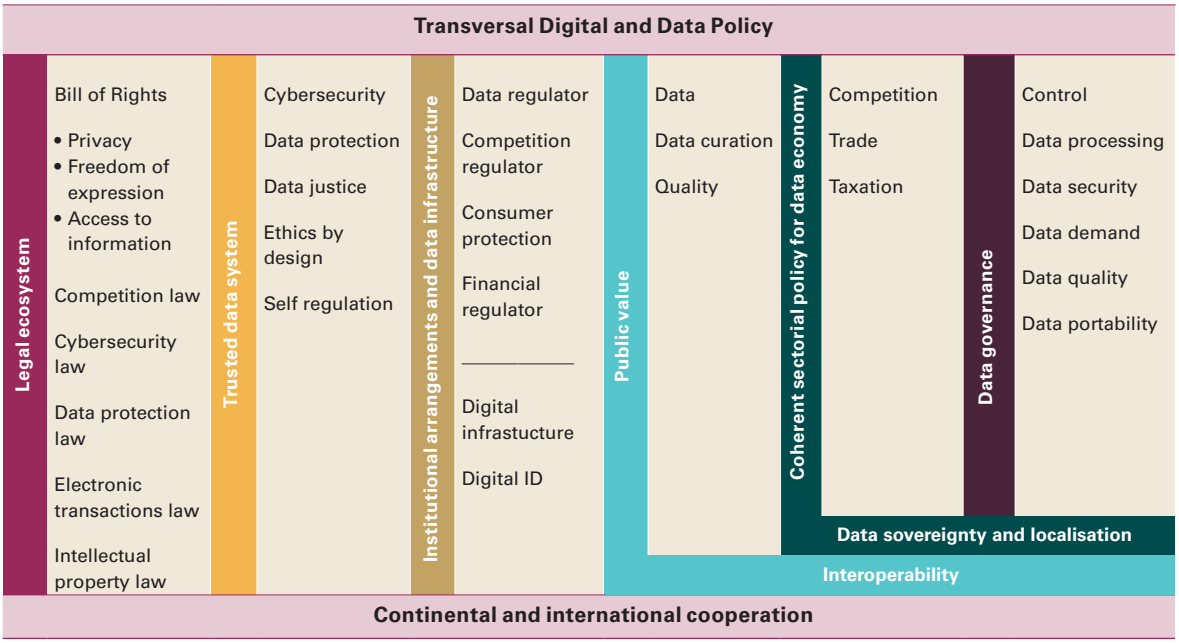
5.2 DATA DEFINITION AND CATEGORISATION

There is no agreement on how data is defined, probably as a result of the very many different types of data that are collected and used and their varying purposes and values. Without recognising these different kinds of data and the various roles they can perform, governments will not be able to effectively address issues such as personal data protection or competition. Better measurement of data and data flows and their role in production and value chains will also help support policy making.

5.2.1 PERSONAL AND NON-PERSONAL DATA

Although data, conceptually, means different things for different communities and depending on the context, an important concept which is at the core of the data protection regulation is that of personal data. Defining specific types of data as personal may help data protection authorities protect data subjects' rights more efficiently, but there are limits to this approach.

Enabling Data Policy Framework



There are numerous ways that data can be categorised that affect the appropriate policy and regulation of that category. Among the most important dimensions are public or private intent and traditional or new collection methods (UNCTAD, 2021; World Bank, 2021).

As data protection authorities start implementing personal data protection legislation, they should provide the industry with definitional clarity on how to differentiate between personal and non-personal data to enable the collection, storage and processing of data by companies compliant with data protection regulation. This will also reduce the risk of non-compliance during data collection, storage, and processing. It is important that data policies and data regulations share the same categorisations of data to ensure policy cohesion and enable compliance.

5.3 ENABLERS TO DRIVE VALUE IN THE DATA ECONOMY

Reaping the benefits from data is highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data; enhancing human, institutional, and technical capabilities to create value from data; encouraging data sharing and interoperability; and increasing legitimacy and public trust in the state to manage citizens' data in a responsible manner. Furthermore, the data infrastructure that enables an integrated data system is a key strategic asset for countries. The environment created by the interplay of elements in the data ecosystem and the nature of the relationships and non-linear processes between and within them determine the interventions to create incentives for technology investments that are required to drive growth in the data economy. These conditions are shaped by the market structure, the competitiveness of the services that arise from it, and how effectively the market is regulated.

The digital economy permeates various industries and social activities, and data policy needs to be located within the context of the wider complex and adaptive digital ecosystem. As discussed, this has implications for other policy areas, including commerce, trade and taxation. States should invest in data capabilities and complementary assets to support policy making.

Investments in data-related innovation and research and development (R&D), as well as in capabilities to harmonise standards, skills and infrastructures, can enable governments to develop better data related policies across the board. Issues of trust and ethics are equally important, while evidence-based and consultative regulations need to be prioritised.

RECOMMENDATIONS

- Member States of the African Union should promote research, development and innovation in various data related areas including, Big Data Analytics, Artificial Intelligence, Quantum Computing as well as Blockchain.
- All stakeholder groups, including governments, should build data analytic and data management capabilities to facilitate the use of quality data and trusted interoperable systems. However, it is important to remember that in many countries, the largest collective producer and collector of data is the state. Therefore many of the observations included in the discussion on data governance below have particular bearing on the actions of governments.

5.3.1 FOUNDATIONAL DATA INFRASTRUCTURE

5.3.1.1 BROADBAND AND DATA ACCESS AND USE

Defining the problem

There are access barriers to broadband infrastructure that prevent people from joining the data economy even as users. According to the ITU Broadband Commission ***Connecting Africa Through Broadband Report***:[5] "Nearly 1.1 billion new unique users must be connected to achieve universal, affordable, and good quality broadband internet access by 2030, and an estimated additional $100 billion would be needed to reach this goal over the next decade."

5 *https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf*

Despite this and a myriad of contextual constraints, Africa has a vantage position to evolve an innovative data ecosystem, being less hampered by legacy data infrastructure and having a relatively lower spectrum utilisation and congestion levels (Saint & Garba, 2016). While fixed broadband penetration in the region is less than one per cent, mobile internet is more ubiquitous with a lower adoption cost.[6] Therefore, the evolution of Africa's data ecosystem will primarily be enabled by mobile broadband networks.

RECOMMENDATIONS

To accelerate the domestication of the framework, there should be a massive robust digital infrastructure roll-out across AU members along with sufficient capacity. Member states should prioritise attaining meaningful connectivity and affordable internet that onboards more users and drives up demand for infrastructure services. For a more effective uptake and utilisation of data in the region, complementary infrastructure deficits which limit the utility of data needs to be addressed.

→ ACTIONS

Member States will need to evolve policies that:

- proscribe prohibitive 'right of way' broadband cable fees and support infrastructure sharing;
- prevent anti-competitive practices arising from dominance in infrastructure markets;
- invest in public Wi-Fi and complementary technologies;
- adopt innovative spectrum utilisation techniques such as dynamic spectrum allocation and access, and the leverage of digital dividend (spectrum bands largely expedited by the analogue to digital broadcasting migration) to expand broadband access for underserved rural areas;
- promote the transition and adoption of IPv6[7], as IPv4 resources become more depleted globally;
- invest in national backbone and crossborder connectivity infrastructure such as Internet Exchange Points (IXPs) at both national and regional levels to leverage available international bandwidth, lower internet access cost and enhance data access speeds within the region; and
- leverage innovative models for data infrastructure funding.

6 ICT Data and Statistics Division, Telecommunication Development Bureau, "ICT facts and figures 2016," International Telecommunication Union, Geneva, Report, 2016.

7 Internet Protocol version 6 is the most recent version of the Internet Protocol that provides an identification and location system for devices on networks and routes traffic across the Internet.

5.3.1.2 DATA INFRASTRUCTURE

Defining the problem

Foundational data infrastructure that facilitates data systems and allows for the sharing, gathering, and storing of big data, or the manipulation of existing data sources, will impact how governments are able to respond to the challenges related to data availability, quality and interoperability, and approach considerations related to legitimacy and public trust.

Foundational data infrastructure refers to a wide range of technologies that facilitate the in- tensive use of quality data, including hard and soft infrastructure[8] addressing existing "traditional" ICT infrastructure deficits that will have to be made in parallel with creating architecture to support increased datafication. It also includes infrastructure resources such as Digital Identification to enable secure online transactions and presence. This Framework will focus on three data infrastructure aspects that require mutually reinforcing policy considerations and also influence data governance: cloud services, big data and platformisation.

Developing public data value from cloud-computing infrastructure and software that complements big data processing and analytics will need to be informed by well-developed security and trust models for cloud storage and processing of sensitive or proprietary data, API management, and support of equitable data ecosystems markets. Beyond the digital infrastructure inadequacies in many governments – including weak enablers to accommodate an environment for supply and consumption of cloud services – African countries face a multitude of challenges in responding to infrastructure requirements as this infrastructure is often supplied by and procured from private Foreign Service providers.

This implies that to leverage opportunities associated with digital transformation, other challenges such as intermediary liabilities, jurisdiction boundaries, interoperability, and sovereignty issues, to name a few, will need to be considered. These challenges underscore the need for collaboration and partnerships in many African data ecosystems to strengthen fundamental enablers of successful data-driven activity markets across different points in the data value chain, regardless of domestic digital maturity and endowments.

The technological, organisational, legal and commercial regulations and legislation in place will impact the efficiency of the shared infrastructure to facilitate various data market participants with access required to operate in the data market. Data ecosystems should be able to support various application domains and allow data exchange and integration at different stages of the data value cycle while preserving data provenance and integrity.

CLOUD SERVICES

It is useful for policy purposes to distinguish between "cloud services" and "cloud-based services." The main benefit offered by cloud services is cost savings through enhanced systems efficiency. For example, resource-constrained public sector and small, medium and micro enterprises (SMMEs) can reduce capital expenditure on IT equipment, including internal servers, networking equipment, storage resources and software, by shifting to a utility-based cloud services model.

8 See Annex for full definition

Interoperability in cloud provision is a critical factor as this allows flexibility and enables users to switch between one cloud provider and the other. Other benefits of cloud computing include reduced spending on energy consumption as well as lower demand for systems management and maintenance by shifting the management of IT resources to third parties. As a result, funds can be shifted to customer-facing activities and better public service delivery. However, as there are certain factors that support a conducive environment for cloud-based services, making provisions to adopt new technologies must be done in parallel with addressing structural digital divide challenges (human capital, infrastructure, etc.). These processes must be mutually reinforcing and suited to Member States' economic realities. Developing data value from cloud-computing infrastructure and software that complements big data processing and analytics will need to be informed by well-developed security and trust models for cloud storage and processing of sensitive/proprietary data, API management, and support of equitable data markets.

BIG DATA

Massive amounts of data are being produced - including as by-products of other activities (such as by social networking platforms when they create profiles of their users for advertisers) - and used for the development of products, services and entirely new forms of businesses, with the potential to generate substantial efficiency and productivity gains. This also holds potential for the public sector, which sits on vast amounts of data that could be used for 'big data' analytics by improving decision-making, forecasting and allowing for better consumer segmentation and targeting. The advantages of scale and scope related to network effects have produced near-monopoly positions, which have been further enhanced through mergers of smaller, new providers of services that do not at first glance appear to be in the same market, such as Facebook and WhatsApp. This makes it nearly impossible for local players to compete (Arntz et al., 2016).

PLATFORMISATION

Datafication has also created entirely new business models and modes of value creation and value extraction. One of these is 'platformisation', which facilitates transactions and networking as well as information exchange, aggregating multiple sellers and buyers on a single platform.

With digital trade and e-commerce platforms increasingly underpinning global and crossborder activity, the integration of traditionally distinct areas of regulation and policy priorities has become increasingly important and intertwined across geographical boundaries. However, policies such as data localisation will not be plausible without the necessary structural and institutional requirements for their effective evolution and implementation, in particular with reference to digital capabilities (Andreoni & Tregenna, 2020).

RECOMMENDATIONS

- Using data as a tool to enhance public interests will require states to strengthen domestic data infrastructure and will need robust stakeholder engagement at the national, regional and global levels. Developing comprehensive enabling data policy frameworks should be accompanied by time-sensitive implementation strategies across different domestic mandates to ensure accountability and transparency.
- Member states should prioritise resources to ensure that there are incentives to increase investments in digital infrastructure, data platforms, and software capabilities to leverage big data. Data infrastructure investments must support the digital social contract. State efforts to enhance Interoperability, quality, and public administration of data must also complement and enhance public digital systems such as digital IDs, digital payments, and open data flows, as far as possible. The appropriate infrastructure is also a necessary component of any interoperable, integrated data-sharing system. Furthermore, reusing or repurposing data typically requires well-functioning data systems that facilitate the safe flow of data in machine-readable formats that make the data valuable to many users.

→ ACTIONS

- As opposed to focusing on the significant upfront investment to replace depreciating legacy ICT equipment, Member States should leverage economies of scale and scope to adopt infrastructure that supports facilitating benefits offered by cloud services and other new technologies that support data value creation.
- Tax, trade (including investment and innovation) and competition policies must be coherent, complementary, and adapted to the data-driven digital economy, particularly to inform infrastructure development strategies.
- Member states must ensure local firms participate in value chains of foreign software as a service (SaaS), infrastructure-as-a-service (IaaS) and platforms-as-a-service (PaaS) providers for state procurement and create incentives to have local SMMEs in data value chains across industries. This can be done by ensuring tax, trade (including investment and innovation), and competition policies are coherent, complementary, and adapted to the data driven digital economy.
- Adopt more sustainable electricity generation models domestically and across the region, to ensure foundational digital infrastructure supports sustainable domestic and crossborder data activities that have fewer extractive impacts on the natural environment.

DATA GOVERNANCE

- Creating data portability rights - including for non-personal data, to make it easier for customers of cloud services to switch between providers.
- Develop contractual standards for public organisations (that can be used by SMEs too) that protect their rights to access, retrieve, delete, etc., the data (including non-personal, again) that is processed by cloud providers.
- Develop Fair, Reasonable and Non-Discriminatory (FRAND) licensing obligations for platforms and cloud providers who have access to datasets that become a vital resource to enter a market.

5.3.1.3 DIGITAL ID

While the African continent hosts the highest percentage of people without legal identity and subsequently uncovered by civil registration and denied essential social services offered by states such as healthcare, basic education or food services[9], the digital economy offers opportunities to redress inequalities such as socio-economic and structural exclusions suffered by minority groups on the continent.

Digital ID, as a form of personal data expression, must be constructed and implemented cohesively in line with overarching data governance frameworks. Digital ID is facilitative for both private and public sector purposes within a data economy, but demands a robust trust-guided framework to mitigate against the potential harms like personal data abuse, exclusion, or discrimination based on inaccurate (or unfair) data representation, that may accompany such initiatives. Further, although private-public partnerships have the potential to expand the public delivery of state services and boost socio-entrepreneurial innovation, such collaborations can potentially exacerbate inequality (through data misuse) on top of the harms mentioned above. The frameworks adopted by existing national identity authorities/ agencies should therefore be revised to reflect these opportunities, risks and harms.

RECOMMENDATIONS

A fair and trustworthy digital identification system is a central prerequisite to combining and repurposing public administrative data with other types of data across various use cases. Regional data policy activities should align with those occurring under concurrent Digital ID activities. Public sector digital identity initiatives must remain guided by data governance frameworks, whether foundational or functional[10].

5.3.2 CREATING LEGITIMATE AND TRUSTWORTHY DATA SYSTEMS

Defining the problem

A trusted data environment requires users to trust the entire political and economic system underpinning the data economy. Fundamental aspects of this kind of system include safeguarding basic human rights through the rule of law; institutional arrangements and regulations that are established through consultative and transparent processes; and requiring that institutions responsible for overseeing the use of data, as well as public and private data producers, are accountable for the use of public and personal data. Inclusion and diversity of people who manage and oversee data environments, for example, through gender diverse teams, is important to build trust. Several African countries already have many of these aspects. The continental challenge is to ensure that all countries have all the necessary aspects and that these are appropriately adapted to rapidly evolving data technological and economic challenges. The framework sets out all the essential components of legitimate and trustworthy data systems to enable benchmarking by countries as to whether they have some or all of the components fully in place.

9 See *https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity*

10 The African Union Commission is developing an Interoperability Framework for Digital ID that will provide a detailed set of recommendations to member states on introducing and safeguarding digital ID systems.

Trust in data transactions, statistical data, and data-based decision making must therefore be sustained by a transparent and robust legal and regulatory framework that simultaneously safeguards against data harms and supports enablers that facilitate access to data, data sharing, and data alterations in a responsible manner. A strong trust framework, and the institutional capacity to support this framework, will allow governments to create value from data, minimise public-private data asymmetries, and curb uncompetitive behaviour in data ecosystems (Macmillan, 2020).

In this context of building a trusted digital ecosystem, three key interrelated areas need specific consideration: cybersecurity, cybercrime, and data protection. The role of ethical design and positive regulation to ensure justice outcomes is also worth highlighting.

5.3.2.1 CYBERSECURITY

As technology evolves and disruptive technologies are adopted, new threats and unwanted risks are created. This not only impacts assets, infrastructures and networks but also economies, societies, and people, with the most vulnerable being the most affected. Because of this, the use actors make of disruptive technologies and the public and private sector norms, rules, and practices to govern security may impact people's fundamental rights of equity, dignity and security.

While policies, laws and regulations can be tools used to push back against threats and protect people from risks, they can also be used to normalise or legitimise systems of oppression and repression. Therefore, any cyber policy response aimed at strengthening data security should consider elements of proportionality (including the legality, legitimate aim, necessity, and adequacy) as the most important requirement that must be satisfied in any form of limitation of online human rights.

5.3.2.2 CYBERCRIME

The data ecosystem highlights both the opportunities and risks of a vast network of linked public and private systems. Due to the transnational nature of cybercrime and cyber operations, policy on data security is mostly shaped in multilateral global or regional forums. While African participation in these forums has increased, the involvement of non-state African actors is still limited. Moreover, an emerging policy challenge is to evaluate what capacity is needed nationally to implement regionally and globally agreed conventions on cybercrime and voluntary and non-binding cyber norms.[11]

5.3.2.3 DATA PROTECTION

The risks of unlawful possession of processed data are borne chiefly by data subjects themselves and not the entity extracting value. Because of this, mechanisms and principles for mitigating privacy risks must be central to any national and regional policy frameworks that seek to harness the potential of data economies.

11 Deficits in implementation capacity have been observed across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organisations and technologies.

While this requires developing sound data governance institutions and laws, these laws also need to be responsive to the particular contexts in which they are being implemented. These include consideration of the socio-economic and technological realities and capacities of the public. Stated differently, a data policy framework needs to develop policy and regulation that is able to acknowledge the realities of a citizen's capabilities and functionalities, along with the risks that accompany digital developments and lead to the unequal distribution of benefits and harms (Sen, 2001; van der Spuy, 2021).

For example, with significant numbers of people digitally and otherwise illiterate in Africa, digital mechanisms of informed consent may not be sufficient to protect the rights of people. There is a risk that the digital means of obtaining consent, such as selecting a button linked to a lengthy legal set of terms, does not actually amount to informed consent because the action that is meant to constitute consent may not be an informed act or understood at all by the person doing it. Other means of data stewardship, such as data trusts which are emerging globally and that ensure that the rights of people over their data are upheld, are discussed below. Similarly, the dominant framing of data governance is generally equated with data protection and data protection with privacy. It is largely understood as an individual right and individual challenge. However, there are issues of community and collective rights that may be important to the foreground in dealing with issues of public interest.

5.3.2.4 DATA JUSTICE

The concept of data justice promotes a broader view than data protection. While a rights-preserving data policy framework will be essential to safeguarding the rights of people, the individualised notions of privacy in current data protection normative frameworks may not be sufficient to ensure more equitable inclusion in a trustworthy data economy. Data justice is a concept that has been gaining traction in response to the exponential adoption of data-driven technologies worldwide, particularly artificial intelligence (GPAI 2021[12], Tyler, 2019). It seeks to ensure that the increasing reliance on data, especially for automated decision-making, does not perpetuate historical injustices and structural inequalities. It addresses the question of fairness in response to the degree to which people are visible, represented and underrepresented and discriminated against as an outcome of their production of digital data.

Data justice also extends beyond notions of political rights and justice to social and economic rights and regulation that is necessary to redress inequities and enable people to exercise their rights. There are many other areas of data governance in relation to data availability, accessibility, usability, and integrity that impact equitable inclusion. If these are regulated in the public interest, they could contribute to a better distribution of the opportunities not only for the consumption of data services but for the production of services.

12 The Global Partnership on Artificial Intelligence has developed a project which aims to fill a gap in data justice research and practice that provides a frame to help practitioners and users to move beyond understanding data governance narrowly as a compliance matter of individualised privacy or ethical design. The project seeks to include considerations of equity and justice in terms of access to and visibility and representation in data used in the development of AI/ML systems. *https://gpai.ai/projects/data-governance/data-justice/*

RECOMMENDATIONS

Member States should seek to establish a reliable and trustworthy data environment through cybersecurity, protection of personal data, the rule of law and capable, responsive, and accountable institutions. They should establish trust in data governance and a national data system by ensuring legitimacy throughout the system. This includes systems and standards that guarantee public and private sector compliance, the government itself adhering to personal data protection rules, and government sharing public data.

→ ACTIONS

- Safeguard basic human rights in the digital environment through the rule of law.
- Ensure institutional arrangements and regulations are established only through inclusive, consultative and transparent processes.
- Ensure institutions responsible for overseeing the use of data, as well as public and private data producers, are accountable for the use of public and personal data to those whose data is used.
- Strengthen cooperation with other DPAs to ensure sufficient safeguard and reciprocal protection of personal data as well as individual and collective digital rights across the continent.
- Strengthen Mutual Legal Assistance Agreements and activities across states for the investigation and prosecution of cybercrimes.
- Ensure institutions responsible for overseeing the use of personal data are empowered to have powers of entry and inspection for purposes of enforcement of privacy and data protection laws and regulations.
- Further ensure institutions responsible for overseeing the use of personal data have the following corrective powers in relation to correcting infringement of aspects of misuse and abuse of personal data:
    - Issue warnings to a data controller or data processor that intended processing operations are likely to infringe provisions of the relevant data protection laws and regulations.
    - Issue reprimands to a data controller or a data processor where processing operations infringe provisions of the relevant data protection laws and regulations.
    - Order a data controller to communicate a personal data breach to affected data subjects.
    - Impose a temporary or definitive limitation, including a ban on personal data processing.
    - Order the suspension of data flows to a recipient in a third country or to an inter- national organisation that does not provide adequate protection similar to that of the data exporting country.
- Institutions responsible for overseeing the use of personal data should be empowered to either assist or seek a court's indulgence to assist a person who has suffered material damage as a result of an infringement of their personal data to receive compensation from a data controller or data processor for the damage suffered.

5.3.2.5 DATA ETHICS

An important way to reduce risk and mitigate harm through the application of new data technologies is through contextually appropriate data ethics. Codes of ethics should be developed by all stakeholder groups working with data, including researchers, industry associations and data experts. These codes of ethics are valuable for guiding the use of data and the processes of designing and implementing data systems, including embedding them in computer code in the case of developing algorithms.

However, codes of ethics have been criticised as representing the views of limited demographics, mostly defined by corporations and technologists. Ethical codes can also relieve corporations of regulatory accountability when used as a form of self-regulation and can be insufficient in enabling the fundamental rights of people when using technology.

Working together enables trustworthy data systems by providing the kind of practical and technical details that support laws since the latter are usually of more general application than specific ethical codes but also sometimes less quickly adaptable to new technologies. Ethics operate prospectively, enabling ethical design, while laws tend to be enacted and operate retrospectively. Ethical codes of conduct should embody digital rights and support compliance with international and national law.

The AU supports efforts to make ethical codes more inclusive through processes that take into account the voices of citizens, consumers, marginalised and underrepresented people. Nevertheless, mechanisms for ensuring adherence to ethical codes, as well as for updating those codes, are underdeveloped.

Human rights treaties – as the product of consensus processes between the legitimate representatives of citizens – enjoy greater legitimacy than codes of ethics and are legally enforceable when enacted at the national level and through regional adjudication. While these treaties sometimes do not have the specificity necessary for data ecosystems, digital rights, which have been formulated variously by civil society amongst others and draw on the human rights framework, provide the kind of specificity that can be drawn on. Although existing human rights bodies and adjudicators have the requisite capacity to develop rights in response to data issues, their legal mandates may not sufficiently empower them to do so.

RECOMMENDATIONS

- Member States should encourage the development and adherence to codes of ethics that are responsive to the African context and which promote digital and human rights. This means people who work with data, regardless of the sector they work in, must respect rights and adhere to these ethical standards. These codes ought to take note of gender considerations within the African context, ensuring they reduce harm and exclusion of women and girls. It is impractical for member states to legislate that all technologies and technology providers dealing with data adhere to particular ethical codes since many of these technologies are designed, built and operated in other jurisdictions. Member States should, however, encourage the adoption of these codes of ethics by themselves, making use only of technologies and technology providers that adhere to approved codes of ethical conduct.
- Besides any regulatory or judicial legal recourse available in a country, there is also scope to consider empowering existing human rights mechanisms at the national, regional and continental levels to adjudicate uses of data.

→ **ACTIONS**

- The data industry and research communities using data need to formulate and implement codes of practice, including the principles of responsibility and ethics by design through processes that include those whose data is affected.
- Member States must require rights-compliant ethical frameworks in public procurement processes.
- Members should include the assessment of data codes of ethics in the mandates of existing human rights bodies such as Human Rights Commissions.

5.3.3 INSTITUTIONAL ARRANGEMENTS FOR REGULATION OF COMPLEX ADAPTIVE SYSTEMS

The following are key considerations in aligning the regulatory context in a country with the requirements of a data economy. The regulation in data economies requires future-facing agile regulatory decisions in the face of uncertainty. Thus, regulators require both the mandate and the confidence to regulate proactively. Complex adaptive regulation responds not only to the challenges of rapid change and uncertainty but the complexity of data ecosystems characterised by multi-factor dynamics.

5.3.3.1 BUILDING CAPACITY OF REGULATORY BODIES

Rapidly intensifying processes of digitalisation and datafication present new regulatory challenges in the traditional areas of competition and consumer protection and entirely new areas of regulation, including the protection of peoples' personal data and algorithmic governance to ensure people are not discriminated against. While the traditional principles of independence, transparency and accountability continue to inform the effective regulation and governance of data, policymakers and regulators need to develop new capacities to face the challenges.

5.3.3.2 A SHIFT AWAY FROM REGULATORY SILOS

While the different institutional endowments will determine whether existing regulators have the capabilities to manage new areas of governance, it is clear there will need to be a shift from regulation within traditional sector silos to integrated or, at the very least coordinated regulatory action. This is made possible by the development of traversal digital strategies and policies that recognise the cross-cutting nature of digitalisation and datafication. This is essential to create the necessary coordination across the various sectors of public services impacted by the data economy and to meet sector-specific data governance needs.

THE AFRICAN NETWORK OF INFORMATION REGULATORS

Provides an example of regional collaboration to establish national data regulators, raise awareness of new information and data governance, provide governance for cross-border data flows and cooperate with regulators internationally. It does this to align governance particularly in relation to the proportional and standardised response to data breaches and rights violations.

National regulators and policy makers have a role to play at the international arena. Intensify international cooperation on cross-border data flows to ensure that data localisation requirements and other restrictions on cross-border data flow do not unduly interfere with cross-border communications and the economic and societal benefits that global data networks make possible and are minimally trade-restrictive, while promoting trust.

Encourage regional and international cooperation on data privacy and cybersecurity initiatives to streamline the patchwork of data privacy and cybersecurity rules and practices into common regional or global standards and laws and allow free flow of data and digital trade (GSR, 2021).

Area of regulation	Topics of potential collaboration with the data regulator
Telecommunications	Availability and quality of foundational infrastructure to enable data services
Competition	Concentration, mergers and acquisitions, anti-competitive practice in digital and data markets but also pricing and market structure's effect on security
Consumer protection	Digital devices and services, e-commerce
Commerce/Trade	Digital taxation, e-commerce, digital services, digital financial services
Finance	Finance blockchain, cybersecurity, financial inclusion, mobile financial services, privacy
Education	Online protection, schools connectivity, availability of data for acquiring data skills

Source: Adapted from TGM 2020 in ITU World Bank 2020.

5.3.3.3 DATA REGULATOR

The capacity of sector regulators to be effective is determined, at least to some degree, by the institutional arrangements and the autonomy of regulators to implement policy. The levels of efficiency and innovation that enable the evolution of the ecosystem depend on the availability of skills and competencies of people and institutions at each node within the ecosystem to harness the benefits associated with integrated networks for economic development and social and political engagement. Developing an integrated data system at a national and regional level is also highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data, enhancing human and technical capacities to create value from data, encouraging data sharing and interoperability, and increasing legitimacy and public trust in the state to manage citizen data in a responsible manner. Creating the conditions that allow for the necessary access to data while safeguarding rights will require building institutional capacity and capabilities to optimise the potential of data and developing enforcement mechanisms.

5.3.3.4 COMPETITION

As regulators in Africa struggle to introduce and enforce traditional competition regulation, there is a danger that static competition regulation to govern dynamic and adaptive systems may inhibit innovation and damage the underlying technology that enables innovation. For example, the regulation that focuses on curbing dominance in only the app layer of the Internet could negatively impact and even harm the entire internet and its infrastructure. Regulators need to be cautions of instrumentally applying single-sided market competition rules based on static efficiency models to new data platforms and products based on dynamic efficiency that may produce innovative complementary products (such as WhatsApp) that enhance consumer welfare and choice or even offer opportunities for local competition on their platforms while being dominant in the underlying global market (Facebook).

Platforms are different from traditional operators in the markets as they are constituted by numerous relevant markets that have multiple 'sides', each with specific competition dynamics. Similarly, Over the Top (OTT) products and services can appear to be vertically integrated when in fact, they are complementary and competition enhancing. These kinds of challenges require equally adaptive regulators able to manage their complexity in the public interest.

5.3.3.5 CONSUMER PROTECTION

As consumer protection authorities are not responsible for one specific sector, in exercising their functions, they have generally relied on other sector-specific regulators. Clear, strong and enforceable rules related to data governance can provide adequate defence for digital consumer protection while creating a predictable, structured framework for doing digital business. Agile regulatory protocols and mechanisms able to adapt to rapidly changing technologies and conditions can go a long way towards enhancing trust in the digital ecosystem. These include complying with requirements related to the access to non-personal data retained by digital platforms, the transparency of certain essential algorithms used by digital services, the portability of essential data of structuring platforms, and the interoperability and maintenance of APIs (International Telecommunication Union, 2020).

A way of increasing transparency on the use of consumers' data is the creation of a transparency portal, but this is dependent on the data regulator having the resources to establish, monitor and enforce breaches. This provides people secure access to a portal where they can see the history of when and with whom their personal data was shared, enabling them to challenge data shared or used without their consent. This may not apply to certain categories of public interest data sharing of data accomplished through pseudonymising or anonymisation of the data.

RECOMMENDATIONS

AU Member States should have adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment. Data regulators should have the requisite powers to enforce compliance with data regulations, such as powers to issue warnings, penalise for breaches, award compensation for victims of data, and to cooperate with other agencies, including enforcement agencies.

→ **ACTIONS**

- Members with data regulators should assess whether the existing enforcement powers are sufficient.
- Members creating data regulators should consider a range of enforcement powers and in addressing resource constraints, how data regulators could potentially rely on other agencies for enforcement.

5.3.4 REBALANCING THE LEGAL ECOSYSTEM

Defining the problem

A number of the different but overlapping branches of law, such as data protection law, competition law, cyber security law, electronic communications and transactions law, and the different categories of intellectual property law, deal with data. However, they may conflict or contradict each other. In contrast to data protection, which applies only to data that can be related to an individual, competition regulation applies to data when control over data has an anti-competitive effect. Concentrated control over data, including data flows and data analytics implicates not only barriers to market entry but the public interest. The concentration of data, data flows and data systems substantially increase the likelihood and damage that can be caused by cyberattacks and data breaches since it leads to a single or a few points of failure that can have large scale consequences. These concerns are not within the purview of many competition authorities but should be since there are public interest concerns. Competition authorities can be mandated to avoid structural centralisation of data firms that increases society-wide risks of cyberattacks or massive-scale data breaches. Access to data is generally pro-competitive but may be in tension with other laws such as intellectual property claims over data and databases and privacy and data protection.

While it is generally accepted that raw data is not protected by any recognised property right, claims have been raised over data based on the different types of intellectual property; copyright, sui generis database protection, trade secrets and patents. None of these grant ownership over data as such. Sui generis database protection is a uniquely European Union law confined to Europe. In a few common law countries, copyright has been extended to databases and compilations of data, but even these countries have different rules, with some courts extending copyright merely for the effort of compilation while others require creativity. Copyright is intended to reward human authors, and its application to databases compiled by computers is undetermined. Disputes between competitors regarding the overuse of industry-standard databases straddle copyright and competition law. A court ruling (Discovery Ltd and Others v Liberty Group Ltd ZAGPJHC 67, 2000) offers a solution that upholds both data protection and competition: in such disputes, if the data is personal in nature, it is 'owned' by the data subject and competitors may not exclude others from accessing this information. While the application of intellectual property laws to data is still being resolved, the rights of people over their personal data should be treated as stronger than any intellectual property claim over that data because data protection is so important to building data economies.

Trade secrets may also apply to data in some circumstances but precisely which circumstances are unclear.

The application of intellectual property laws is both complicated and undetermined, but it is at least clear that claims over data based on intellectual property, even though contested, potentially jeopardise the beneficial flows of data and data protection.

Cybercrime laws prohibit the unauthorised access, use or alteration of personal data or ID systems. As reiterated throughout the policy framework, safety and security are essential to the effective implementation of the policy and a threshold, though not sufficient, requirement for building a trustworthy system. Cybercrime laws have the potential to raise the barriers of entry into the data economy. The Malabo Convention enacted by the African Union and specifically tailored for the region deals with both cybercrime and data protection. However, it is not yet in force as it awaits ratification.

Members have an opportunity to reinvent a harmonised legal system that adequately balances competing interests.

RECOMMENDATIONS

In order to ensure equitable and safe access to data for innovation and competition, member states must establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. Where necessary, existing legal instruments should be revisited regularly to ensure that they are not in conflict with one another and that they offer complementary levels of protection and obligations within member states. In accordance with their legal systems, member states should support the stream-lining of these policies at the subnational level to facilitate proper implementation at all economic levels. Intellectual property laws should be revised to clarify that they do not generally impede the flow of data or data protection.

→ ACTIONS

- Contracts that purport to give up digital rights, personal data protection and that inhibit competition should, as a general rule, be unenforceable. This can be articulated in data protection and competition regulation, which can also consider on a case-by-case basis whether the pro-competitive effects of such contracts outweigh the anticompetitive effects.
- National law reform commissions or similar expert legal institutions should investigate and consider how to harmonise different branches of laws, regulatory regimes and supervisory authorities that deal with data.
- Member States should support the update or adoption of competition law frameworks and regulations that consider the challenges of analysing competition issues, designing remedies and enforcing their powers to safeguard competition in data-driven markets, as well as building the capacity of competition regulators to implement these rules.
- Intellectual property laws should be amended to provide:
  - that if copyright applies to databases and compilations of data at all, it shall apply only to the work of human authors that exhibit originality/creativity and that the copyright extends only to the original selection and arrangement of data in a database or compilation and not to the data itself;
  - that any copyright or other intellectual property right, including trade secrets that enables control of data, does not apply to personal data;

- that any copyright or other intellectual property right, including trade secrets that enables control of data, is limited by the provisions of competition regulation and alternative rights that offer protection to local innovations not envisaged in current frameworks;
- adaptations to existing IPR regimes to leverage next frontier technologies, such as enabling AI to use data;

5.3.4.1 COLLABORATING WITH REGIONAL AND GLOBAL GOVERNANCE PROCESSES

Regulation of digital and data economies is increasingly beyond the scope of individual national regulatory authorities (NRAs). Effective regulations require that regulators collaborate with regulators in their regions and globally to ensure the realisation of the internet as a public good and its productive and rights-based use in the digital economy.

Formal regulation should leave sufficient space for self-regulation, hybrid and collaborative regulatory models and oversight mechanisms for law enforcement. The range of tools and remedies at hand for regulators to explore is wide, from incentives and rewards through forbearance to targeted obligations. Regulatory instruments have expanded to cover regulatory sandboxes, ethical frameworks, technology roadmaps, regulatory impact assessments, multi-varied research and big data simulation to determine the most balanced, proportionate and fair regulatory response. AI, IoT and online disinformation are some of the complex issues waiting to be addressed (International Telecommunication Union, 2020).

5.3.4.2 CONSULTATIVE AND EVIDENCE-BASED REGULATIONS

In order to harness the expertise of stakeholders, regulation should also be the result of consultative multi-stakeholder processes focused on the public interest. They should also be evidence-based and contextual. Improved administrative data through better collection and analysis and on which regulators can make decisions would greatly enhance decision-making within agencies. This would also enable them to provide greater certainty to stakeholders within a flexible and adaptive framework, enhancing their credibility (World Bank & ITU, 2020).

RECOMMENDATIONS

- In creating institutional arrangements, Member States should clearly distinguish between the roles of the state as policy maker and the regulator, which should be sufficiently independent of the state and industry, so as to implement policy in the public interest and the service providers and platforms operators.
- Regulatory institutions should be established on principles of autonomy, transparency, and accountability to avoid state and regulatory capture. Regulators should undertake regulatory Impact Assessments at an early stage of regulation to implement the best approaches that balance regulation and economic growth. Regulators should publish policy performance, and regulatory efforts to improve regulatory strategies across states, including public participation reports on emerging regulations. Regulators also need to be self-financed or financed through parliamentary appropriation to enable financial independence. Regulatory decisions should be based on good data and harness private sector and civil society knowledge through public consultation. Competition and sector regulators should avoid instrumental competition regulation by adopting dynamic efficiency rather than static efficiency models.

→ **ACTIONS**

- Clearly distinguish between the roles of the state as policy maker and the regulator, which should be sufficiently independent of the state and industry, so as to implement policy in the public interest.
- Create or maintain competition authorities to deal with dominance in the market and concentration through mergers and acquisitions.
- Implement clear procedures for co-jurisdiction between sector and competition authorities to ensure the coordinated regulation of the digital infrastructure and services sector and to avoid 'forum-shopping'.
- Data regulators should collaborate at the regional and continental levels to harmonise their frameworks, particularly in support of the AfCFTA.
- Those subject to decisions of regulatory authorities should have clear mechanisms of appeal and redress heard by a different body from the regulator, making the decisions in line with the rules of natural justice and fair administrative action.

5.3.5 CREATING PUBLIC VALUE

Defining the problem

Having data without human capacity, sufficient control, or incentives for value is much the same as not having data. These constraints apply to many African countries. There are also challenges in fostering a data-driven public sector. Data valuation is highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data, enhancing human, institutional, and technical capabilities to create value from data, encouraging data sharing and interoperability, and increasing legitimacy and public trust in the state to manage citizens' data in a responsible manner. Furthermore, the data infrastructure that enables an integrated data system is a key strategic asset for countries. The environment created by the interplay of elements in the data ecosystem and the nature of the relationships and non-linear processes between and within them determine the interventions to create incentives for technology investments that are required to drive growth in the data economy. These conditions are shaped by the market structure, the competitiveness of the services that arise from it, and how effectively the market is regulated.

5.3.5.1 PUBLIC SECTOR CAPACITY

The public sector's digital and data capabilities are a key determinant of service delivery in many priority areas. Creating the conditions for data to be optimised in the public sector to meet the needs of citizens more effectively are necessary conditions for social and economic inclusion. However, there are multidimensional inequalities and overlapping policy inefficiencies that limit human and institutional capabilities to enhance a culture of digital entrepreneurship, foster inclusive digital innovation communities, and promote fair and equitable data ecosystems markets — where Africans with varying capabilities can work with frontier digital technologies and contribute to the data value cycle or participate in data value chains in a more inclusive manner.

For a data-driven public sector to materialise, the civil service needs to be revamped with leadership and political will to ensure that public servants at all levels are equipped with a basic understanding of how data can be used to enhance service delivery and policy implementation. Furthermore, a data-driven public sector requires a common approach and a data infrastructure architectural model that can address potential cross-industry, cross-application, and cross-platform integration and exchange of data and data-driven applications.

5.3.5.2 PUBLIC DATA CURATION

The public sector is mandated to manage key economic development data. This includes statistical data and economic indicators used for reporting purposes with multilateral institutions and administrative data, such as Digital IDs. This is often anonymised and combined with other data across various use cases that range from commercial hyper-personalisation, such as credit worthiness, to public interest in social grants and disaster management.

Effective data-driven value creation in the public sector requires a coherent transversal approach to understanding the need for data and how it can be used to enhance socioeconomic efforts and public service delivery. A lack of general consensus on data governance frameworks that are supplemented by the appropriate sector best practices (depending on the use case) can pose a significant threat to interoperability, open data sharing efforts, and create limitations on the extent to which governments can embrace practices to create value from data in the public sector. Facilitating interoperability is a critical issue. Open data systems require a common approach and data infrastructure models that can address potential cross-industry, cross-application and cross-platform integration and exchange of machine-readable data and data-driven applications. Data sharing and interoperability do not only depend on data systems, technical protocols, infrastructure, or governance — they also require leadership and political will for consensus around an approach to interoperability that is supported and adopted across various public sector mandates.

In the public sector, data is often used to enhance the social contract and mitigate information asymmetries in policymaking, monitor intervention impacts and service delivery, including deciding how government resources are allocated. Anonymised public data can be combined with other datasets for commercial use to lower market entry costs, disrupt industries, enhance efficiency, and facilitate the development of innovations, products, information, and opportunities that can be available online without the limitations of geographical and physical boundaries. However, institutions that curate public data face various challenges, which are discussed below.

5.3.5.3 ENSURING QUALITY AND RELEVANCE OF PUBLIC SECTOR DATA

There are several theories or models for studying data quality challenges. As a result, defining data quality determinants and relevance from a technical perspective are informed by a wide range of application scenarios such as the data availability, type of data, domain characteristics, and how and why the data is used and/or collected, amongst others (Wang et al., 2019; Wook et al., 2021). For instance, in health research, a data quality assessment framework would consist of 30 or more data quality indicators, while for sensor data quality collected from IoT devices, only two dimensions may be considered (Schmidt et al., 2021; Teh et al., 2020). Furthermore, the advent of big data analytics, including ML and technical capabilities beyond data science such as data engineering and data management, means that data is pro- cessed (cleaned) and can enhance the quality of the collected data, making it available for a wide variety of use cases (Wook et al., 2021, Svolba, 2019).

With education systems not adapted to the digital reality and, therefore, poor STEM and ICT and digital skills means, there is limited existing talent to fully make use of big data analysis techniques and data science to create value from accumulated or produced data. Inadequate data curation and data sharing across the public sector inhibit the development of integrated data systems and the benefits associated with them.

RECOMMENDATIONS

Given the breakneck pace of digitalisation, as the major steward of citizen data, the public sector needs to be adequately resourced to leverage data to enhance public interests in a manner that safeguards citizens. One way this can be done is through targeted training and knowledge co-creation initiatives with other international agencies — under-resourced institutions that curate public data already house existing analytical professions (statistics, quantitative economics, operational research and social research etc.,). These existing resources can be upskilled and utilised to enhance data value creation in the public sector context.

Member states should commit to a whole government approach to using data across various policy priorities, and public entities that curate various types of data must be given clear mandates and be resourced with technical, institutional, and human capacity. This can assist with ensuring they are accountable stewards of quality data that can be shared and repurposed in a responsible manner for multiple use cases.

To promote trust in public data stewardship, sector regulators and public data stewards must ensure collaboration with industry stakeholders. As private-sector data quality assessments are often beyond the public sector's control, industry data governance efforts are more suited for making laws and regulations that promote the use of high-quality data. This is necessary to accommodate various use cases that require different data quality assessment indicators. These assessment guidelines should be done through multi-stakeholder efforts — governance must be considered in the context of operational realities of various data use cases across industries.

→ ACTIONS

- Sector regulators and public data stewards must operate within specific guidelines on how data quality assessments should be implemented, depending on common use cases, algorithms, and type of data used. These guidelines can be informed by global best practices (including data and AI governance) but should be adapted to the context of African data use cases. The exchange, combinations, strategic storage, and repurposing are required to create data value. An effective data quality strategy across the public sector should be informed by technical/practical/operational realities and should outline the roles, responsibilities, and mandates of various government agencies in collecting and maintaining high-quality data in a manner that safeguards citizens.
- Member States need to participate in efforts to establish and adopt a normative framework for harmonised data standards and systems aimed at establishing national, regional, and international interoperability. These may include targeted human, technical, and institutional training interventions, sub-regional infrastructure projects, and REC regulatory sandboxes.

- A continental approach facilitates economies of scale to incentivise private investments in foundational digital infrastructure, including cloud-based technologies. Regional harmonisation of regulations for data governance could further reduce compliance costs and reduce uncertainty and operational risk for major ICT related infrastructure investments.
- Public institutions that curate data should be adequately resourced in order to contribute to multilateral fora regarding data and to be stewards of inclusive access and responsible use of data guided by appropriate industry technical and regulatory norms, standards, and best practices that underpin both the informational and economic characteristics of data in priority industries.

5.3.6 COHERENT SECTOR POLICIES TO ENHANCE DATA VALUE

Defining the problem

Competition, trade and taxation policies are significantly intertwined. Competitive local data economies, for example, may increase data-driven services, and trade openness can spur international digital trade and foreign direct investment (FDI) in domestic data economies. However, this can also reinforce the dominance of global oligopolies in domestic data ecosystems, creating trade tensions related to cross border data flows. Simultaneously data-driven digital business models may undermine domestic competition and reinforce market concentration as tax authorities struggle to quantify, value, establish and track digital value chains due to characteristics such as third-party vendors and the absence of physical presence as a basis for establishing corporate tax liability in the data-driven sector.

For Member States, collective action through a unified approach will more likely provide better outcomes that capture African contexts when addressing competition, trade, and taxation challenges in data markets.

5.3.6.1 COMPETITION POLICY

Defining the problem

The dynamic characteristics of data-driven business models create challenges for implementing traditional competition policy tools, effective competition enforcement, remedies, and merger regulation in digital markets. Resolving these challenges requires pre-emptive market interventions and continuous collaboration with complementary policies such as consumer protection, trade, industrialisation and investment.

Competition policy should take into account not only the economic effects of data market structures but also the security and privacy effects, particularly in terms of avoiding the concentration of data brokers or platforms, since this creates a risk of a single point of market failure. Thus, enforcement of competition regulation and ex-ante regulation and policy design needs to be adjusted for the data economy.

5.3.6.2 TRADE POLICY

Defining the problem

Digital systems no longer operate within clearly defined national jurisdictions. Trade policy reform is required to navigate increasing digital trade and e-commerce. Different geo-political influences, endowments, and institutional and human capabilities on the continent can affect unilateral approaches to digital trade and regional harmonisation efforts. The crossborder data strategy adopted domestically will require different institutional capabilities, can only be effective based on the existing data ecosystem endowments, will influence how data value will be created or extracted within and between African countries, and will determine who will benefit most from the data value cycle at a domestic and regional level. Furthermore, "offline" factors such as physical road infrastructure, postal reliability, logistics and supply chain efficiency, amongst others, are crucial enablers that facilitate both digital trade and e-commerce.

SERVICES TRADE, CROSS BORDER DATA FLOWS AND LOCALISATION

For digital trade to occur, data has to be moved across borders. While data accumulation can be a safe and secure way to manage data, hoarding data without means to use, exchange, or repurpose in a safe manner can also create underutilisation risks, which may decrease efficiency and diminish other benefits of digital trade. Domestic data protection and regulations not only impact local business opportunities but also affect intraregional trade and participation in the global data-driven digital economy.

While non-personal data is used and exchanged across borders, the importance of user-generated data and digital services as inputs in various industrial activities provides enormous scope to enhance exports of digital services. Services are also inputs in many manufactured products and in different data value chains. For this reason, three common general stylised data governance regimes for personal data cross-border flows have emerged that range in openness, intervention required, and actors responsible. There are also variations of all the three stylised models depending on the type of data and use case. Often, sensitive data such as personal data has more stringent crossborder data requirements than non-personal data. Data protection rules and standards can also be incorporated into sectoral regulations in highly regulated industries like health and finance that require more rigorous quality assessments and ethics considerations.

Choosing one stylised cross-border data protection regime over another should strike a balance between promoting equitable economic development and providing adequate data safeguards. Member States need to understand the economic effects of different cross-border data governance regimes based on their economic realities and development priorities.

Furthermore, given the data infrastructure deficiencies for many African countries when it comes to storing and accessing massive amounts of data, while cloud data services are a more cost-effective alternative to setting up and running a physical data centre, they require certain factors that accommodate an environment for supply and consumption of cloud services. Ultimately, crossborder provisions for cloud computing services and data centres, such as data privacy, security, and restrictions on where data are housed (localisation requirements), need to be decided in consideration of broader economic development priorities.

The table below summarises the main pros and cons of each data governance regime to aid policymakers with deciding the best approach to follow in the context of their sovereign and development priorities.

Three stylised approaches to governing cross border data flow

Cross-border data governance regime	Description	Pros	Cons	Assumptions
Open transfers regime	Relatively low a priori mandatory approval requirements, and voluntary private sector industry standards inform the free movement of data (eg. USA, APEC)	Minimal regulatory burden allows for the greatest flexibility in the movement of data Most suitable for digital services trade and data value creation Privacy is a consumer right	Risks of proliferation of standards across firms and jurisdictions, without guaranteeing any minimum standard for personal data protection Requires, technical human, and institutional capacity to monitor private firms and excercise ex post accountability Limited data subject rights - lack of consent for personal data use	Interoperable data systems and infrastructure Human, technical and institutional capacity to create value from data Strong preconditions (enablers) to leverage the data-driven digital economy Data subjects with digital capabilities to provide consent
Conditional transfers regime	Consensus base, established regulatory data safeguards and overarching regulatory guidance from data protection authorities or international agreements (eg. GDPR)	Offers more balance between data protection and the need for openness of data transfer for value creation Encourages establishment of domestic data processing authority (DPA) Clear guidelines and mandatory regulatory safeguards that once met allow for the free flow of cross-border data	Base on strong data subject rights Certain conditions need to be fulfilled ex-ante Can perpetuate compliance burdens and digital trade bottlenecks	Same as above International collaboration and geopolitical influence to enforce ex-ante conditions
Limited transfer model	Cross-border data flows are conditional based on government approval and localization requirements for domestic storage or processing of data (eg. China, Russia)	Based on strong national security and public data control imperatives	Stringent regulatory approval for international data transfers and may require explicity or implied data localization and mandatory storage	Same as above

Source: Authors own interpretation summarised from Ferracane and van der Marel (2021), WDR (2021)

E-COMMERCE

E-commerce platforms allow consumers to benefit from a wider variety of choices at more competitive prices. Strategies to enhance e-commerce cannot be formulated in isolation since e-commerce intersects with a multiplicity of other issues, including Digital ID, data governance, customs duties, crossborder data flows, cybersecurity, payments system interoperability, consumer protection,[13] competition, taxation, and standards, to name a few. Furthermore, improving e-commerce adoption requires addressing factors such as internet penetration, postal reliability, use of payments services (bank accounts or mobile money), and security of internet servers.[14] For Member States, collective action through a unified approach will more likely provide better outcomes that capture African contexts when addressing overlapping challenges that affect different government mandates at multilateral fora.

Trade agreements alone are not the appropriate cross-border data governance instruments. The current common approach to using trade agreements to govern cross-border data flows has not led to binding, universal, or interoperable rules governing the use of data across jurisdictions. However, in the context of the AfCFTA, a harmonised, coordinated approach to addressing challenges associated with datafication domestically will contribute to better alignment with various overlapping intra-regional digital trade and e-commerce coordination efforts beyond the forthcoming e-commerce[15] and services trade protocols[16] in the strategy.

RECOMMENDATIONS

- To foster competitive, safe, trustworthy and accessible data ecosystems, competition authorities need to find coordinated, effective ways to regulate concentration while preserving the benefits that dominant firms offer in the context of different development needs across the continent. This includes ex-ante regulation of competition issues before they escalate in the market.
- Policy makers in the tax, competition and trade landscape will need to build human and technical capacity to address emerging issues beyond the traditional sectoral mandate that may affect data-driven markets.
- Member States must promote predictability and convergence of regimes across complementary policy areas in a manner that is mutually reinforcing. This needs to be done to navigate the emergence of new dynamic data-driven business models that can foster intra-Africa digital trade and data-enabled entrepreneurship. At the same time, policymakers should heed the two-way linkages between economic outcomes and data governance and carefully weigh the trade-offs.
- Member States should foster a coordinated, comprehensive and harmonised regional approach to global governance challenges associated with the global data-driven digital economy, such as:
  - cross-border collaboration in implementing competition policy instruments to address anti-competitive behaviour in data-driven digital markets;

13 Online consumer protection and product returns, consumer safety and supplier liability.
14 *https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf*
15 The AfCFTA e-commerce protocol is an important tool to preserve the consolidated African market in the digital sphere, and preclude other arrangements which could potentially undermine the liberalisation and integration agenda. Guidelines are expected to be finalised in Phase III of AfCFTA negotiations.
16 Phase II of AfCFTA set to address trade in services, intellectual property rights, investment and competition policy.

- encouraging data portability through regulation and other enabling activities;
- the Organisation for Economic Co-operation and Development's (OECD) efforts to prevent tax avoidance in relation to data-driven businesses;[17]
- World Trade Organisation's (WTO) agreements in data-enabled services and e-commerce;
- establishing coordinated regional foundational data infrastructure and digital data systems development initiatives;
- strengthening human, technical, and institutional capacity to support data interoperability, value creation, and equitable participation in data economies; and
- contributing to the international harmonisation of technical standards, ethics, governance, and best practices regarding data, big data analytics and AI.

→ ACTIONS

- Member States should encourage dynamic policy and regulatory reform and experimentation (e.g. regulatory sandboxes at the industry and REC level).
- Policy makers should heed the two-way linkages between economic outcomes and data governance and carefully weigh the trade-offs. Different state entities must endeavour to establish safe and responsible data-sharing frameworks that facilitate data demand, data interoperability, cross-border data flows, data value chains, and open data standards and systems within key priority sectors as assigned by the DTS. Where remedies are imposed, they should be based on an economic assessment that accounts for long term impacts on incentives for investment and innovation.
- For data use to be efficient, inclusive and innovative, it will require collaboration between regulatory institutions across different mandates and coordinated market regulation (in interrelated policy areas such as telecommunications, finance, competition, trade, taxation and data regulation).
- Competition authorities or related institutions will need to build human and technical capacity to address emerging competition issues beyond market concentration that may affect data-driven markets.
- Traditional competition tools such as guidelines on market definitions, assessing dominance, anticompetitive practices (e.g. abuse of dominance, coordinated practices, and abuse of buyer power), merger assessment, and theories of harm and designing remedies will need to be adjusted to incorporate the dynamism of data and characteristics of data-driven businesses.
- AfCFTA signatories will need to determine how the e-commerce protocol will operate alongside existing laws and policies and will need to account for and support the objectives of the other protocols, such as investment, intellectual property and competition policy (to be negotiated in Phase II).
- Develop and enhance public-private dialogue mechanisms to improve e-commerce-related policy making.

17 *https://www.oecd.org/tax/beps/*

5.3.6.3 TAXATION POLICY

Defining the problem

There is an incongruence between where the profits of global platforms are currently taxed and where and how value is created from data within the digital economy. In Africa, most countries are mainly data markets for global platforms, with users contributing appreciably to the generation of platform profits without a plausible value capture mechanism. Currently, Africa's data traffic is growing at an annual rate of 41% (UNCTAD, 2019), implying greater usage and adoption of the services provided by global digital platforms within the region. While there have been ongoing engagements by multilateral institutions, chiefly led by the OECD's Inclusive Framework on Base Erosion and Profit Shifting (BEPS) (albeit not wholly inclusive for Africa with only 23 participating countries), a global consensus has not been reached for the different proposed options (Pillars One and Two) with respect to digital taxation.

Several African countries, reluctant to delay taxation of digital services or not aware of the benefits for their countries of the international reforms, are already implementing unilateral mechanisms. These include digital services taxes and equalisation levies based on significant economic (data) to capture some of the data value by taxing some parts of the digital economy within their jurisdictions. These mechanisms also include expanding sector-specific taxation on the telecommunications industry and taxing mobile money transactions and the usage of some over-the-top communications applications (OTTs) within the region, such as WhatsApp, Facebook, Twitter, Skype, and Instagram. While these taxes are driven to increase government revenues, the negative consumer impact has slowed digital access and inclusion (due to shifted consumer costs) and has restricted the right to free speech for citizens. On the supply side, the expanded taxes on the telecommunications sector impacts negatively on the profits of resident sector operators (with consequent negative implications for infrastructure investments critically needed within the resource-constrained region), while the data-based OTTs are largely untaxed locally (CTO, 2020; ICTD, 2020; RIA, 2021).

From a sovereignty and tax benefit perspective, every country is entitled to tax the profits of global digital platforms as long as they have an economic interaction with its citizens and residents (this is largely via sales of their personal data). However, despite having millions of its citizens and residents as users of data applications run by global digital platforms, African countries under the current international taxation regime do not have the required nexus for taxing the profits of these entities. While some of the platforms have some form of local presence in African countries, these subsidiaries are only set up as administrative support services and do not legally own the assets of these platforms (which are largely intangible and currently not included within the proposals of most apportionment formulas), and therefore do not receive any accruable revenues on the assets.

More so, the different tax propositions for the digital economy - which include formulaic apportionments, application of Significant Economic Presence (SEP), and the use of indirect mechanisms such as value-added tax (VAT) and more direct withholding tax (WHT) – all require access to transaction data, of which global digital platforms are currently not willing to share (especially in non-resident markets). Even in cases where some of this data is accessed, it will need to be verified and validated.

Recent legislative and policy measures introduced by select African countries, within the context of the several multilateral and unilateral efforts at taxing the digital economy, may not be conducive to either the creation of a single market or to accessing international resources

to realise global public goods and meet some of the preconditions for a competitive data economy on the continent. Tapping into new sources of tax revenue might allow African countries to eliminate excise duties on social networking and data services, reducing distortions to both the local market and the global tax system.

RECOMMENDATIONS

African governments need to increase economic activities within their jurisdictions that leverage digitalisation and datafication mechanisms, as enhanced productivity within this remit will amplify capacities for higher tax revenues. This process will require the development of more local data-based companies within the purview of the region's industrial policy. This pathway can help ameliorate fiscal compliance risks that are amplified within the current situation where a significant portion of public data within the region is captured and controlled by foreign data companies (Khan & Roy, 2019).

→ ACTIONS

- Member states should support the harmonisation of the tax regime for digital goods and services at the regional level and alignment at the global level, which would mitigate the risks associated with small data economies markets being unable to generate significant value and compete in global markets to contribute to the scale and scope required for data-driven value creation and to generally limited tax bases.
- Complementarily, a public data fund coalesced by AU member countries could be set up in collaboration with the private sector to build the requisite infrastructure for extracting these transaction data, where the data can be retained as part of a regional data commons beyond just the remit of taxation purposes.
- Facilitating a public data fund will require African countries to digitalise their tax administration systems to enable the more efficient assessment and collection of digital platforms taxes. A digital tax administrative system will enhance the capacity for tax registration, transaction data sharing with the National Tax Authorities and the exchange of tax obligation information with the digital platforms for compliance while lowering operational costs.
- Member States should use the opportunity to coordinate taxation of digital services for a single digital market to tap into new sources of tax revenue that might allow them to eliminate regressive and fiscally counterproductive excise duties on social networking and data services and reduce distortions to both the local market and the global tax system.

5.4 DATA GOVERNANCE

For data governance policy to be effective, it should encourage an ecosystem where there are multi-stakeholder efforts to improve data access and use. It should also encourage the repurposing and combination of data to limit harms and risks associated with the processes of datafication while ensuring that a wide variety of data will be used to its greatest economic and social potential. Some of these policies involve making data available, while others restrict the flow of data (Macmillan 2020).

5.4.1 DATA CONTROL

Facilitating control of data for firms and government is an important mechanism for extracting data value (Carrière-Swallow & Haksar, 2019; Couldry & Mejias, 2018; Savona, 2019). Policy helps to limit the manner in which control can be exerted and also encourages mechanisms for control that align with the strategic objectives of a data policy. An important role of policy is helping to ensure clarity in terms of control for the assignment of obligations and responsibilities (Carrière-Swallow & Haksar, 2019; Zuboff, 2018).

5.4.1.1 DATA SOVEREIGNTY

Data control can also be understood at a national level in relation to data sovereignty (Ballell, 2019). Data sovereignty draws on the concept of the sovereign nation state. It refers to the view that data that is generated in or passing through national internet infrastructure should be protected and controlled by that state (Razzano et al., 2020). In the digital context, it can be understood as a subset of cyber sovereignty defined as the subjugation of the cyber domain (which is global by definition) to local jurisdictions (Polatin-Reuben & Wright, 2014). Two approaches of weak and strong data sovereignty exist. Weak data sovereignty refers to private sector-led data protection initiatives with an emphasis on the digital rights aspects of data sovereignty. Comparatively, strong data sovereignty favours a state-led approach with a focus on safeguarding national security (Polatin-Reuben & Wright, 2014).

In general, the transfer of personal data to another country is allowed only under certain conditions, for instance, when another country has a law that requires sufficient safeguards (including privacy and security) for the processing of personal data. States often exercise data sovereignty for the protection of the rights of their citizens, such as through data protection regimes that regulate cross border data flow to protect the rights of data subjects, often through agreements setting data protection standards and reciprocal protection of exchanged data. While sufficient legal standards are necessary for reciprocity, so is the practical ability of states to enforce mutually agreed standards. Ensuring sound data governance practices is a foundational step for realising data sovereignty.

5.4.1.2 DATA LOCALISATION

Defining the problem

While data localisation is often seen as an expression of state sovereignty, as a possible policy option, data localisation needs to be assessed on a cost-benefit basis. This policy choice may present a practical challenge. While data localisation is sometimes motivated by the need to protect data subjects, data localisation can be applied to non-personal data. This is why it is essential data localisation is read in the context of control in order to emphasise in policy the importance of supporting mechanisms that can facilitate the act of sovereignty.

Data localisation involves the artificial erection of legislative barriers to data flows, such as through data residency requirements and compulsory local data storage (Cory, 2017). Strict data localisation rules requiring the storage of all data locally, and not merely a copy, renders such data susceptible to security threats, including cyber-attacks and foreign surveillance.

Some African countries face acute technological capacity constraints so that localisation capacity demands may vastly exceed national data centre capacity. Concomitantly, requirements for duplicate copies of data may place undue financial obligations on local companies.

RECOMMENDATIONS

- Member States should prioritise politically neutral partnerships that take into account their individual sovereignty and national ownership to avoid foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States.
- AU Member States have the right to formulate digital and data rules in line with their priorities and interests, notably to protect the information security of the state and its citizens and to prevent third parties from unfairly exploiting resources and local markets.
- Bilateral and multilateral agreements need to be established to exert domestic sovereignty and control, and recourse avenues for infringements are required.
- Localisation needs to be evaluated against potential harm to human rights.
- Data localisation requirements require data specificity. Data localisation solutions have been strongly articulated within sectoral (vertical) data silos across different jurisdictions; for instance, Nigeria instituting certain forms of financial data localisation, Australia prescribing forms of health data localisation, etc. This is an area in which specificity is strongly required for facilitating broader flows as far as is conducive with policy imperatives like the Africa Free Trade Area, and for clarity, which can help minimise the costs for local businesses and innovators and reduce the risks of unintended consequences.
- Data policy requires clarity not just through specificity but also in relation to data categorisation, which can allow Members to exert sovereignty through the establishment, for instance, of security classifications or specific levels of data sensitivity. These should be consistently applied across data (and information) policy.
- Data infrastructure development should be explored as a mechanism for exerting control but must be contextualised in consideration of environmental impacts, safety and security infrastructure, duplicated costs for local data communities, and overall costs.
- Public sector capacities should be invested in to inform domestic and effective data control initiatives.
- Data subject rights should be designed and expressly provide effective personal data control. Data trusts and stewardships should be explored as another form of effective personal data (and other data) control.

→ ACTIONS

- Data protection authorities (DPA) need full empowerment, including the remit on data sovereignty.
- DPAs are encouraged to adopt international and regional cooperation practices taking note of different stages of implementation and enforcement across the Member States.
- Risk assessment and multi-stakeholder engagement should be used to design data localisation solutions in policy by drafters, which includes civil society participation.
- Data infrastructure policy should be aligned with data control imperatives by policy drafters but must consider cybersecurity, personal data protection, environmental risks and cost.
- Public administration and investment policy should align with data control capacities as a priority.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation.

MECHANISMS FOR EXERTING DATA CONTROL

There are mechanisms for exerting data control, such as through data trusts. Data trusts and/or stewardships are alternative forms of discrete governance solutions in the context of data. A legal trust is a legal instrument used to manage property, both corporeal and incorporeal. A trust allows someone to hold assets (which they do not own) for the benefit of the trust beneficiaries. The person who holds the assets has been authorised to do so and owes the beneficiaries of that trust a fiduciary duty to act responsibly in the management of their assets. This traditional legal structure has been posited as a way of managing collections of data on behalf of groups and facilitating mass data sharing in situations where licensing or open data models might not be feasible to foster innovation through facilitating fair access (Stalla-Bourdillon et al., 2019).

The Open Data Institute defines data trusts as providing "…independent, fiduciary stewardship of data" (Open Data Institute, 2018). The addition of the fiduciary element to the definition (as opposed to merely defining it as a form of legal trust) was added as being an essential element of responsibility and obligation, which forms an important foundation of the concept (Open Data Institute, 2020). In addition, it can include privacy-by-design solutions within the architecture of any mechanism designed to facilitate the trust, thus in ensuring privacy in substance and process (Stalla-Bourdillon et al., 2019). While data protection laws might create standards for how a person's data can or cannot be processed, outside of consent or recourse for violations, the mechanisms for persons to act in relation to their data is limited - thus, data trusts help to facilitate realising data control. Data trusts provide a data subject with a mechanism through which they can provide (or 'share') their data while also removing from them the sole responsibility for 'ensuring' data protection compliance by both public and private sector actors through the establishment of a fiduciary relationship.

5.4.2 DATA PROCESSING AND PROTECTION

Defining the problem

While data control principles help to outline delineation and obligations in respect of both personal and non-personal data, data processing seeks to outline the policy guidelines for the processing of personal data, as discussed earlier. Regulation of non-personal data is determined by data categorisation and specific access regimes.

These forms of guidance are important as a mechanism for realising privacy and data protection. Personal data processing is a critical component of data governance and fostering a trusting environment. The building of trust is understood as a necessary part of fostering a sound data and digital economy. By constraining process limitations to personal data, such constraints need not impede the data flows for digital trade; but to ensure such lack of impediment requires consistent data policies across the region based on shared but flexible principles (United Nations, 2017).

As an aspect of personal data processing, data subject rights also offer ancillary benefits for helping to ensure data integrity and quality.

A privacy-by-design approach can be taken when developing digital technologies and systems by which privacy is incorporated into technology and systems by default during the design and development process (Cavoukian, 2009). For instance, it may entrench minimality in its data collection or automate rigid de-identification. It means a product is designed with privacy as a priority, along with whatever other purposes the system serves. This design should incorporate a particular understanding of how data subjects engage with products and their capabilities for asserting their privacy.

De-identification techniques, including anonymisation and pseudonymisation, can facilitate some uses of data while providing at least partial data protection. Pseudonymisation can be accomplished through the use of a signifier or mask that can only be connected to an identifiable individual through additional data. While both anonymisation and pseudonymisation may enable both private service providers and the public sector to make greater use of data, they are reliant on the current state of technology and mathematics. As new mathematical approaches are developed, and computer processing power increases, data that was deemed de-identified may become identifiable. While data protection regulations often require de-identification, these techniques are insufficient without strong legal rights for data subjects and a regulator with the capacity to enforce data protection.

RECOMMENDATIONS

- DPAs must be established that are independent, funded and effective. Additionally, as a method of ensuring effectiveness, accountability metrics are crucial for helping a DPA have a clear scope. Lawful data processing frameworks must be established, including clear deterring penalties to ensure compliance. They must cover all relevant data processing actors.
- Personal data risk assessment should be obliged in the deployment of personal data technology development.
- An important sub-principle, which must be actioned with data processing frameworks for public and private stakeholders, is that of minimisation. The minimisation of personal data collection is one of the most effective mechanisms for mitigating data subject risks and harms.
- Codes of Conduct should be explored to promote data and sector-specific needs. Such Codes, approved by the relevant DPA, can provide sector and industry expertise in managing the real risks and harms associated with processing and ensuring best practices in the management of those harms. It can also help to consider the sectoral exceptions required for a constructive data economy to thrive but also feed into a broader Sustainable Development agenda, such as through the ready facilitation of research (in health or other social development arenas).

→ ACTIONS

- Data processing frameworks should be established in partnership with all relevant multi-stakeholder partners but driven ideally by the DPA. These should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (including incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity.
- DPAs should be established as a matter of urgency alongside national legislation on personal data protection.

5.4.3 DATA ACCESS AND INTEROPERABILITY

Data access and accessibility are understood both in terms of reactive forms of access facilitated by laws and regulations, as well as through proactive forms of data access (such as through open government data) (Open Data Charter, 2015). Accessibility also implicates sharing of data across agents or departments, an important benefit of data's non-rivalrous nature. Yet this requires interoperability between these different agents (Jones & Tonetti, 2020). In the context of competition, data is not simply portable in a way that can facilitate scale effects easily between firms (Rinehart, 2020). Requiring forms of data portability remains a key cited regulatory strategy for facilitating competition and consumer benefit, though the realities have not yet been established as definitively beneficial (Mitretodis & Euper, 2019; Rinehart, 2020). From a privacy perspective, outside of just interoperability changes, the nature of big data collection means that data portability implicates other users' privacy (Nicholas & Weinberg, 2019).

RECOMMENDATIONS

- Open data standards should be prioritised in public data creation and maintenance. The creation of data to these standards does not preclude overlaid mechanisms for control or limiting access in defined data categories for compelling purposes.
- Data portability should be supported. Data portability can be a form of data subject right, defined as the right of the data subject to obtain data that a data controller holds on them in a structured, commonly used and machine-readable format and to re-use it for their own purposes. Portability can be facilitated through a policy on data portability in public sector data and by establishing specific data portability rights in consumer contexts.
- Data partnerships (including options like databanks) should be prioritised as mechanisms for advancing quality and privacy-preserving open data.
- As a method of facilitating specificity, data categorisation can be a method for ensuring cohesion within data processing frameworks within processing allowances and security principles. The categorisation referred to here is not such as the sectoral typologies considered more broadly but rather as a specific mechanism for realising particularly forms of risks that align to data and information types and might include sensitive categories (such as children's data), security classifications of relevance, as compared to forms of data already in the public domain.
- Restrictions on processing need to be clearly articulated and limited in order to not interfere with low risk processing that might be increasingly central to the training of AI through large-scale data processing.

→ **ACTIONS**

- Member States should establish an open data policy which sets open standards for the production and processing of data so that when decisions are made to open the data, the high costs of ensuring it is usable and manipulatable are avoided.
- Sectoral laws and codes of conduct from DPAs should be reviewed to ensure lawful data access in conjunction with the data policy.
- DPAs should have dual access to information and privacy functions.
- Multi-sectoral open data initiatives should be implemented in priority data sectors like health, research and planning.

5.4.4 DATA SECURITY

Defining the problem

Data security includes the set of policies, norms, regulations, legislation and practices to protect the confidentiality, integrity, and availability of data from unauthorised access, corruption or theft throughout the entire lifecycle of data. These fundamental principles of data security also define the three main areas of accountability of information security. The concept of data security encompasses many aspects, from the physical security of data centre hardware and storage devices to administrative access controls, as well as the logical security of networks, software, and applications. It also includes organisational procedures and policies.

Confidentiality, integrity, and data availability, from a regulatory perspective, depend on national cybersecurity policies and legislation. The security of data (including confidentiality, integrity and availability) also does not depend on the physical location of the servers hosting such data. Rather, it is a function of the normative rules - including norms, policies, regulations, laws and protocols (such as data standards and technical interfaces), and the implementation of technologies and security measures (such as encryption, firewalls and access controls) - that are put in place by public or private service providers in the way that they store, access, share and use the data.

Increasing data security legislation and technical measures may both improve confidentiality, integrity and availability (positive security) as well as undermine fundamental freedom and rights of privacy, dignity, and safety online (negative security). For example, some countries may impose restrictions on data sharing and transfer by enacting cybersecurity legislation to protect users' data safety and security. These can be barriers to the free flow of data. From a cybersecurity perspective, some states may believe that data is more secure if it is stored within national borders. States may erroneously refer to it as principles of data sovereignty, while these measures are simply forms of data protectionism and data localisation.

A principle that is difficult to uphold with regard to data security is that of transparency. While countries continue to witness an increase in the number of attacks reported to law enforcement, improvements in this area have been driven almost entirely by data protection regulations, and reported incidents are primarily data breaches. On the other hand, increasing transparency on data security includes both technical aspects, such as reporting on zero-day vulnerabilities and adherence to international cybersecurity standards, as well as policy aspects related to the assessment of cyber capacity maturity. Transparency in data security has the potential to improve technical and procedural defence mechanisms against attacks and to strengthen collaborative practices based on information sharing.

RECOMMENDATIONS

- Member States should develop national cyber security policies as well as necessary legal and technical measures to sustain trust in their digital space.
- Member States are encouraged to co-operate regionally to develop cybersecurity standards to be met in both the public and private sectors to increase regional eco- nomic growth.
- Data policies should align with cybersecurity and cybercrime policies, and legislation dealing with cybercrime should respect human rights.
- A joint sanction regime for cyber-attacks should be established.

→ **ACTIONS**

- Member States, who are yet to develop cybersecurity measures, should immediately develop cybersecurity plans and streamline them within government governance structures to promote robustness and reduce vulnerabilities.
- Cybersecurity institutions like CSIRTs should be incorporated into data policy development.
- Data processing roles as a form of security protection should be specified in policy by policymakers.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation and could be supported by DPAs.

5.4.5 CROSS-BORDER DATA FLOWS

An increasingly important issue regarding international and regional trade is the cross-border transfer of personal and other data (Deloitte, 2017). In the African context, international and regional frameworks that facilitate cross-border transactions and personal data flow across countries are essential for the creation of common markets and particularly for the realisation of the African Free Trade Area. Cross-border data transfer of personal data, in particular, is shaped by the data sovereignty approach that a country wants to pursue, which refers to the legal principle that information (generally in electronic form) is regulated or governed by the legal regime of the country in which that data resides. As noted, this concept is challenged by the modern reality of data movements. Critiques of the supposed 'data flows' narrative and the extent of its benefits for digital dividends in development should however be acknowledged, as should recognition that significant amounts of data flows actually occur horizontally within firms rather than between firms (UNCTAD, 2021).

It is also worth mentioning the common position that the transfer of data is dependent on whether the receiving country has an adequate level of protection (Razzano et al., 2020). However, what amounts to this 'adequate' level will frequently be determined by a country's Data Protection Authority or similar. Thus, in the absence of a data protection law in the receiving country, the transfer of personal data cannot be subject to proper regulation unless the law of a country forbids the transfer of data except to a country with an adequate level of protection, or through the establishment of bilateral obligations through contracts between the transferring parties.

The reality is that broad limitations on cross-border data transfer could result in business opportunities lost and reduce the ability of an organisation to trade internationally, leading to a reduced geographical footprint and loss of market competitiveness. Data regulation that is synchronous with regulations in other jurisdictions contributes to mutual trust and lays a foundation for a trusted exchange of data, including (but not limited to) personal data. In this sense, personal data protection regulation enables and improves trust and trade in the cross-border movement of persons, goods and services (Information Society, 2018).

RECOMMENDATIONS

- Data protection frameworks should provide minimum standards for cross-border data flows.
- The establishment of norms and standards should expressly ensure reciprocity as a central principle for permitting cross border flows.
- Data specificity should be prioritised to avoid unintended restrictions on productive data sharing.
- Law enforcement considerations should be incorporated into the policy-making process.
- To ensure effective cross-border resolution, a degree of capacity must be ensured across agencies.
- Members of the African Union should rigorously define a framework and modalities to regulate cross borders data flows and identify the African entity and persons entitled to manage this system.

→ ACTIONS

- DPAs should ascertain minimum standards for data transfer.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation and driven ideally by DPAs in conjunction with educational facilities and government skills programmes and units.

5.4.6. DATA DEMAND

While there are significant data and digital economy recommendations that relate to helping create a broader data ecosystem, there are also specific policy interventions to be pursued in relation to demand-side data stimulation. Data users may be the public sector, private companies (of different sizes), and also individual users and citizens. However, capacity needs to be developed across these profiles to stimulate demand for data, data cultures and innovation. The role of policy in fostering the productive use of data across stakeholders is facilitated by the preceding policy areas but may also require more specific considerations. This is especially the case given that the data reality for many local actors within the data ecosystem is one of data scarcity rather than saturation.

RECOMMENDATIONS

- Data communities should be prioritised in innovation policy. These communities require domestic policy incentives and support, including the active promotion of data hubs and other forms of community innovation that can help engender data competencies and data cultures, as should civil society actors more broadly.
- Regulatory provision for data management should include provision for regulatory sandboxes to encourage local data development.

→ **ACTIONS**

- Data communities should be incorporated into data policy-making processes by policymakers.
- Data communities should be drawn into the establishment of open government data initiatives by departmental implementers.
- Universities should be included as relevant policy stakeholders to help establish the "knowledge-base" from which the local data economy can draw sufficient scientific and technological knowledge.

5.4.7 DATA GOVERNANCE FOR SECTORS AND SPECIAL CATEGORIES OF DATA

Certain categories of data and certain specific sectors require tailored data governances that take into account the particular issues that affect that category or sector. Categories such as health data or children's data are not the same as sector-specific typologies such as financial data, but both may require distinct treatment. However, the special treatment creates a threat of data silos that render data less useable and may raise compliance costs, especially if there are incompatible regulations or requirements. Special treatment is sometimes necessary but should be in harmony with general data governance and this policy framework.

A key recommendation of Data Access and Interoperability is that types of data that require special consideration be identified and clearly specified so that special access and other requirements in respect of that data integrate with general data rules. As discussed under Data Localisation, clearly specified types of data are sometimes subject to data localisation requirements in pursuit of policy objectives peculiar to the type of data. In the Data Processing and Protection recommendations, it is recommended that codes of conduct, subject to approval by the national DPA, can be used for sector-specific requirements.

RECOMMENDATIONS

- Members should avoid special data regimes that are not integrated into national data regimes and that do not incorporate the principles of good data governance.
- Governance mechanisms and policies should enable the development of category and sector-specific data governance for children's data, health data and other kinds of sensitive data or sector-specific data that warrant distinct treatment through processes that are in accordance with the principles in the framework.

5.5. INTERNATIONAL AND REGIONAL GOVERNANCE

At a transnational and continental level - particularly to provide capability for cybersecurity and to address data protection concerns associated with the changes in data economics - cooperation between countries is of increasing significance. The scope of cooperation needed includes dialogue between governments, collaboration with the private sector, and effective, integrated processes to investigate and prosecute cross-border breaches. A global trust architecture that accounts for the limitations of existing national or otherwise fragmented systems is essential to secure a digital economy and digital inclusion (African Development Bank 2019).

Certain international and continental-wide initiatives serve as a foundational step for precipitating implementation.

For instance, the African Union and regional initiatives on digitally encoded genetic data[18] and geographical and environmental data, respectively. The African Union Commission will ensure harmony between these initiatives and the ongoing data policy work[19].

RECOMMENDATIONS

The African Union, with the support of sister Pan African organisations, should:

- Facilitate collaboration between the various entities dealing with data across the continent through the establishment of a consultation framework within the digital ecosystem community to safeguard the interest of each actor.
- Strengthen links with other regions and coordinate Africa's common positions on data related international negotiations to ensure equal opportunities in the global digital economy.
- Support the development of regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and Artificial Intelligence) and the necessary enabling environment and data-sharing mechanism to ensure circulation across the continent.

5.5.1 CONTINENTAL DATA STANDARDS

To facilitate cross-border cooperation, it is important to achieve consensus on data standards, which is an integral consideration for advancing interoperability. These multistakeholder forms of consensus should reference the work done through the International Organisation

18 While the category of digitally encoded genetic data includes the genetic data of humans, where these are identifiable individuals, this should be regarded as sensitive data and dealt with as required by the Malabo convention. But there are other kinds of digitally encoded genetic data that require specific/special treatment that are neither sensitive nor personal. These include demographic genetic data, and the genetic data of organisms other than humans.The African Union is currently engaging with other countries who are parties to the Convention on Biodiversity (CBD) to ensure that digitally encoded data should be treated as biological resources as that term is used in the CBD.The convention states that biological resources "include genetic resources, organisms or parts thereof, populations, or any other biotic component of ecosystems with actual or potential use or value for humanity".The convention governs both access and benefit sharing to both enable research and to require that people who are custodians of biodiversity share in the benefits of that research. Applying the rules of the convention will enable beneficial data flow while also ensuring that Africans benefit.

19 The Regional Data Strategy for Marine and Coastal Areas Management in Western Africa promotes more sustainable management of natural resources through mutual sharing of data.

for Standardisation and other forms of international consensus achieved in specific sectoral contexts. However, while international standardisation is important for competitiveness, it should be noted that these international standards may not be sufficient for the region's needs. This is demonstrated, for instance, in language challenges found in the context of spatial or geographical data.

RECOMMENDATIONS

- Consensus on data standards should reference the work of the International Organisation for Standardisation, amongst other relevant forums.
- However, standards need to be set with specific reflections on contextual factors impacting the continent.

→ ACTIONS

- Establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards.

5.5.2 OPEN DATA PORTAL AND OTHER INITIATIVES

There are important open data initiatives already occurring centrally, which should remain supported in the name of a sound regional data economy. These include the African Development Bank's central open-data portal (*https://dataportal.opendataforafrica.org/*), and institutionally driven initiatives (as in *https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/central/about*) and volunteer-driven communities (such *https://africaopendata.org/*).

5.5.3 CONTINENTAL INSTRUMENTS

The broad range of existing relevant instruments are outlined in section 4. However, two specific areas need to be highlighted.

Cross-border data flow mechanism

There is an opportunity to leverage this framework to begin collaboration towards a regional cross-border data flow mechanism facilitated by an overarching instrument, such as those by the OECD and ASEAN.

AU Convention on Cybersecurity and Personal Data Protection

It is recommended that the AU Convention be ratified as soon as possible to serve as the foundational step for the harmonisation of data processing. Additional protocols to the Convention should also be explored to reflect changes since the original drafting.

African Continental Free Trade Agreement

The AfCFTA provides an opportunity for cooperation on a number of important aspects of the Data policy framework, most saliently in the development of the agreements on competition, intellectual property and investment.

RECOMMENDATIONS

- Promote and facilitate data flows within and among AU Member States by developing a Cross Border Data Flows Mechanism that takes into account Africa context, namely the different levels of digital readiness, data maturity as well as legal and regulatory environments.
- Facilitate data circulation across sectors and cross borders by developing a Common Data Categorisation and Sharing Framework that considers the broad types of data and their different levels of privacy and security.
- Work in close collaboration with national authorities in charge of personal data protection of AU members, with the support of the African Network of Authorities (RAPDP), to establish a coordination mechanism and body that oversees the transfer of personal data within the continent and ensures compliance with existing laws and rules governing data and information security at national level.
- Enable data sharing and enhanced interoperability among AU Member States and other AU mechanisms, including the African Union Mechanism for Police Cooperation (AFRIPOL).
- Work towards building a secure and resilient cyberspace on the continent that offers new economic opportunities through the development of an AU Cyber Security Strategy and establishment of Operational Cybersecurity Centres to mitigate risks and threats related to cyberattacks, data breaches, and misuse of sensitive information.
- Establish mechanisms and institutions, or empower existing ones, within the African Union to build capacity and render technical assistance to AU Member States for the domestication of this data policy framework.
- It is recommended that the negotiation of the competition chapter of the AfCFTA should set minimum standards to ensure that putatively proprietary non-personal data is accessible to innovators, entrepreneurs, and others in the value chain to encourage competition across the continent.
- Members of AfCFTA should consider including provisions in the competition chapter that mandate competition authorities to consider market structure issues to also consider the security and privacy effects of market structure. This is important to avoid the concentration of data brokers or platforms both nationally and regionally since this creates a risk of a single or few points of failure with far-reaching consequences.
- Members of AfCFTA should also consider including provisions in the intellectual property chapter of AfCFTA that clarify the status of data with respect to intellectual property, in particular:
    - that if copyright is extended to databases and compilations of data that it only applies when databases and compilations are created by human authors and exhibit originality and that the copyright extends only to reproduction of the original selection and arrangement of data in the database and not to the data itself;
    - that any copyright or other intellectual property right, including trade secrets that enables control of data, does not apply to personal data; and
    - that any copyright or other intellectual property right, including trade secrets that enables control of data, is limited by the provisions of competition regulation.

→ **ACTIONS**

- Member States should ratify the AU Convention on Cybersecurity and Personal Data Protection and develop additional protocols, as required, to reflect changes since the original drafting.
- Establish, or empower a mechanism within the African Union for centralising regional engagements on data standards.
- Once adopted, alignments with the AfCFTA process should immediately be explored.
- Include data in negotiations on the AfCFTA chapters on competition and intellectual property.
- Agree on common and consistent criteria for assessing adequacy in the levels of protection of personal data across the continent to facilitate and enable transborder transfer of data and standardise protection.

5.5.4 CONTINENTAL AND REGIONAL INSTITUTIONS AND ASSOCIATIONS

Regional institutions and associations create a central mechanism for creating a unified regional voice on data issues. Many associations already exist, and ensuring the implementation of this framework speaks to existing associations is a priority recommendation. Continental and regional bodies are particularly important due to the crossborder nature of data flow required to benefit from data.

Regional economic and development communities

The Regional Economic Communities, as building blocks of the African Union can assist member states to create capacity, domesticate data policy and reach consensus on harmonisation of data policy, participate in standards making, and enable data flow.

Human rights adjudicators

The African Court on Human and People's Rights, the East African Court of Justice, and the ECOWAS Community Court of Justice provide for a skilled capacity to adjudicate complex disputes on privacy and equality, which are relevant to personal data protection and the use of data to unfairly discriminate.

The SADC Tribunal, once recapacitated, could also offer a forum for data disputes, albeit within a more limited mandate. Continental and regional adjudication mechanisms are best placed to resolve cross-border data disputes.

African Network of Data Regulators

Empowering DPAs and improving the level of enforcement of legislative and regulatory frameworks at national level significantly assist individual's enjoyment of digital rights. An avenue for this capacitation is through the promotion and support of existing associations, such as the African Network of Data Protection Authorities.

ICT regulatory authority associations

There are existing ICT associations, such as the Regional Association of Regulators (ART-AC, WATRA, CRASA and EACO), that stand as important mechanisms for peer learning on cross-border associations. They can also facilitate collaboration and knowledge sharing as cross-border instruments and standards are explored.

Sectoral associations

Sectoral associations like the African Tax Administration Forum will be needed to help realise data economy recommendations areas in particular. Given the importance of digital identity within the data economy, the Association of National Registrars is also important.

African Competition Forum

The African Competition Forum (ACF) describes itself as "an informal network of African national and multinational competition authorities". The ACF can create capacity for competition authorities to better regulate data issues.

RECOMMENDATIONS

- Strengthen regulatory cooperation and knowledge sharing among African countries and regions by building capacities of the African Network of Data Protection Authorities and the Regional Association of ICT Regulators.
- Existing continental and regional adjudication mechanisms should be explicitly empowered to deal with data issues implicated in digital rights and data rights and cross-border data disputes.
- African tax authorities should collaborate through the African Taxation Administration Forum (ATAF) to develop an African position to more effectively represent common interest in the international taxation reforms process, such as BEPS.
- Establish an Annual Data Innovation Forum for Africa to serve as a platform for multi-stakeholder discussions, facilitate exchanges among Countries and raise awareness of policymakers on the power of data as the engine of today's digital economy.

5.6. IMPLEMENTATION FRAMEWORK

5.6.1 PHASES OF IMPLEMENTATION FRAMEWORK

It should be noted that while the activity areas below are identified as phases, their fulfilment is not strictly linear. Particularly, Phases 2 and 3 are considered concurrent processes which can occur alongside domestication activities. The implementation framework should be read in conjunction with the stakeholder mapping outlined in 5.6.2

	Activity	Description	Lead Responsibility
PHASE 1: ADOPTION OF THE FRAMEWORK			
A	Member states adopt Framework		Members
B	Design of Monitoring for Framework	High-level monitoring framework established.	AUC
C	Establish or empower a mechanism within the AU for centralising regional engagements on data.	Activities to include implementation support, coordination on data standards, and other specific areas enunciated in the recommendations requiring regional collaboration	AUC
PHASE 2: ESTABLISHING BUY-IN/OWNERSHIP			
A	Assess Continental Framework	Ensure alignment with continental instruments	AUC, RECs, AUDA-NEPAD Smart Africa
B	Engage Continental Structures	Engage associated structures on potential areas of collaboration in implementing the framework	AUC
C	Assess International Frameworks	Focusing on principles, explore alignment with frameworks of international structures	AUC
D	Engage International Structures		AUC, AU Member States
PHASE 3: CONTINENTAL SUPPORT FOR MEMBER STATES TO MEET PRECONDITIONS			
A	Develop broadband infrastructure and regulatory frameworks	Broader policy implementation initiated in relation to the enabling data environment domestically.	RECS, AUDA-NEPAD, ATU, PAPU, SMART AFRICA

	Activity	Description	Lead Responsibility
PHASE 4: DOMESTICATION			
A	Multi-stakeholder engagement	Leveraging the Policy Framework, engage domestic actors	Members, private sector, civil society
B	Establish multi-stakeholder buy-in	Reflecting on the stakeholder mapping under Phase Two*, ensure policy alignment	Members
C	Domesticate instrument	Develop Legal and Regulatory Frameworks, establish data regulators and data governance systems.	Members
D	Budgetary framework	Allocate resources for implementation.	Members
PHASE 5: COLLABORATION			
A	Engage Decision-Making International Fora	Engage rule-making fora on data standards and rules (see stakeholder mapping)	AU Member States
B	Monitoring of member implementation		AUC, RECs, AUDA-NEPAD, Smart Africa
C	Drive awareness on the centralising continental mechanism on data.	Accept direct requests for assistance	AUC, Regional Institutions
D	Participate in continental activities	Participate in the continental activities outlined in Section 10	Members

5.6.2 STAKEHOLDER MAPPING

A cursory stakeholder mapping is provided to facilitate implementation, particularly in Phase 2, Phase 4 and Phase 5.

DESCRIPTION	SUB-TYPES	PURPOSE
INTERNATIONAL		
United Nations	International Telecommunication Union, UN Department of Safety and Security	Alignment of development policy
Multilateral Organisations	Organisation for Economic Co-operation and Development, World Bank	Alignment of economic policy

DESCRIPTION	SUB-TYPES	PURPOSE
Internet Governance Structures	Internet Governance Forum, Internet Engineering Task Force, Internet Corporation for Assigned Names and Numbers	Alignment of digital and Internet policy
International Standards	International Organisation for Standardisation	Alignment of data standardisation
Multilateral Organisations (sectoral)	World Health Organisation, World Trade Organisation	Alignment of sectoral components of policy
REGIONAL		
Regional Economic Communities	ECOWAS, SADC, EAC, ECCAS, COMESA, IGAD, CEN–SAD, UMA	Alignment of economic and development policy
Internet Governance Structures	AFRINIC, African IGF	Alignment of digital and Internet policy
Regional Community (regulatory)	Network of African Data Protection Authorities, Other Regulatory Associations, African Tax Administration Forum	Cross-border policy alignment
Regional Community (sectoral)	African Development Bank	Alignment of sectoral components of policy
DOMESTIC		
National Departments	Telecommunications, Justice, International Cooperation, State Security	Policy alignment
Statistical Agencies		Capacitation
Regulatory Authorities	Data Protection, ICT Regulation, Competition	Implementation
Firm-level	Data governance committees	Capacitation, multi-stakeholder engagement

RECOMMENDATIONS

Following the endorsement of the AU Data Policy framework by AU Organs, the AU Commission, in collaboration with regional institutions and relevant stakeholders, will develop an Action Plan to guide the implementation of the framework that takes into consideration the digital sovereignty of states as well as the different levels of development, vulnerability of populations and digitisation within AU Member States, namely aspects related the gap in ICT infrastructure and lack of cybersecurity policies and legislations. The action plan (short, medium and long term) will identify roles and responsibilities and emphasise the key priorities and immediate actions both at regional and continental levels, and in line with AU Member States' levels of data maturity.

REFERENCES

African Development Bank. (2019). Annual Report 2019 | African Development Bank—Building today, a better Africa tomorrow. https://www.afdb.org/en/documents/annual-report-2019

Ahmed, S. (2021). A Gender perspective on the use of Artificial Intelligence in the African FinTech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana. 23rd ITS Biennial Conference. https://www.econstor.eu/handle/10419/238000?author_page=1

Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics, 54, 324-340. https://doi.org/10.1016/j.strueco.2020.05.008

Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries. https://www.oecd-ilibrary.org/content/paper/5jlz9h56dvq7-en

Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018

Carrière-Swallow, Y., & Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Cavoukian, A. (2009). Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner.

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Deloitte. (2017). Privacy is Paramount | Personal Data Protection in Africa Personal Data Protection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Global Symposium for Regulators. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Hawthorne, S. (2020). Impact of Internet Connection on Gifted Students' Perceptions of Course Quality at an Online High School. Boise State University Theses and Dissertations. https://doi.org/10.18122/td/1748/boisestate

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

International Telecommunication Union. (2019). Measuring Digital Development Facts and Figures (978-92-61-29511-0). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

International Telecommunication Union. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. The American Economic Review, 110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Khan, M., & Roy, P. (2019). Digital identities: A political settlements analysis of asymmetric power and information. https://eprints.soas.ac.uk/32531/1/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Macmillan, R. (2020). Data Governance: Towards a Policy Framework (Policy Brief No. 9). https://www.competition.org.za/ccred-blog-digital-industrial-policy/2020/7/6/data-governance-towards-a-policy-framework

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). Public Value and Platform Governance (SSRN Scholarly Paper ID 3741641). Social Science Research Network. https://doi.org/10.2139/ssrn.3741641

Mitretodis, & Euper. (2019). Interaction Between Privacy and Competition Law in a Digital Economy. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law. https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

OECD. (2019). Data governance in the public sector. 23–57. https://doi.org/10.1787/9cada708-en

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://opendatacharter.net/principles/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.902.7318&rep=rep1&type=pdf#:~:text=Weak%20data%20sovereignty%20as%20defined,on%20safeguard%2D%20ing%20national%20security.

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Rinehart, W. (2020, September 14). Is data nonrivalrous? Medium. https://medium.com/cgo-benchmark/is-data-nonrivalrous-f1c8e720820b

Saint, M., & Garba, A. (2016). Technology and Policy for the Internet of Things in Africa (SSRN Scholarly Paper ID 2757220). Social Science Research Network. https://doi.org/10.2139/ssrn.2757220

Savona, M. (2019). The Value of Data: Towards a Framework to Redistribute It (SSRN Scholarly Paper ID 3476668). Social Science Research Network. https://doi.org/10.2139/ssrn.3476668

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational health research data collections with software implementations in R. BMC Medical Research Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

Sen, A. (2001). Development As Freedom. OUP Oxford; eBook Collection (EBSCOhost). http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2089308&site=ehost-live

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa. https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

Taylor, L. (2019). Global data justice. Communications of the ACM, 62(6). https://doi.org/10.1145/3325279

Teh, H., Kempa-Liehr, A., & Wang, K. (2020). Sensor data quality: A systematic review. Journal of Big Data, 7. https://doi.org/10.1186/s40537-020-0285-1

UNCTAD. (2020). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

UNCTAD. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].

United Nations. (2017). Looking to future, UN to consider how artificial intelligence could help achieve economic growth and reduce inequalities—United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/

Van der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic Literature Review on the Spread of Health-related Misinformation on Social Media. Social Science & Medicine, 240, 112552. https://doi.org/10.1016/j.socscimed.2019.112552

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop, N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

World Bank. (2021). Data for Better Lives. World Bank. Doi : 10.1596/978-1-4648-1600-0

World Bank, & ITU. (2020). The World Bank and International Telecommunication Union launch handbook on digital regulation [Text/HTML]. World Bank. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

World Economic Forum. (2016). Networked Readiness Index. Global Information Technology Report 2016. http://wef.ch/29cCKbU

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf

ANNEX - WORKING DEFINITIONS

Anonymisation is the removal of direct and indirect personal identifiers from data.

Cloud services are used on-demand at any time, through any access network, using any connected devices that use cloud computing technologies. They utilise software and applications located on the cloud and not on users' own devices.

Cloud-based services include mass-market applications (i.e. social media and webmail offered over the Internet). The data does not sit on the individuals' devices but is stored remotely in a data centre. Examples include Facebook, YouTube and Gmail.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Continental, for the purposes of this framework, refers to Africa.

Cybercrime: Unlawful acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure (Malabo Convention).

Cybersecurity: Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access (*https://digitalguardian.com/blog/what-cyber-security*).

Data classification is broadly defined as the process of organising data by relevant categories so that it may be used and protected more efficiently.

Data controller means any natural or legal person, public or private, any other organisation or association that alone or jointly with others, decides to collect and process personal data and determines the purposes.

Data ecosystem - for the purposes used here not only to the programming languages, packages, algorithms, cloud-computing services, and general infrastructure an organisation uses to collect, store, analyse, and leverage data, but to the underlying value chain associated with data as a factor of production, the governance of data systems and the protection of data subjects.

Datafication refers to the process by which daily interactions of living things can be rendered into a data format and put to social and economic use.

Data minimisation is a principle within data protection frameworks, which entrenches collecting the minimum amount of personal data needed to deliver an individual element of a service or product.

Data protection regulates how data is used or processed and by whom, and it ensures citizens have rights over their data. It is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between 'data subjects' and the institutions or people who collected data.

Data protection authorities (DPAs) are independent public authorities that monitor and supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law.

Data subjects means any natural person that is the subject of personal data processing (Malabo Convention).

Digital identity is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person, enabling the distinction of one individual from another.

Digital capability is the term used to describe the skills, literacy, social norms, and attitudes that individuals and organisations need to thrive, live, learn and work in a digital society and economy.

E-commerce can be summarised as commercial transactions occurring through electronic channels - buying and selling of goods or services via the Internet and the transfer of money and data to complete the sales - by methods specifically designed for the purpose of receiving or placing orders.

Foundational data infrastructure refers to advanced technologies which facilitate the intensive use of quality data. This may include broadband networks, data centres and cloud services, electronic hardware and software, and digital applications available on the Internet.

Harmonisation is ensuring uniformity in the systems through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g. for levels of assurance) to set rules and build confidence in respective systems.

Interoperability is the ability of different function units – e.g. systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units (adapted from ISO/IEC 2382:2015).

Level of assurance (LOA) is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity (ID4D Public-Private Cooperation). The overall level of assurance is a function of the degree of confidence that the applicant's claimed identity is their real identity (the identity assurance level or IAL), the strength of the authentication process (authentication assurance level or AAL), and—if using a federated identity — the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from NIST 800-63:2017).

Open standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus-driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T).

Open data: Open means anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness (*http://opendefini- tion.org/*).

Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Privacy and security by design means proactively embedding privacy and security mechanisms into the design and operation of products and services, both non-IT and IT systems, networked infrastructure, and business practices. This requires that privacy and security governance is considered throughout the whole engineering process and product lifecycle.

Pseudonymisation is processing of data so that it cannot be associated with an individual without additional information.

Regional for the purposes of this Framework refers to the five regions of Africa recognised by the African Union.

Sensitive data means all personal information relating to religious, philosophical, political opinion as well as to sex life, race, and health, social conditions of the data subject (Malabo Convention).

Department of Infrastructure and Energy
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int