African Union

An Integrated, Prosperous and Peaceful Africa

Guidelines for Integrating Data Provisions in Protocols on Digital Trade

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

The *Guidelines for Integrating Data Provisions in The Protocol on Digital Trade* were prepared under the overall guidance of H.E Dr. Amani Abou-Zeid Commissioner for Infrastructure and Energy, AU Commission team comprising Dr. Kamugisha Kazaura, Director of Infrastructure and Energy Department, Mr. Moses Bayingana Ag. Head of Information Society Division and Ms. Souhila Amazouz, Senior Digital Policy Officer (Taskforce Coordinator) as well as valuable contributions and inputs from the Taskforce Members representing Regional Economic Communities, AUDA-NEPAD, AU Specialized Institutions, Regional and Pan-African Organizations, Network of African Data Protection Authorities (NADPA) as well as UN Agencies and International Organizations operating in Africa in the field of data and digital trade.

The framework benefited from financial support from GIZ and technical support from Mr. Paul Baker, CEO of International Economic Consulting Ltd.

Comments were also received at various stages of production of this document by African experts from AU Member States attending the virtual validation workshops.

These Guidelines were endorsed by the 44th Ordinary Session of the Executive Council held in February 2024 and they are in line with the AU Data Policy Framework endorsed by the AU Summit in February 2022.

ACRONYMS

4IR	Fourth Industrial Revolution
ADR	Alternative Dispute Resolution
AfCFTA	African Continental Free Trade Agreement
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
ASEAN	Association of Southeast Asian Nations
AU	Africa Union
B2B	Business-to-Business
BATNA	Best Alternative to a Negotiated Agreement
CAGR	Compound Annual Growth Rate
CBPR	Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEA	Digital Economy Partnership
DEPA	Digital Economy Partnership Agreement
DFFT	Data Free Flow with Trust
DMF	Data Management Framework
DPA	Data Protection Act
DSM	Dispute Settlement Mechanism
DTS	Digital Transformation Strategy
E-Commerce	Electronic Commerce
ECOWAS	Economic Community of West African States
EU	European Union
FTA	Free trade Agreement
G20	Group of Twenty
GATS	General Agreement on Trade in Services
GBP	Great British Pound
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GMV	Gross Merchandize Volume
ICT	Information and Communications Technology
IFC	International Finance Corporation
IoT	Internet of Things
ISP	Internet Service Providers
JSI	Joint Statement Initiative
MCCs	Model Contractual Clauses
OECD	Organisation for Economic Cooperation and Development
POPIA	Protection of Personal Information Act

RCEP	Regional Comprehensive Economic Partnership
RECs	Regional Economic Communities
RTAs	Regional Trade Agreements
SADC	Southern African Development Community
SDG	Sustainable Development Goal
TAPED	Trade Agreements Provisions on Electronic-commerce and Data
TCA	Trade and Cooperation Agreement
TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDG	United Nations Development Group
US	United States
US$	United States Dollar
USMCA	United States–Mexico–Canada Agreement
WEF	World Economic Forum
WTO	World Trade Organization
ZOPA	Zone of Possible Agreement

1. INTRODUCTION

1.1. GLOBAL DEVELOPMENT TREND OF THE DIGITAL ECONOMY

Digitalisation has become a main source of socio-economic growth. The digital economy was worth US$11.5 trillion globally, equivalent to 15.5% of global GDP in 2016, and has grown two and a half times faster than global GDP since 2000 (Huawei & Oxford Economics, 2017). Progress in expanding connectivity has brought enormous opportunities for socio-economic development. Nowadays, 95% of the world's population is covered by a mobile broadband network, and 63% of the global population was using the Internet in 2021 (GSMA, 2022; ITU, 2021). According to GSMA (2023), in 2023, mobile technologies and services generated US$5.2 trillion of economic value added or 5 percent of GDP. Digital connectivity has also shown its role in fostering societal resilience during the COVID-19 crisis by enabling people to continue their usual economic and social activities during the worldwide lockdowns of 2020-2021 (ICC, 2022).

Digital trade has also been expanding at an impressive pace. In terms of e-commerce merchandise trade, UNCTAD estimates that global e-commerce sales amounted to US$26.7 trillion globally in 2019, with B2B e-commerce representing 82% of all e-commerce (UNCTAD, 2021). The COVID-19 pandemic has undoubtedly altered shopping behaviour from offline to online (UNCTAD, 2021). Trade in digitally-delivered services has also been increasing over the years, growing by around 7% a year between the 2005-2021 period. In 2021, exports of digitally-delivered services amounted to USD 3.8 trillion, accounting for approximately 63% of global trade in services, according to UNCTADStat.

Data is embedded in all of the frontier technologies that are propelling the digital economy.[1] Data does not only serve as an input for the production of goods and services, but it also possesses unique characteristics (see Box 1) that have allowed it to become a factor of firm competitiveness (Hagiu & Wright, 2020). As noted by Giddlings et al. (2021), *"the ongoing economic and financial digitalisation is making individual data a key input and source of value for companies across sectors, from bigtechs and pharmaceuticals to manufacturers and financial services providers. Data on human behaviour and choices—our "likes," purchase patterns, locations, social activities, biometrics, and financing choices—are being generated, collected, stored, and processed at an unprecedented scale."*

1 ADBC - artificial intelligence, blockchain, cloud and data—are considered the alphabet of the future. See (GovTech Singapore, 2018; CloudSufi, 2021)

Box 1. The unique characteristics of data

The added-value of data comes from the processing, transmission, storage and combination of data. Data are intangible and non-rival, which means that many people can use the same data simultaneously or over time, without depleting them. At the same time, access to data can be limited by technical or legal means, resulting in varying degrees of excludability. For example, data collected by major global platforms are not readily available for others to use, giving the platform owners a monopolistic position to benefit from the data. Moreover, aggregated values may often be greater than the sum of individual values, especially if combined with other complementary data.[...] Moreover, data are of a multidimensional nature. From an economic perspective, they can provide not only private value for those who collect and control the data, but also social value for the whole economy. The social value cannot be ensured by markets alone. Furthermore, the distribution of private income gains from data is highly unequal. As a result, there is a need for policymaking to support efficiency and equity objectives. However, there are also non-economic dimensions to consider, as data are closely related to privacy and other human rights, and national security issues, all of which need to be addressed. From the perspective of the socio-economic benefits, data can serve as fundamental conditions or enablers that allow governments to deliver more effective public services, offer effective environmental stewardship, and improve on the transparency and governance of government actions. Due to these benefits, the need for open data, interoperability standards and data-sharing initiatives have been emphasised 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. Source: (UNCTAD, 2021; African Union, 2022)

1.2. THE POTENTIAL OF AFRICA'S DIGITAL ECONOMY

Africa's digital economy is poised to become a huge and resilient source of growth. The continent has seen substantial mobile phone growth, with 61% and 40% of the population now having access to mobile phones and the Internet, respectively. Growth in broadband services is impressive, led by mobile broadband, which reached 42% of the population in 2022 (ITU, 2022). According to a jointly developed report by IFC and Google (2020), the African digital economy has the potential to add up to US$180 billion to Africa's gross domestic product (GDP) by 2025. Currently, nineteen of the top twenty fastest-growing countries in the world are in Africa. The continent also has the world's youngest, fastest-growing, and increasingly urbanised workforce (Google & IFC, 2020). These demographics, coupled with improved lifespan and education levels, major investments in ICT infrastructure, and improved competition amongst internet service providers (ISPs), are expected to give a boost to both the demand and supply capacity of digital goods and services, contributing to the continental digital economic growth.

While still facing several infrastructure and governance challenges, the African digital economy is driven by young, dynamic digital entrepreneurs. Startups are solving some of Africa's most challenging issues, such as access to healthcare for remote populations, employment opportunities for women, and the ability to securely send and receive money. Many African consumers have experienced a leapfrog of transitioning directly from cash to

mobile payments without ever owning a plastic card – a story admired and followed by many countries globally (Smart Africa Alliance, 2021). The successful history of Africa's mobile-first payment landscape has strengthened the credence of shaping an African solution. The new business models in Africa are now taking advantage of advanced technologies—tailored to data-driven, scalable, and pan-African approaches (Google & IFC, 2020). Africa's data markets are on a path to double every five to six years. The value of data markets in Africa is estimated to reach over USD 3 billion by 2025, growing by over 12% between 2019 and 2025 (Koigi, 2020). The sector received investments of USD 2.6 billion in 2021 (Research and Markets, 2022). The African data centre industry has witnessed steady interest from major global cloud services providers such as AWS and Microsoft, along with Huawei, over the last five years (Koigi, 2020).

1.3. THE CRITICAL ROLE OF DATA IN THE AFRICAN TRANSITION TO DIGITAL ECONOMY

Data has been increasingly contributing to digital and technological transformations by fuelling new business models. In fact, data has been referred to as the new oil (Rotella, 2012), because while both data and oil have intrinsic value, they both must be "refined" or otherwise transformed to realise their full potential (World Bank, 2021). Nowadays, data is considered an asset and a potential source of growth and innovation. The increasing volume of personal, non-personal, industrial, and public data, combined with emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and cloud computing, have dramatically impacted the way data is collected, stored, processed and transmitted across the globe. Data's importance to modern societies demands a high-level and strategic policy perspective that can balance multiple policy objectives – from unleashing the economic and social potential of data to the mitigation of risks associated with the mass collection and processing of personal data.

For Africa, significant opportunities can arise in the near future from digital transformation. The ever-increasing production and use of data have the chance to support the development of a sustainable and inclusive data-driven economy and society in line with Agenda 2063 aspirations. To enable countries to take advantage of the substantial amount of personal, non-personal, industrial, and public data generated by their citizens and industries and to also facilitate the easy flow of data across sectors and across borders, there is a need to foster the establishment of a common data space and creation of an enabling and supportive policy environment to boost innovation and introduction of new business models.

The continent's leadership indicates strong support for prioritising and accelerating digitalisation. The Africa Union (AU)'s Digital Transformation Strategy, adopted by the AU Summit in February 2020, calls for, among other recommendations, the development of continental approaches and policies on cross-cutting issues such as Data Protection, Digital ID, Cybersecurity, and Emerging Technologies. The African Union Data Policy Framework, developed in 2021 by a Pan-African Task Force and endorsed by the African Union Summit in February 2022, sets out a common vision, principles, strategic priorities, and key recommendations to guide AU 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. Furthermore, the Framework aims to optimise cross-border data flows, 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.

The African Continental Free Trade Agreement (AfCFTA) provides an opportunity for cooperation on important aspects of digital transformation and data policy. The wider adoption of the digital underpinnings for continental initiatives, such as the AfCFTA, will be essential to realising the benefits of greater economic cooperation. This can be facilitated by rules mandating better cross-border data interoperability, thus creating a harmonised continental approach to the data-driven digital economy. This approach should strike a balance between, on the one hand, promoting the socioeconomic benefits of digital trade and e-commerce while ensuring that sensitive information remains safe and secure and that the relevant regulations on personal data protection are respected. The on-going negotiations of the AfCFTA Protocol on Digital Trade provide a unique opportunity for AU Member States to harmonise digital economy regulations, including data regulations, to support the collective economic growth from a trade perspective.

In this context, this policy brief aims to provide a key map of principles and guidelines (including recommendations) to promote the responsible, secure, and equitable use of data in trade agreements in the context of the on-going negotiations of the AfCFTA protocol on digital trade as well as the prospective negotiations of the AfCFTA on digital services and goods (the second phase). More significantly, the protocol on digital trade will lay the groundwork for a continental single digital market.

2. OVERVIEW OF THE GLOBAL DATA POLICY LANDSCAPE

2.1 TRENDS IN THE GOVERNANCE OF DATA FLOWS

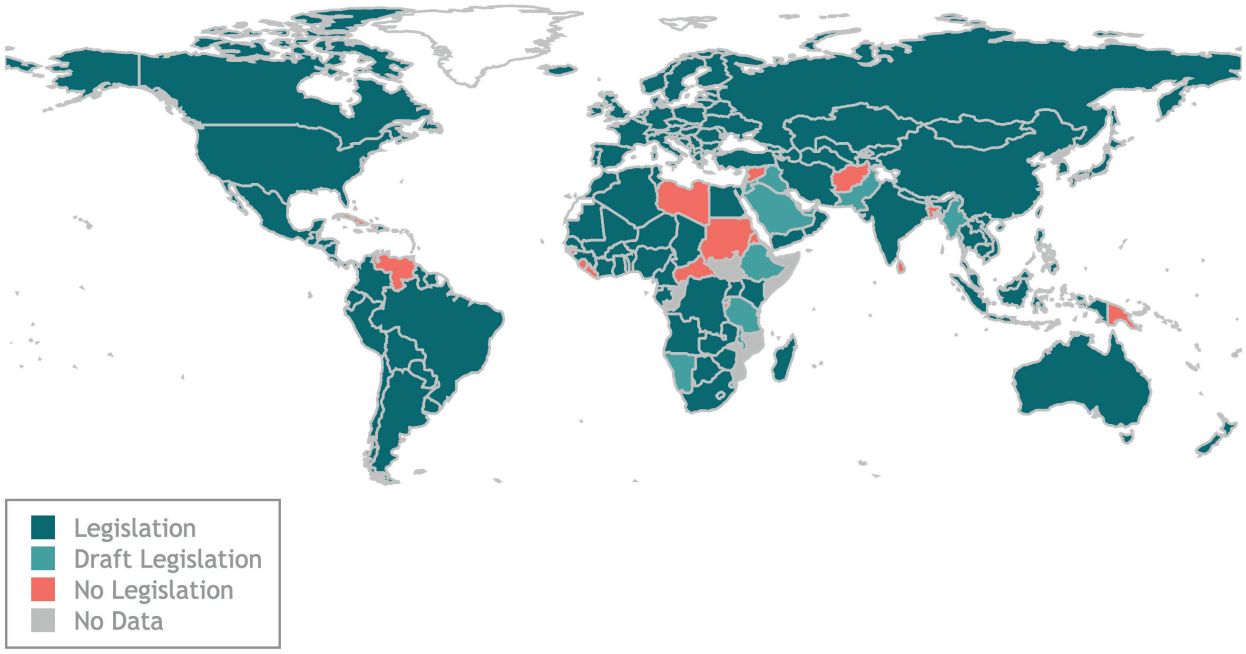
2.1.1. GLOBAL AND REGIONAL DATA GOVERNANCE LANDSCAPE

As data becomes an increasingly integral part of contemporary society and its importance continues to grow in the digital age, the role of effective data governance cannot be underestimated. The governance of data flows has become a crucial issue as data holds considerable economic value and merits proper use and protection of sensitive information. As such, there have been various trends in the governance of data flows, each seeking to address the challenges posed during the collection, processing, use, and monetarisation of data.

Data governance frameworks have been driven by the need to balance the increasing importance of data as an asset and the need to protect individuals' privacy rights. This gives rise to diverse focuses of different jurisdictions in regulating data-related issues depending on states' views of who should 'control' data. For example, there are currently three major focuses of the three digital kingdoms. The United States focuses on control of the data by the private sector, China emphasises control of data by the Government, meanwhile the European Union (EU) favours control of data by individuals based on fundamental rights and values (UNCTAD, 2021).

One of the most prominent trends in the governance of data flows is the adoption of data protection laws (UNCTAD, 2016). Data protection laws seek to regulate the collection, processing, and storage of personal data (Crocetti, Peterson, & Hefner, n.d.). As of December 2021, around 71% of countries globally have implemented laws on data protection and privacy, while 9% have draft legislation (Figure 1) (UNCTAD, 2021). Globally, data protection laws and regulations vary across countries and in the case of the United States, for instance, vary across states. Among all existing data protection legislation, the EU's General Data Protection Regulation (GDPR) is considered the toughest set of privacy rules, which has given rise to several GDPR-like data privacy laws (Satariano, 2018; Simmons, 2022).

Figure 1. Data Protection and Privacy Legislation Worldwide, 2021



Source: UNCTA, 14/12/2021

Moreover, there has been increasing convergence toward greater transparency in the governance of data flows. There are greater expectations both from regulators and consumers for increased transparency regarding data practices (Harvard Business Review, 2021). Organisations are expected to provide individuals with clear information on how their data is collected, processed, and stored.

Many countries are also increasingly introducing data localisation regulations. Given that data can be sensitive to national security, there is increasing concern over whether data needs to be stored and processed within a country's borders (Yayboke & Ramos, 2021). Hence, certain countries are introducing laws that require data to be stored within the jurisdiction where it was collected. Between 2017 and 2021, the number of jurisdictions with data protection laws increased significantly, rising from 35 to 62. These 62 countries implemented a total of 144 restrictions pertaining to data localisation, in contrast to 2017, when only 67 such measures were in place (Cory & Dascoli, 2021).

While deemed necessary for security reasons, data localisation requirements can create barriers to cross-border business operations and international trade (Hinrich Foundation, 2019). Data localisation policies also increase the cost of business for foreign companies, thereby decreasing their global competitiveness. In a study conducted by the Information Technology and Innovation Foundation, it was found that increasing data restrictiveness by 1% can lead to a decline of 7% in a country's gross trade output, a decline of 2.9% in productivity, as well as a drop of 1.5% in downstream prices (Cory & Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, 2021).

Data localisation is closely associated with data sovereignty. The concept of data sovereignty advocates that data should be subject to the laws and regulations of the country in which it is generated. The demand for data sovereignty is driven by concerns about the control and ownership of data, particularly in the context of cloud computing and cross-border data flows (Gao, 2022). This concern has emerged predominantly in the context of multinational corporations that may store data in multiple locations. Certain countries have adopted a stance on data sovereignty, implementing regulations that require companies to store data locally and provide the government with greater access to this data (Kuo, 2022).

On the other end of the spectrum, there have been initiatives to support free flows of data. While the two concepts do not necessarily contradict, they present different perspectives on data governance approaches. As early as 2000, the Joint Statement on Electronic Commerce of the Jordan–US FTA already highlighted the 'need to continue the free flow of information'. Since then, an increasing number of regional trade agreements (RTAs) have embedded similar aspirations and commitments. In 2019, the Data Free Flow with Trust (DFFT) initiative was proposed by Japan and endorsed by members of the G20 group of nations (Kudo & Soble, 2022), while the EU embraced a more cautious approach to promoting 'free flow of non-personal data' (European Commission, 2023).

Additionally, open data, especially open government data, has focused on transparency and innovation-enabling aspects of data. An increasing number of countries and institutions recognise that data is a valuable resource that can be used to propel innovation and create new opportunities (World Bank, n.d.). As such, they advocate for non-sensitive and non-personal data to be made freely accessible and usable. Many governments around the world are increasingly opening their data to the public, making it available for use by different stakeholders (OECD, 2020). For instance, the UK Government launched data.gov.uk, an online portal with data published by the UK central government, local authorities, and public bodies on a range of sectors and topics, including the economy, health, transport, and education, among others (data.gov.uk, n.d.).

Given the diverse approaches to data governance, businesses engaging in international trade may thus face difficulties and increasing compliance costs in multiple jurisdictions. To mitigate the challenges posed by varied regulations, it is important for countries to engage in the development and adoption of international standards regarding data governance that can assist in streamlining and harmonising regulations. Numerous international frameworks, most remain voluntary, have been designed in this respect to provide guidance on best practices for data governance. Below are some of the most significant frameworks adopted worldwide. A more comprehensive review of the best practices is provided in Annex 2.

The United Nations (UN) has developed a set of data privacy principles that aim to promote the responsible use of data for sustainable development while also safeguarding privacy and protecting human rights (UN Global Pulse, n.d.). These include the UN Principles on Personal Data Protection and Privacy 2018 (the 'Principles') and the UN's Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection (the 'Guidance'). These Principles aim to: (i) harmonise standards for the protection of personal data across the UN System; (ii) facilitate the accountable processing of personal data; and (iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy. These Principles may also be used as a benchmark for the processing of non-personal data (United Nations, 2018).

The Organization for Economic Cooperation and Development (OECD) Privacy Guidelines are also an important international framework for data protection. The OECD Privacy Guidelines were first adopted in 1980 to guide the responsible handling of personal data and have since been updated and revised to conform with the rapidly changing landscape of data privacy (OECD, n.d.). The OECD's Privacy Guidelines are based on certain fundamental principles centred around the importance of data quality, purpose specification, accountability, and individual rights (OECD, 2013). One of the key characteristics of the OECD Privacy Guidelines is their emphasis on cross-border data flows. The OECD Privacy Guidelines emphasise the importance of adopting comprehensive data protection laws that include provisions for cross-border data transfers whereby adequate safeguards need to be maintained in such transfers. Moreover, the Guidelines state that any limitations imposed on the transborder flow of data must be proportional to the risks (OECD, 2013).

The APEC Privacy Framework provides principles for the collection, holding, processing, use, transfer, or disclosure of personal information applied to persons or organisations in the public and private sectors who control each of the afore-mentioned processes. This Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows (APEC, 2005). In implementing the APEC Privacy Framework, the APEC Cross-Border Privacy Rules (CBPR) System provides a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognised data privacy protections (APEC, 2019). The CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework.

A more recent initiative, the World Economic Forum (WEF) Data Free Flow with Trust (DFTT), aims to facilitate the free flow of data while ensuring trust in data privacy and security. The DFFT initiative is founded on the premise that the free flow of data is crucial for economic growth and innovation and that data protection and privacy are key to maintaining trust in the digital economy (WEF, 2020). Hence, the initiative seeks to find a balance between promoting the free flow of data and the protection of personal information. A roadmap for cooperation was adopted in 2021, focusing on four areas of cooperation, namely data localisation; regulatory cooperation; government access to data; and data sharing for priority sectors (Arasasingham & Goodman, 2023). An action plan was further designed in 2022. Given its international scope and the focus of the private sector, the initiative could help to reduce regulatory fragmentation globally, which would ease businesses' accessibility and use of data across borders.

The EU GDPR as a comprehensive and robust regulations on Personal data protection. Given its depth and broad scope of coverage, the GDPR has served as an inspiration for developing legislation around the world. The EU GDPR is applied outside of the EU territory, requires consent for the processing, collecting or using of information on EU subjects, recognises privacy rights for data subjects, and provides sanctions for non-compliance. The EU GDPR also imposes certain restrictions on the transborder flow of personal data. As per the provisions of the GDPR, personal data can only be transferred to territories where an adequate level of protection is guaranteed under domestic laws. The European Commission is responsible for determining the adequacy of the level of data protection in non-EU countries. Only a few countries are recognised as having adequate laws (European Commission, n.d.).[2] Where there is no adequacy, organisations have recourse to other legal mechanisms to transfer personal

2 The countries that have been recognized as having adequate data protection laws by the EU Commission include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

data outside of the EU. These can include standard contractual clauses, binding corporate rules, codes of conduct and certification mechanisms (European Commission, n.d.).

The robust development of legislation on data protection reflects the crucial roles of data and data flow in the economy. In the modern society, data has been the force driving disruptive "data-driven innovation" and profitable business models, such as platform companies or the data-aggregators (Thirani & Gupta, 2017; Redman, 2015). In addition to its economic benefits, the role of data goes beyond the relatively narrow perspective of a firm's business models to touch upon the multiple facets of the society, such as personal privacy and security. In this context, there is a need for a balanced approach to ensure the economic benefits of data-driven innovation are captured while social se curity and personal privacy remain properly protected. The next section will discuss several efforts at the multilateral, regional, and country levels in order to reach this balancing point.

2.1.2. MULTILATERAL AND REGIONAL TRADE AGREEMENTS THAT INCLUDE PROVISIONS ON DATA

(I) WTO DISCIPLINES ON DATA ISSUES

While being considered as 'pre-internet law', the existing WTO multilateral rules still have certain applicability to data governance measures. The principle of technological neutrality provides an important basis for applying the existing GATS rules to e-commerce (Mattoo & Schuknecht, 1999). Basically, this principle seeks to ensure no policy distinctions between products based on the means of delivery, thus allowing a rule's longevity and equal application across different technologies (Greenberg, 2016). A Report of the WTO Council for Trade in Services (1999) provides that *"Members agreed that the GATS applied to all services regardless of the means of technology by which they were delivered. ... It was noted that the principle of technological neutrality also applied to scheduled commitments, unless the schedule specified otherwise: it was, therefore, possible for Members to schedule commitments in a non-technologically neutral manner"* (WTO, 1999). The WTO progress report for Work Programme on Electronic Commerce also confirms the technological neutrality of the GATS *"in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied"* (WTO, 1999). This provides an important ground for reading the WTO Members' schedules of commitments: restricting or banning cross-border data flows, thus obstructing the cross-border supply of services in sectors where members have made explicit GATS commitments could violate market access obligation (Mitchell & Hepburn, 2017).

The WTO General Agreement on Trade in Services (GATS) provides important ground for imposing legitimate measures to protect personal data and privacy. Specifically, Article XIV(c)(i) acknowledges the importance of privacy protection and therefore allows derogation to Members' existing obligations where it is necessary to protect the privacy of individuals in relation to the processing and dissemination of personal data.[3] The exception on 'public morals' under Article XIV(a) GATS can also be interpreted to cover privacy. Furthermore, the GATS Telecommunications Annex also allow for measures "necessary to ensure the security

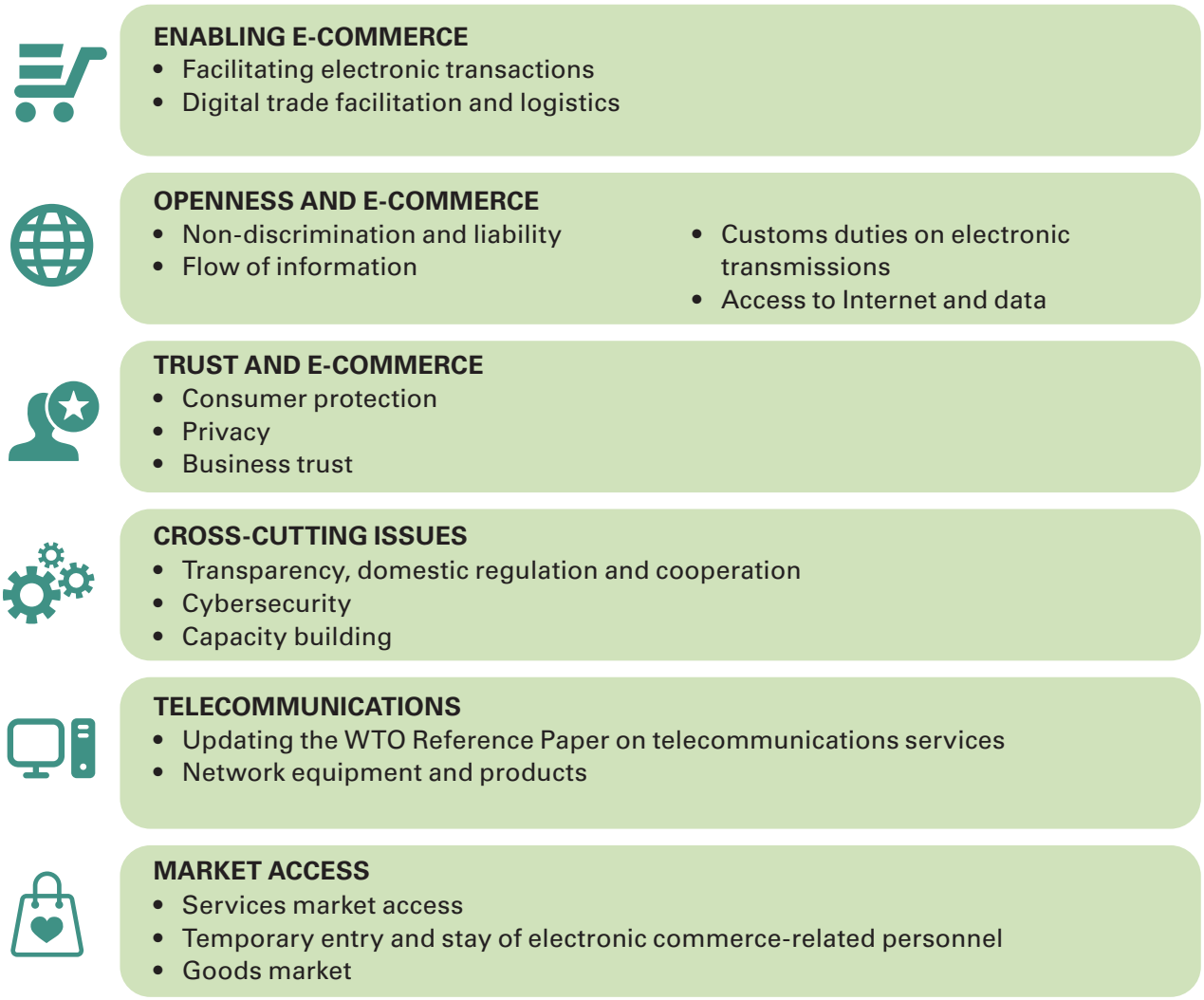
3 Article XIV(c)(i) of the GATS: "Nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

and confidentiality of messages."[4] As a rule of thumb for all GATS exceptions, these measures should not be adopted on a discriminatory basis or for protectionist purposes. It is also worth noting, however, that the GATS does not specifically address data and personal information protection, thus resulting in crucial gaps in this international trade regime in the digital age.

In the absence of explicit rules for digital trade in WTO Agreements, the Joint Statement Initiative (JSI) on E-Commerce presents a step towards data governance discipline. In 2017, at the 11th Ministerial Council, 76 WTO Members agreed to initiate work towards future negotiations on matters pertaining to e-commerce, including data governance. The JSI consolidated draft negotiating text is centred on six key areas, as presented in Figure 2. At the end of March 2023, participants involved in the initiative convened to discuss various proposals relating to e-commerce, including data flow (WTO, 2023). In an earlier statement, it was communicated that Members had achieved good consensus on areas such as online consumer protection; unsolicited commercial electronic messages; open government data; and open internet access (WTO, 2021). Meanwhile, Members are still finding convergence on topics such as data protection and privacy, cross-border data flows, source code and cryptography (WTO, 2023). The same tug-of-war on data governance issues is also featured in the Trade in Services Agreement (TiSA) negotiations. On the one hand, the US advocate for cross-border data transfer, including personal data, in connection with the conduct of the service supplier's business (Berka, 2017). The EU, on the other hand, opposes such a proposal on the grounds that "the right to privacy should have to be recognised as fundamental rights, not as a trade barrier" and promotes the adequacy system (European Parliament, 2016).

4 Paragraph 5(d) of GATS Telecommunications Annex states: "[A] Member may take such measures as are necessary to ensure the security and confidentiality of messages, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services".

Figure 2. Key areas from WTO E-Commerce JSI negotiations



Source: (WTO Plurilaterals, n.d.)

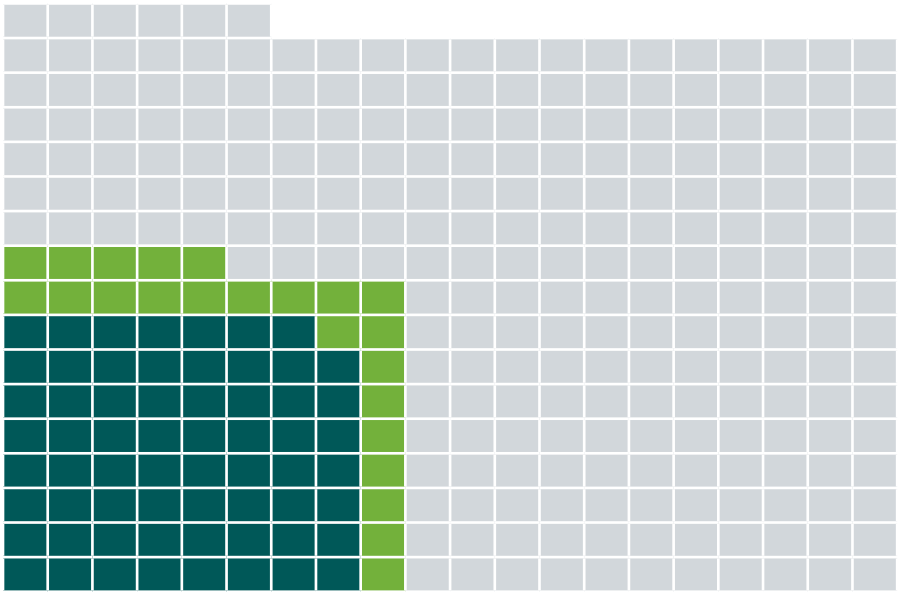
(II) KEY DATA PROVISIONS IN RTAS

An increasing number of RTAs include provisions relating to digital trade and subsequently also incorporate certain provisions pertaining to data. In a recent study, Burri (2021) finds that out of 347 RTAs concluded between 2000 and 2019, 184 contained provisions on digital trade, thus amounting to more than half of the RTAs signed during that period (Burri, Big Data and Global Trade Law, 2021). The incorporation of such provisions experienced a greater rise from 2010 onwards, with 68% of all RTAs concluded between 2010 to 2019, including some type of provision on digital trade. Likewise, across the years, the number of provisions included under such chapters increased. For instance, in 2000, the average number of articles pertaining to digital trade was one. In 2019, the average number of articles relating to digital trade increased to thirteen (Burri, Big Data and Global Trade Law, 2021). However, it is noted that the provisions contained in these chapters are highly diverse and address a range of different topics ranging from e-commerce and paperless trade to data protection. Moreover, it was also found that the level of enforcement of these provisions varies between agreements.

Data provisions are a relatively new phenomenon to RTAs. The United States has played a prominent role in incorporating provisions relating to data in its RTAs, pushing for liberal rules in light of its 'Digital Agenda' (Burri, Big Data and Global Trade Law, 2021). Agreements that were concluded with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, Panama, Colombia, and South Korea all contained provisions pertaining to digital trade, whereby the US has gone above and beyond WTO commitments on the matter.

However, other countries, namely Singapore, Australia, Japan, and Colombia, have equally played an important role in diffusing such provisions in RTAs (Burri, Big Data and Global Trade Law, 2021). Up to 2020, according to the DESTA database, sixty-three out of 346 RTAs signed since 2000 (or 18% of all) include data provisions (Figure 3). Over the years, the number of FTAs, including e-commerce provisions, remains higher than those containing data, indicating the still reluctance of countries to incorporate rules on data governance in trade agreements.

Figure 3. Data and E-commerce coverage of all FTAs signed since 2000



25%
(**86** out of 346) of the FTA covers E-commerce provisions

18%
(**63** out of 346) of the FTA covers data provisions. They also cover E-commerce provisions.

FTA that includes only E-commerce provisions.

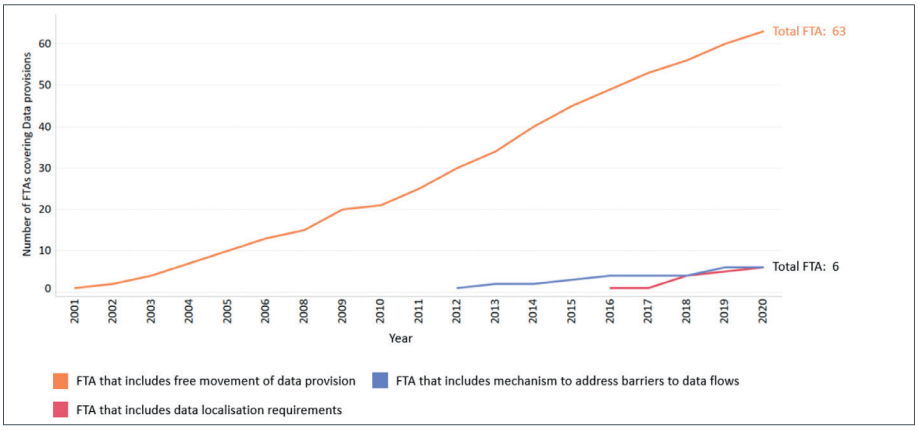
FTA that includes both data and E-commerce provisions.

FTA that does not include data and E-commerce provisions.

Source: Author calculations based on (Dür, Baccini, & Elsig, 2022)

While the provision of free movement of data has been included since 2001, provisions for mechanisms to address barriers to data flows started only in 2012. The first inclusion was in the Pacific Alliance agreement. At the end of 2020, six such agreements across the world included provisions to address barriers to data flows. These are the Pacific Alliance, the EU-Colombia and Peru, Mexico-Panama, Japan-Mongolia, Argentina-Chile, and EU-Japan agreements. As of 2016, data localisation requirements started to be included in the FTAs. The first one was the Japan-Mongolia agreement, which entered into force in 2016. At the end of 2020, six agreements included data localisation requirements (Figure 4).

Figure 4. FTAs containing Data provisions enforced since 2000 by type of coverage



Source: Author calculations based on (Dür, Baccini, & Elsig, 2022)

(III) A CLOSED EXAMINATION OF DATA PROVISIONS IN SELECTED RTAS

This section assesses some of the most recent and comprehensive agreements that include provisions on data governance. In all, 6 RTAs have been assessed regarding 14 different types of provisions. Table 1 highlights the coverage of different data provisions contained in the selected RTAs.

Table 1. Coverage of different data provisions in RTAs

Agreements	Cross Border Data Flows	Data Localisation	Data Protection	Digital Identities	Open Government Data	Data Innovation	Digital Inclusion	Cooperation	Cybersecurity	Cryptography	Source Code	Online Safety & Security	Spam
CPTPP	Y	Y	Y	N	N	N	N	Y	Y	N	Y	Y	Y
DEPA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
EU-UK TCA	Y	N	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
UK-Singapore DEA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USMCA	Y	Y	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
RCEP	Y	Y	Y	N	N	N	N	Y	Y	N	N	Y	Y

N	The Agreement does not include a specific provision on the subject
Y	The Agreement includes a specific provision on the subject
	Data governance provisions
	Provisions related to responsible, secure and equitable use of data

*Spam or also Unsolicited Commercial Electronic Messages

Source: Author's compilation

In terms of coverage, it is found that all the six selected RTAs include provisions on data governance. The UK-Singapore Digital Economy Partnership (DEA) is the most ambitious agreement studied in the context of this report, with the agreement covering all 14 different types of provisions being assessed. It is followed by the Digital Economy Partnership Agreement (DEPA), containing 13 out of 14 types of provisions pertaining to data. The only area not covered by the DEPA, in this case, relates to provisions on source code. In contrast, the agreements with the fewest provisions on data are the EU–UK Trade and Cooperation Agreement (TCA) and the Regional Comprehensive Economic Partnership (RCEP), with only eight different areas covered in each.

Across all the RTAs, the free flow of information is included as an important provision. The first mention of the free flow of information in any FTA can be traced back to the Jordan-US FTA of 2000, where the Joint Statement on Electronic Commerce expressed the "need to continue the free flow of information" (Burri, Big Data and Global Trade Law, 2021). Recent trade agreements include more substantive provisions on the free flow of information. As per Article 8.61F of the UK-Singapore DEA, neither of the two Parties *"shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person."* The CPTPP, on its part, states that "each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." The wording of the other four agreements is similar in this regard, and hence, there is a greater convergence towards adopting binding provisions in this regard.

Except for the EU-UK TCA, all the agreements assessed include provisions limiting the application of data localisation requirements. In all five agreements, it is prohibited to impose restrictions on data localisation. Article 4.4.2 of the DEPA states that *"no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory"*, and the language contained in the other agreements is very similar. In fact, most RTAs that include provisions on data localisation include strong language and binding commitments. The first agreement with binding commitments on data localisation was the Japan–Mongolia FTA in 2015. The TPP negotiations greatly influenced such provisions in later agreements, including the CPTPP and the USMCA, among others (Burri, Big Data and Global Trade Law, 2021).

As far as the protection of personal data is concerned, five out of six agreements entail binding commitments. Aside from the EU-UK TCA, the provisions on the protection of personal information are consistent across the RTAs. For instance, as per Article 19.8.2 of the USMCA, *"each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade..."* Most of the agreements also state that any legal framework adopted must align with international standards and principles. For this purpose, the USMCA refer to the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). Moreover, the agreements also include binding provisions requiring the adoption of non-discriminatory practices in protecting users of digital trade from personal information protection violations and the publication of personal information protections it provides to users of digital trade.

Aside from these three key areas of data governance, an increasing number of RTAs also seek to incorporate provisions aimed at ensuring the responsible, secure, and equitable use of data. For this assessment, 11 different areas have been identified and assessed as per Table 1. In this regard, the provisions contain a mix of both binding and non-binding commitments. For instance, when it comes to the transfer and access to source codes, all four agreements where the subject is covered include binding commitments. In this respect, the CPTPP states that "no Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory." At the other end of the spectrum, provisions on digital innovation, contained only in the DEPA and the UK-Singapore DEA, for instance, are best-endeavour provisions and, therefore, are non-binding.

2.2 AFRICAN POLICY AND REGULATORY FRAMEWORK ON DATA FLOW

The African continent has been proactively embarking on the digital transformation journey. In 2020, the AU Summit adopted the **AU Digital Transformation Strategy (DTS)** for Africa 2020-2030, which aims to guide a common, coordinated African response to the challenges and opportunities of the Fourth Industrial Revolution (4IR) as it sets out the objectives of achieving universal access to digital networks and establishing a Digital Single Market (DSM) by 2030.

As per the **AU Strategy on Enabling Policy and Regulatory Environment for Africa's Digital Single Market,** Single Data Market is identified as one of the three key pillars supporting the realisation of the African DSM.[5] In order to realise the potential benefits of having a common data market, enabling legal frameworks are needed throughout African countries to enable and facilitate the free flow of data. Enabling legal frameworks are critical to the development of a common data market in Africa because they provide the necessary rules and regulations for the free flow of data across borders. Such frameworks are necessary to ensure that data can be collected, shared, and analysed without intruding on individual rights, national security concerns, or intellectual property laws. By providing a clear and consistent set of rules and regulations for data collection, sharing, and analysis, these frameworks can help to unlock the potential of data-driven development in Africa. The following sections, sub-chapters 2.2.1 and 2.2.2, highlight some of the key advances made in this regard at the regional and country levels, respectively.

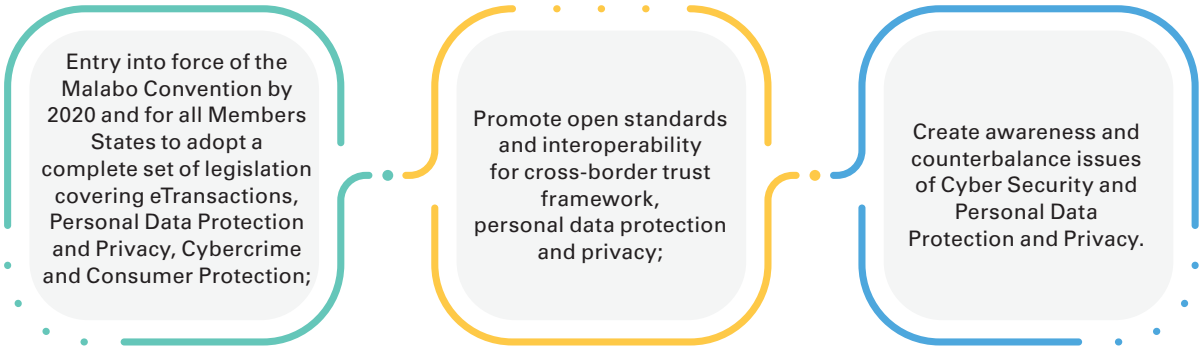
2.2.1 CONTINENTAL AND REGIONAL FRAMEWORKS

(I) DIGITAL TRANSFORMATION STRATEGY FOR AFRICA

The Digital Transformation Strategy for Africa (DTS) 2020-2030 is the key instrument guiding the digital journey of the continent. The DTS, endorsed at the 36th Ordinary Session of the African Union Executive Council, aims to harness digital technologies and innovation to transform African societies and economies, among other things, for the continent's socioeconomic development and ensure Africa's ownership of modern tools of digital management (African Union, 2020). The DTS sets the agenda for greater coherence across existing and future digital policies and strategies to position Africa as a strategic partner in the global digital economy. Recognising data as a critical driver to digital transformation, integration, innovation and entrepreneurship, trade, and financial services, the DTS noted the challenges around the development and use of good data and proposed various policy recommendations and actions to improve access and use of data. Some of the DTS's specific objectives relating to data governance are presented below.

5 The three pillars are: Single Connectivity Market; Single Data Market; and Single Online Market. See (African Union AU Strategy on Enabling Policy and Regulatory Environment for Africa's Digital Single Market, Adopted by AU Summit in February 2024).

Figure 5. The DTS's specific objectives pertaining to data governance



Source: (African Union, 2020)

The DTS presents an ambitious roadmap with regard to data governance and protection. One of the proposed recommendations under the DTS is to ensure that the Malabo Convention is consistent with international standards in order to ascertain African companies' competitiveness in global markets. The instrument set the goal to establish regulations in 10 out of the 14 areas related to data (as identified in section 2.1.2). The only areas where the DTS has not specified details on the transfer and access to source code in cross-border flows, unsolicited commercial messaging, products utilising cryptography, and data innovation. Thus, if properly implemented and enforced, the objectives of the DTS would result in a fairly robust regulatory landscape for African countries. In this sense, the ambitious scope and coverage of the DTS can serve as an important guideline for negotiators in the context of negotiating data provisions in the context of the AfCFTA's Protocol on Digital Trade.

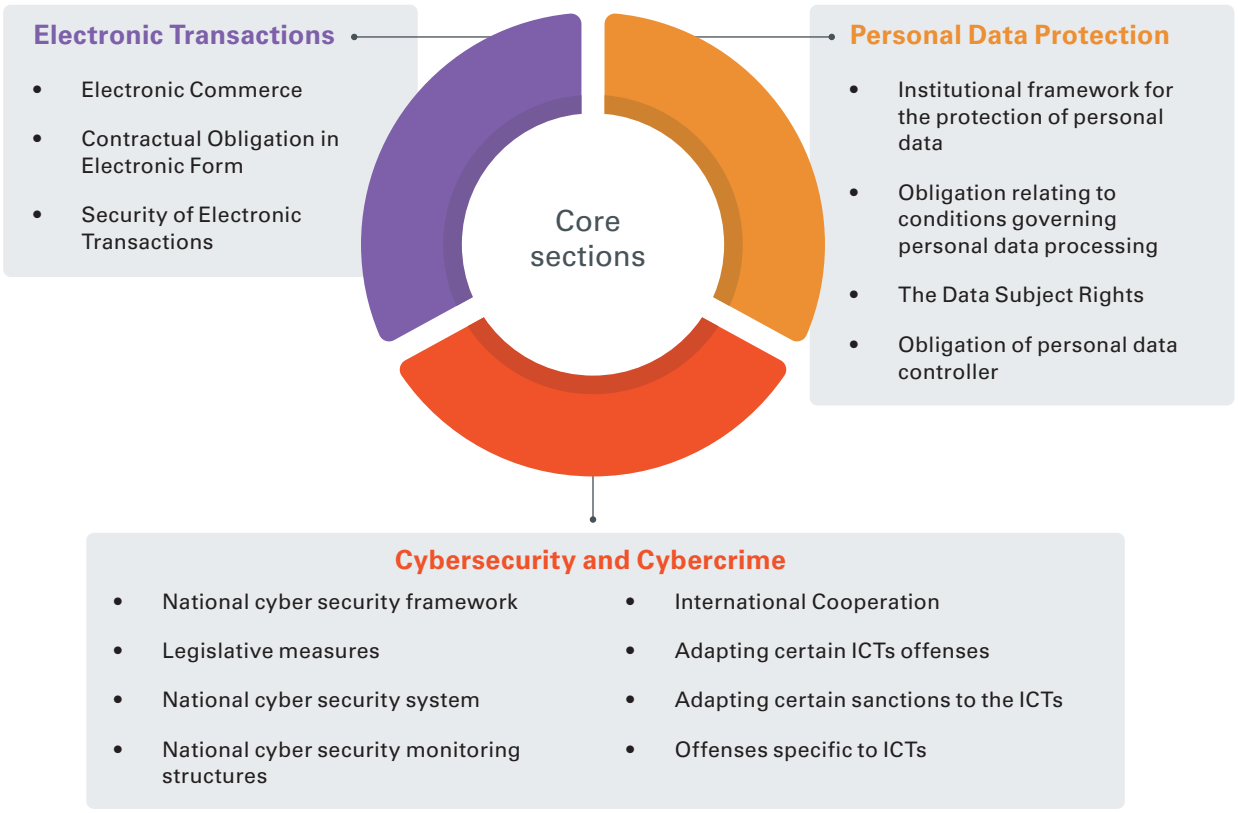
(II) MALABO CONVENTION

Over the past decade, Africa has witnessed the development of various governance instruments intended to address and facilitate the creation and strengthening of Africa's digital ecosystems. In June 2014, the African Union adopted the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) to establish a credible framework for cybersecurity and data protection in Africa. The Malabo Convention was developed in light of the rising importance of data and digital technologies in Africa and the need for comprehensive legal frameworks to govern their use. The Malabo Convention aims to set "the essential rules for establishing a credible digital environment (cyberspace) and address the gaps affecting the regulation and legal recognition of electronic communications and electronic signature; as well as the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems and privacy online" (African Union Commission, 2018).

The Convention focuses on three key areas, notably electronic transactions; personal data protection; and cyber security and cybercrime. The Convention would be fundamental in the development of common standards that promote and regulate data use on the Continent. The Convention provides countries with a common legal framework and aims to establish an enabling ecosystem for the transmission and sharing of data across borders. The various sections of the Convention are summarised underneath. In addition, the Convention also acknowledges the significance of cross-border data flows for economic development in

Africa. It allows for the free flow of data across borders, subject to appropriate safeguards for data protection and cybersecurity. The convention also requires that countries establish mechanisms for the mutual recognition of data protection standards and for the resolution of disputes related to cross-border data flows.

Figure 6. Core sections in the Malabo Convention



Source: (African Union Commission, 2018)

The ratification of the Malabo Convention has been slow owing to numerous factors. As of May 2023, 19 out of 55 African Member States have signed the Convention, of which 15 have proceeded with ratification (African Union, 2023). The latest ratification was undertaken by Mauritania on 9 May 2023, which triggered the entry into force of the convention on 8 June 2023 (Ayalew, 2023).[6] One of the key reasons for the delays surrounding the ratification and implementation of the Convention could be attributed to the lack of dynamism and political will among African countries, many of which have already established national regulations and standards with regard to data governance (Okwara, 2022).

Moreover, there has also been a lack of awareness of the Convention among African countries, with insufficient marketing and momentum generated around it after its adoption in 2014. With the drafting of the AfCFTA's Protocol on Digital Trade, there is an opportunity to further push for the ratification of the Malabo Convention, as it has the potential of providing guidance and direction for concerns and challenges arising from digital trade.

6 The countries that have ratified the Convention include Angola, Cabo Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia.

(III) THE AFRICAN UNION'S DATA POLICY FRAMEWORK

Another important development with regard to data governance on the African continent is the African Union's Data Policy Framework. The AU Data Policy Framework was developed in recognition of the opportunities presented by the DTS and the AfCFTA to address and harness the growth of data that will be enabled by Africa's digital economy (African Union, 2022). The Policy Framework represents a significant step toward creating a consolidated and harmonised data and data governance environment 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.

The 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. It recognises data is a prerequisite for value creation, entrepreneurialism, and innovation in Africa (African Union, 2022). In order to develop and harness data in Africa, the Framework proposes that the generation and development of data across the continent must align with the principles of cooperation; integration; fairness and inclusiveness; trust, safety and accountability; comprehensive and forward-looking; and integrity and justice. As such, when implemented, the Framework will:

1. 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;
2. Create, coordinate and capacitate governance institutions to regulate, as necessary, the ever-changing data landscape and to increase the productive and innovative use of data to provide solutions and create new opportunities while mitigating risk; and
3. 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 (African Union, 2022).

The Framework also proposes that data models and security must be transversal, with specific emphasis on cloud storage and processing of sensitive/proprietary data, API management, and the support of equitable data economies (African Union, 2022). 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.

(IV) DIGITAL IDENTITY INTEROPERABILITY FRAMEWORK

A related framework that has also been advanced by the African Union is the Digital Identity Interoperability Framework. Digital IDs have numerous advantages for a society where governments and businesses, for instance, can use digital IDs to streamline, expand and innovate their operations and improve service delivery through digitalisation and automation, especially when envisioned as a 'digital stack' with trusted data sharing and digital payment platforms. The Framework provides for a common standard at the continental level to represent, digitally, the proofs of identity issued by trusted sources from the AU Member States and to ensure interoperability throughout the continent. The framework will be key in facilitating digital trade by enabling the use of trusted and authenticated digital identities and will enable the generation of datasets that can support the development of other services in Africa.

(V) REGIONAL MODEL LAW INITIATIVES

At the regional level, numerous African regional economic communities (RECs) have also developed instruments aimed at regulating the use and storage of data across their Member States. These include the East African Community (EAC) Legal Framework for Cyberlaws 2008; the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection; the Model Laws on Telecommunications/ICT and Cybersecurity that include provisions on data protection, cybercrime and electronic transaction of ECCAS region; and the Southern African Development Community's (SADC) Model Laws on E-Commerce/ E-Transaction, Data Protection, Cybercrime, etc.

The EAC Legal Framework for Cyberlaws 2008 was among the first initiatives in Africa to adopt a modern and effective regional harmonised framework for cyberlaws. The framework was developed to meet the needs of the region to support the regional integration process regarding e-government and e-commerce (UNCTAD, 2012). The framework comprises two sets of documents: Framework I covers electronic transactions, including electronic signatures; Cybercrime; Data protection and privacy; Consumer protection; and Framework II covers Intellectual Property; Competition; E-taxation; and Information Security. However, the transposition of these frameworks and rules will require further work to be done to ensure alignment and enforcement at the national level. Amongst the six EAC Partner States, only Rwanda has signed and ratified the AU Convention on Cyber Security and Personal Data Protection.

The ECOWAS Supplementary Act on Personal Data Protection, signed on 16 February 2010, aims to establish a harmonised legal framework for the processing of personal data across its Member States. The Act is legally binding, and the Member States are required to implement the Act within two years of its adoption. Accordingly, each Member State is obliged to establish a legal framework for the protection of personal data relating to the collection, processing, transmission, storage and use of personal data. Additionally, each Member State must also establish an independent data protection authority (DPA), which is responsible for ensuring that personal data is processed in compliance with the provisions of the Act. Administrative and financial sanctions are also provided to counter violations of the provisions of the Act by data controllers or processors (OneTrust, 2022).

Developed in 2013, the SADC Data Protection Model Law serves as a general framework for SADC states for developing their own national laws on data protection. It covers a wide r ange of different areas, including the establishment of a data protection authority, guidelines on the quality of data, general rules on the processing of personal data, duties of the data controller and data processor, rights of the data subject, recourse to the judicial authority, sanctions, and transborder flows of information (ITU, 2013). Based on international principles and being compatible with the Malabo Convention, the Model Law provides a strong foundation for protecting personal data and facilitating global flows of information to ensure consistency in data protection practices across Member States. However, given that the Model Law was developed over a decade ago, it contains numerous gaps and thus needs to be further modernised and updated (SADC, 2021).

2.2.2 COUNTRY-LEVEL REGULATORY FRAMEWORKS

Given the increasing significance of data protection, various African countries have started to develop policies and strategies to promote data development and use. Prior to 2016, only 16 African countries had laws pertaining to data protection. As of 2021, 33 countries, equivalent to 60% of the continent, had adopted such laws.[7] However, in approximately half of these jurisdictions, the laws on data protection have not yet come into force or are not fully implemented (Greenleaf & Cottier, International and regional commitments in African data privacy laws: A comparative analysis, 2022).

Generally, the legislation and regulations that have been developed throughout the continent include certain common elements, such as principles of data processing, and data subject rights. However, there are equally divergences between the laws of various countries. For instance, with regard to the scope of application, certain countries may apply data protection laws only to the private sector or public sector. There may also be divergences with regard to the definition of personal data or the treatment of cross-border flows of information and what would constitute equivalence.

According to a Continental Analysis on Africa Data Protection and Localisation Landscape conducted by AUC within the framework of the Policy and Regulation Initiative for Digital Africa (PRIDA) Project to assess countries to see the level of alignment and convergence of their national policies, regulations and legislations to 10 harmonization indicators/ principles namely:

1. Right to privacy and Legal Framework,
2. Individual Data Protection Rights,
3. Cross-border Personal Data Flows,
4. Enabling Provisions for the Digital Economy,
5. Adequate Enforcement of Data Protection Law,
6. Adequate Security Safeguards,
7. Specific Limitations to information privacy,
8. Cooperation with civil society,
9. Multilateral and Bilateral Engagement,
10. Training and Skills Development.

The comparative analysis follows once principles/indicators are identified through content analysis of data related to regional and continental frameworks, and a harmonisation index is created using harmonisation principles. The comparative analysis compares the identified principles/ indicators with the country's legal practices. This stage investigates whether the indicator/principles are implemented in the specific country. Thus, in conducting the analysis, only legal and regulatory official documents are visited/ used for comparison purposes. The analysis includes seven steps, namely: (i) Browsing and pre-qualifying the legal document, (ii) Identifying relevant sections, (iii) Searching for keywords (pre-determined keywords from the identified principles), (iv) Highlighting provisions with relevant keywords, (v) Compare the

7 These include Cape Verde (2001, amended 2013), Seychelles (2003), Burkina Faso (2004, revised 2021), Mauritius (2004, revised 2017),Tunisia (2004, under revision), Senegal (2008, under revision), Benin (2009 revised 2017), Morocco (2009, under revision), Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Ivory Coast (2013), Mali (2013), South Africa (2013), Madagascar (2014), Chad (2015), Malawi (2016), Equatorial Guinea (2016), Sao Tome e Principe (2016), Guinea (Conakry) (2016), Mauritania (2017), Niger (2017), Algeria (2018), Botswana (2018), Nigeria (2019), Uganda (2019), Kenya (2019), Republic of Congo (2019), Togo (2019), Egypt (2020), Rwanda (2021), and Zimbabwe (2002).

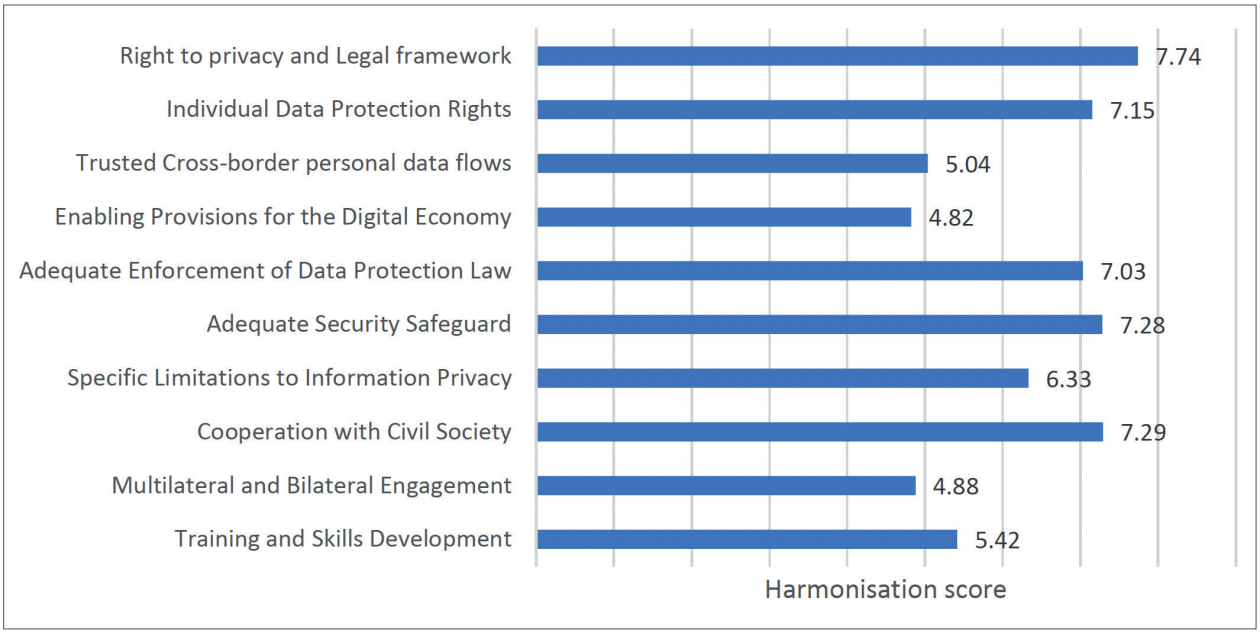
provision in the legal document with principal/ indicator, (vi) Analyse and record the extent of harmonisation with principal/ indicator as the basis of the score, (vii) Repeat for the next principal/indicator.

Scoring is used as a technique to set values in a particular variable depending on whether the country in question has harmonized or not harmonised a particular aspect of a principle where the indicator has a scale between zero (0) and ten (10), where 0 indicates a legal/regulatory vacuum, 5 shows partial, and 10 means full compliance.

While an assessment and analysis were conducted at the national level where individual country reports that reflect the extent of harmonisation of each country, demonstrate different levels in the adoption and implementation of laws and regulations on data protection and localisation, an overview of the state of data protection policy, legislations and regulations across the 33 participating countries in Africa was provided. As shown in Figure 7 below, at the aggregated level, a lot of work has been done on the right to privacy and legal frameworks, individual data protection rights, adequate security safeguards and cooperation with civil society as many countries established platforms for information sharing and sensitising people on privacy and data protection. However, even with these strong performers, there are some shortfalls impacting the harmonisation processes at the continental level. On the other hand, the indicators with weaker performances, which require a lot more interventions at both the country and continental levels, include:

a. Trusted Cross-border data flows;
b. Enabling provisions for the digital economy;
c. Specific limitations to information Privacy;
d. Multilateral and Bilateral Engagement; and
e. Training and Skills Development.

Figure 7. Harmonisation level of African national policies and regulations on Data Protection and Localisation



Source: AUC (2023)

Overall, harmonisation of the laws continues to be a challenge despite significant progress in the development of policies, laws and regulations across the continent in recent years. This is due lack of a common framework that provides a base for implementation along with a lack of data professionals with adequate skills to ensure effective data governance and value creation. While the Malabo convention is a good starting point, uptake has been slow, affecting its take-off and implementation. Of the countries that have data protection laws, very few have completely implemented the laws. In order to facilitate harmonisation that enables data flows within and across countries in support of Africa's digital trade and data-driven economy, the laws and authorities in member states must be strengthened, and continent-wide trainings and skill development programs are critical to enable countries to self-manage their data and facilitate secure and trusted cross borders data transfers.

To sum up, while the development of data protection laws in many jurisdictions is a great advancement, it is evident these are being developed unilaterally. Without a harmonised and coordinated approach, the continent will likely inherit policies and strategies that are fragmented and diverse. These will have detrimental impacts on the effective implementation of the AfCFTA. As the AfCTA's Protocol on Digital Trade is drafted, it is essential to consider the specificities of legislation in different jurisdictions and ensure that Member States are willing to transition to a common set of standards and practices in order to ensure consistency and coherence. Moreover, as evidenced in the previous section, there have been numerous developments that have been undertaken at the continental and regional levels. These would constitute important stepping stones in guiding the drafting of the data provisions in the Protocol.

Further readings

- African Union. (2020). The Digital Transformation Strategy for Africa (2020-2030).
- African Union. (2022). AU Data Policy Framework.
- WTO. (n.d.). Joint Initiative on E-commerce. From World Trade Organisation: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*
- OECD. (2013). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. From *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*
- UNCTAD (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. United Nations Conference on Trade and Development.
- UNDG (2017). United Nations Sustainable Development Goals Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection. United Nations Development Group.
- WEF (2020). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. World Economic Forum.
- Burri, M. (2021). Big Data and Global Trade Law. Cambridge: Cambridge University Press.
- Gao, H. (2022, January 18). Data sovereignty and trade agreements: Three digital kingdoms. Hinrich Foundation.

3. REFERENCE GUIDE TO INTEGRATE DATA PROVISIONS IN THE AFCFTA PROTOCOL ON DIGITAL TRADE

3.1 OBJECTIVES AND SCOPE

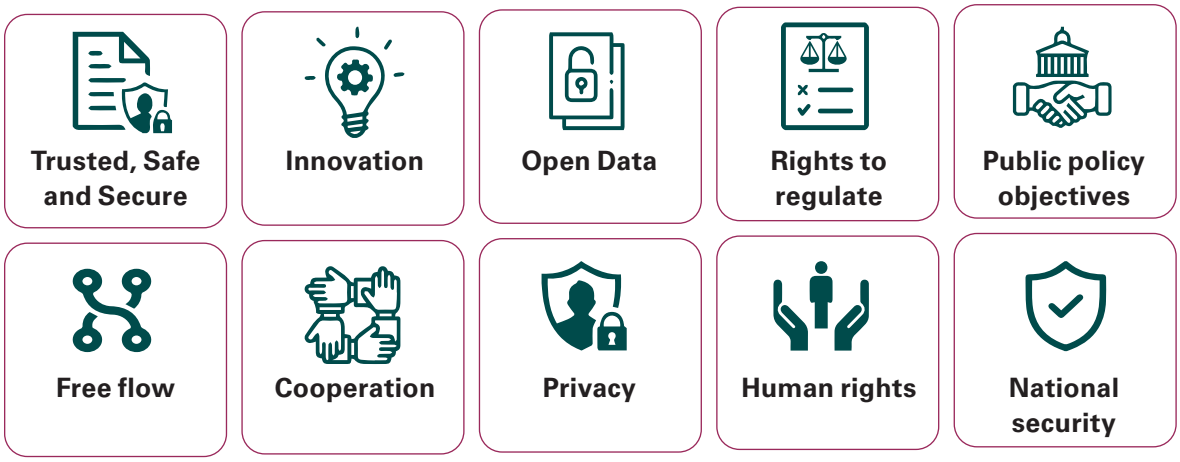
These Guidelines for Integrating Data Provisions in protocols on Digital Trade is in line with The AU Data Policy Framework, as endorsed by the African Union in February 2022, sets out the vision to guide African Union Member States in developing their national data systems (African Union, 2022). This can serve as the basis for the overarching principles guiding the governance and use of data. Specific to the role of data in digital trade and digital economy, the objective and purpose can be multi-fold: to promote innovation and economic growth; to provide a safe and secure environment to enhance trust; to preserve the policy space for the states in protecting legitimate public interests, such as national security and human rights; or to balance the benefits ad responsibilities of parties engaging in the digital economy.

It is worth emphasising that the RTA provisions, including data provisions, are binding among Member States of the agreements, and therefore, they only provide the minimum commitments of the Parties. This corresponds to the 'right to regulate' principle, whereby the RTA provisions only serve as the general minimum rules, while the states have the power to design the specificity of their respective domestic regulations for the application of such rules.

While the preambles are generally not considered as having any immediate legal significance (Schenker, 2015) as they do not specify the Parties' obligations as most substantive clauses, the statements provided in the preamble section will be used for interpretation of the provisions following Article 31 of the Vienna Convention on the Law of Treaties 1969[8]. A treaty's preamble defines, in general terms, the purposes, considerations, or motivations that led the parties to conclude a treaty (Mbengue, 2006). In other words, preambles are frequently associated with a treaty's object and purpose. Being an integral part of a treaty, the preambular text has been increasingly associated with substantial legal and interpretive weight, particularly in the recent contexts of the WTO and international investment dispute (Hulme, 2016). This provides a strong motive for negotiators to carefully consider the implications that preambles may have in crafting these opening texts of the treaties.

8 Article 31 (General rule of interpretation) of the Vienna Convention 1969 state that:
- A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.
- The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes: (a) any agreement relating to the treaty which was made between all the parties in connection with the conclusion of the treaty; (b) any instrument which was made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.[…]

Figure 8. Some key considerations for data provisions in FTAs



Based on the wording of the AU Data Policy Framework's vision, the following text would be an example for the data-related preamble statements of the AfCFTA Protocol on Digital Trade to support responsible, secure, and equitable use of data:

[The Parties to this Agreement, resolving to:][9]

- Recognise 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;
- Recognise the need for **trusted, safe and secure** data systems integrated on the basis of common standards and practices;
- Acknowledge the need for an enabling environment that stimulates innovation and entrepreneurialism to foster the development of data-value-driven economies;
- Acknowledge the need for **open data**, interoperability standards and data-sharing initiatives to harness the potential of data for driving development and ensuring better distributive benefits of the data-driven economy;
- Recognise the need to ensure the sovereignty of Member States and their ability to set legislative and regulatory priorities to **regulate** the ever-changing data landscape and to increase the productive and innovative use of data to provide solutions and create new opportunities while mitigating risks in the digital economy;
- Recognise the need for a **balancing approach** to facilitate the free flow of data across borders while achieving an equitable distribution of benefits and addressing risks related to public welfare, human rights, national security, and other legitimate public policy objectives;
- Reaffirm the importance of promoting corporate social responsibility, cultural identity and diversity, environmental protection and conservation, gender equality, indigenous rights, labour rights, inclusive trade, sustainable development and traditional knowledge, as well as the importance of preserving the right to regulate of states in the public interest matters;
- Recognise the need to facilitate cross-border data flows and increase business opportunities while ensuring an adequate level of protection of **personal data and privacy;**

9 This list of sample preambular text is not exhaustive and does not cover the more general objective statements of the digital trade chapter.

- Recognise the need for Member States to **cooperate on matters of data** governance to achieve common objectives related to the sustainable development of their economies and societies.

These statements offer the vision and goals of the Protocol on Digital Trade. Typically, they are not specifically binding or providing any commitments in terms of any restriction or facilitation of flows of data. The preamble is a statement of intent on how the parties wish to regulate and facilitate aspects of the data market and highlights the alignment of the parties against some core principles.

3.2 CONSIDERATIONS OF CORE PROVISIONS

This section provides considerations on the core provisions, including, where relevant, the need for having such provisions in the African context; the implications for regulation, competitiveness, and market access; any implementation challenges, and options for negotiations of different types (in terms of areas of issues).

This section focuses on nine provisions that are closely linked to data governance or have an impact on responsible, secure, and equitable use of data (as listed below). Rules related to the data policy framework may also be found in the competition and intellectual property protocols, but these are out of the scope of this policy guide and, therefore, are not included.

As a general approach, based on the taxonomy and the text analysis of different agreements, this section suggests a number of options for different data provisions.[10] To facilitate the navigation of the options, different levels of commitments are indicated through the combinations of verbs and modal verbs in square brackets ([…]): from merely aspirational (as indicated via the use of 'Parties recognise', 'shall strive to', 'shall endeavour to', etc.) to more strongly binding commitments (through the use of 'shall', 'shall adopt', 'shall not fail to', etc.) (Baker, 2021). Alternative terminologies are also provided in squared brackets ([…]) to indicate possible options. Option number is indicated in each of the possible mutually exclusive options for negotiators' easy reading. Some provisions, such as those on cooperation or data innovation, are generally similar across most agreements, as they do not impose hard obligations on Parties. Therefore, only one option (with potentially different choices of words) is provided for each of these types of provisions.

3.2.1. PERSONAL DATA PROTECTION/ DATA PRIVACY

The inclusion of personal data protection measures in trade agreements has been driven by concerns about either the privacy of individuals or national security (Banga, Macleod, & Mendez-Parra, 2021). While resistance to the inclusion of data protection persists for fear of derogating privacy (Greenleaf, 2018), the provisions on data issues recently endorsed in preferential trade negotiations may provide opportunities to balance the conflicting goals of data protection versus data protectionism (Burri, 2017), as well as building a harmonised approach to data protection across the board. This is even more important in the context of Africa and the negotiations of the AfCFTA Protocol on Digital trade, as only 33 African countries (or 61% of all AU Member States) have data protection and privacy legislation in force.

10 Noted that in this guide we separate the type (or sub-type) provisions based on their content/regulated issue; therefore, one article may include one or more provisions (or clauses). The provisions are not necessarily mutually exclusive, and several non-conflicting options can be selected for inclusion in the negotiating text by negotiators.

According to the TAPED database, eighty-one out of the 370 RTAs concluded during the 2000-2022 period include provisions on 'data protection' with varied levels of binding commitments (Burri, Callo-Müller, & Kugler, 2022). While RTA provisions on data protection do not go into mandating the specific rights of data subjects (like domestic laws), they often require that countries put in place a legal framework or measure to ensure the protection of personal information (see details below).

In addition to the most common provisions mandating Parties to have or maintain a domestic legal framework on data protection, many RTAs also ask that in the development of online personal data protection standards, each party shall take into account the existing international standards or guidelines of relevant international organisations – such as the APEC Privacy Framework or the OECD Guidelines on Transborder Flows of Personal Data (2013). Certain agreements even specify principles on the protection of personal data, including the principles of purpose limitation; data quality and proportionality; transparency; security; right to access, rectification and opposition; restrictions on onward transfers; and protection of sensitive data, as well as provisions on enforcement mechanisms, coherence with international commitments and cooperation between the parties in order to ensure an adequate level of protection of personal data.[11]

Many RTAs with data protection provisions also recognise Parties' different legal approaches to protecting personal information, and therefore, encourage Parties to develop mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously (such as the EU's adequacy decision), by mutual arrangement (such as the EU-US Privacy Shield, which was declared invalid by the European Court of Justice on 16 July 2020), or under broader international frameworks (such as the OECD Privacy Guidelines or the APEC Cross-Border Privacy Rules).

As countries might be at different stages of developing domestic legal frameworks for data protection, cooperation activities have also been incorporated into RTAs to improve the level of protection of privacy in electronic communications while avoiding obstacles to trade. These provisions might include sharing information and experiences on regulations, laws, and programmes on data protection; research and training activities; the establishment of joint programmes and projects; maintaining a dialogue; holding consultations on matters of data protection, etc. (Burri, 2021). It is also significant for parties to the agreement to work towards recognising the adequacy of regulations between themselves, something which is promoted in the CPTPP (Baker & Le, 202 (Baker & Le, 2022).

Based on these considerations, the following options for Personal Data Protection provisions are suggested. In the African context, the Malabo Convention signifies an important step for the harmonisation of the continent's regulatory framework on Cyber Security and Personal Data Protection. Therefore, a sample provision is added to encourage AU Member States to accelerate the ratification process.

11 Article 199-200, CARIFORUM-EC EPA

(I) OBJECTIVES

Reaffirmation of the benefits of personal data protection: The State Parties[12] recognise the economic and social benefits of protecting the personal [information/data] of participants in [the digital economy/digital trade/electronic commerce] and the importance of such protection in enhancing confidence in [the digital economy/digital trade/electronic commerce].[13]

Recognise privacy rights: The State Parties recognise that the protection of personal [information/data] and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

Emphasise the proportionality of data protection measures: The State Parties recognise the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented. [14]

(II) DOMESTIC REGULATIONS

[Option 1] Domestic regulations to promote digital trade/e-commerce: Each State Party [may/shall] adopt [*and/or*] maintain [*a legal framework/measures*] that provide[s] for the protection of the personal [*information/data*] of the users of electronic commerce and digital trade.[15]

[Option 2] Domestic regulations to ensure privacy protection: The State Parties [may/shall] adopt [*and/or*] maintain [*a legal framework/measures*] that ensure the protection of personal [information/data], including the cross-border transfer and processing of personal [information/data] and the conditions and requirements relating to it, to promote the fundamental values of respect for privacy and protection of personal [*information/data*]. [16]

(III) SPECIAL CONSIDERATIONS FOR STATE PARTIES[17] AT AN EARLY STAGE OF DEVELOPING NATIONAL DATA SYSTEMS

[Option 1] Allowing State Party to develop national framework at their own pace: [*State Party's name*] is not required to apply this Article before the date on which that Party implements its legal framework that provides for the protection of personal data of the users of electronic commerce. For greater certainty, a State Party may comply with the obligation in this Article by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.[18]

12 Most RTAs use either Parties or Members to indicate signatories. The AfCFTA uses the term "State Party" to refer to an African Union Member State that has ratified or acceded to the Agreement and for which the Agreement is in force. Therefore, this guide also use the term "State Party" (or "State Parties" in plural form) for consistency.
13 Based on Article 14.8.1, CPTPP; Article 4.2.1, DEPA.
14 Paragraph 3, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
15 Based on first sentence, Article 14.8.2, CPTPP; Article 12.8, RCEP; first sentence, Article 4.2, DEPA.
16 Paragraph 4, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
17 These sample clauses are provided under Personal Data Protection provision, but State Parties may also consider putting similar language under other provisions based on the needs and agreement among State Parties.
18 Based on Footnote 5 and Footnote 6 of the CPTPP.

[Option 2] Providing a specific transitional period upon request by State Party: [*State Party's name] is required to apply this Article no later than [citing number of transitional years*] following the date of entry into force of this Agreement for that Party. Notwithstanding [reference to specific clause], [*State Party's name*] may request an extension of [*citing number of additional transitional years*] to fully implement the commitments under [*reference to specific clause*] by providing a written request to the [*stating the specific committee*] no later than six months before the expiry of the [*citing number of original transitional years*] period provided for in this paragraph.

(IV) ADOPTION OF INTERNATIONAL GUIDELINES

[Option 1] Generic encouragement: In the development of its [*legal framework/measures*] for the protection of personal [*information/data*], each State Party shall take into account the principles and guidelines of relevant international bodies.[19]

[Option 2] Citing the specific international guidelines: In the development of its [*legal framework/measures*] for the protection of personal [*information/data*], each State Party [*should/may/shall*] take into account international standards, principles, guidelines, and criteria of relevant international organisations or bodies, such as the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013). [20]

(V) KEY PRINCIPLES

Emphasising users' consent principle: The State Parties shall ensure obtaining the directly expressed individual's consent for cross-border transfer and processing of his personal data. [21]

Listing key principles for domestic legal framework: The State Parties recognise that the principles underpinning a robust legal framework for the protection of personal information should include collection limitation; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.[22]

(VI) COMMITMENT TO RATIFYING THE MALABO CONVENTION

The State Parties will make continued and sustained efforts towards ratifying the African Union Convention on Cyber Security and Personal Data Protection 2014 (the Malabo Convention). The State Parties [*commit/shall strive*] to respecting, promoting and realising, in their laws and practices, the principles as stated in the Malabo Convention.

(VII) NON-DISCRIMINATION

Overarching non-discrimination rule regarding e-commerce users' personal data: Each State Party [shall endeavour to/shall] adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. [23]

19 Based on second sentence, Article 14.8.2, CPTPP; second sentence, Article 4.2, DEPA.
20 Based on Paragraph 5, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
21 Paragraph 8, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
22 Based on Article 19.8.3, USMCA; Article 4.2.3, DEPA.
23 Based on Article 4.4, DEPA; Article 14.8.3, CPTPP; Article 19.8.4, USMCA; Paragraph 7, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.

Non-discrimination with an emphasis on consumers and medical patients' information: Each State Party [*shall endeavour to/shall*] adopt non-discriminatory practices in protecting citizens, consumers and medical patients from personal information protection violations occurring within its jurisdiction.[24]

(VIII) PUBLICATION OF INFORMATION

Each State Party [*should/shall*] publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; (b) businesses can comply with any legal requirements. [25]

(IX) PROMOTION OF COMPATIBILITY OF REGIMES

Mechanisms to promote compatibility and/or mutual recognition: Recognising that the State Parties may take different legal approaches to protecting personal information, each State Party shall [*pursue/encourage*] the development of mechanisms to promote compatibility [*and/or*] interoperability between their different regimes for protecting personal information.[26]

These mechanisms may include: (a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; (b) broader international frameworks;[27](c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or (d) other avenues of transfer of personal information between the State Parties. [28]

Exchange of information: The State Parties [*shall endeavour to/shall*] exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. [29]

3.2.2. CROSS-BORDER DATA FLOWS

The growing importance of data in the economy has given rise to discussions around rules governing cross-border data flows. Restrictions on cross-border data transfer are shaped by the data sovereignty approach pursued by a country. Limitations on cross-border data transfer could result in lost business opportunities and reduce the ability of an organisation to trade internationally. The general approach to the transfer of data requires an adequate level of protection in the receiving country. For example, the Malabo Convention, while guaranteeing the free flow of information, requires that "The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed."[30] In this context, it is essential to establish the basic principle for data protection that provides a synchronous or similar with regulations in other jurisdictions to lay a foundation for a trusted exchange of data, including personal data.

24 Paragraph 7, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
25 Based on Article 4.5, DEPA; Article 14.8.4, CPTPP; Article 19.8.5, USMCA; Article 12.8.3, RECP; Paragraph 9 Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
26 Based on first sentence, Article 19.8.6, USMCA.
27 Based on first and second sentences of Article 14.8.5, CPTPP.
28 Based on Article 4.6, DEPA; Paragraphs 10 and 11, Section C.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
29 Based on Article 4.7, DEPA; second sentence, Article 19.8.6, USMCA.
30 Article 14.6(a), Malabo Convention.

The AU Data Policy Framework encourages Member States to leverage economies of scale of digital infrastructure offered by cloud services and other new technologies for data value creation for both the public and private sectors (African Union, 2022). This would entail the need for allowing free cross-border data flows within the continent and beyond, subject to conditions and standards to ensure data security. Furthermore, intra-continental free flows of data will be an essential element for the creation of the African common market and particularly for realising the vision of an African Digital Single Market as anticipated in the Digital Transformation Strategy for Africa (2020-2030) (African Union, 2020).

References to data flow appeared in RTAs as early as the 2000s. Under the Jordan–US FTA, the Joint Statement on Electronic Commerce highlighted the 'need to continue the free flow of information' (Burri, 2021). Since then, an increasing number of RTAs have incorporated more strongly binding provisions to facilitate cross-border data flows. However, the current legal frameworks on cross-border data flows show a high level of diversity (UNCTAD, 2023). As a result, the scope of cross-border data flow has been less robust than that of data protection, giving the need to reconcile the differentiated approaches to cross-border transfer of data, including personal data.

Generally, three types of cross-border data flow provisions can be found in the existing RTAs, including those with the most extensive scope, such as the DEPA or the UK-Singapore DEA. These include provisions citing the right to regulate, the commitments to allow cross-border transfer of information by electronic means, and the non-discrimination treatment. [31] The specific conditions for cross-border transfer, however, are left to be regulated at the domestic level. This probably corresponds to the emphasis on the right to regulate of Parties, but also requires collaborative work at the bilateral and regional levels, especially in the context of Africa, to ensure both the free flow of data and data security.

Based on the consideration of the current practices, the below provides the different options for these types of cross-border data flow provisions of the AfCFTA Protocol on Digital trade.

(I) OBJECTIVES

Balance of rights: The State Parties recognise the importance of the free flow of information on the Internet, while agreeing that this should not impair the rights of other persons, entities or businesses, including intellectual property rights.

(II) RECOGNITION OF RIGHTS TO REGULATE

Generic right to regulate: The State Parties recognise that each State Party may have its own regulatory requirements concerning the transfer of information by electronic means. [32]

Right to regulate in line with essential security interest: Nothing in this Article shall prevent a State Party from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests. [33]

31 The non-discriminatory rule also emphasis a Party's power to regulate to serve public policy objectives, and therefore, in this guide, we include this type of provision under the same 'right to regulate' cohort.

32 Based on Article 4.3.1, DEPA; Article 14.11.1, CPTPP; Article 12.15.1, RCEP; Paragraph 4, Section B.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.

33 Based on Article 12.15.3(b), RCEP; Paragraph 6, Section B.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.

Right to regulate without discrimination or inhibiting trade: Nothing in this Article shall prevent a State Party from adopting or maintaining a measure inconsistent with [requirement on allowing cross-border transfer of information by electronic means] that it considers necessary to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[34] and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective. [35]

(III) GOVERNANCE OF CROSS-BORDER DATA FLOW

[Option 1] Best endeavour: The State Parties shall endeavour to support cross-border data flows with trust through model data protection contracts and the use of emerging technologies. Both sides will also explore collaborations on the use of privacy-enhancing technologies.[36]

[Option 2] Free flow with no condition: No State Party shall [prohibit/restrict/prevent] the cross-border transfer of information [nil/including personal information] by electronic means where such activity is for the conduct of the business of a covered person.[37]

[Option 3] Free flow without localisation requirements: The State Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by: [38]

a. Requiring the use of computing facilities or network elements in the State Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the State Party;
b. Requiring the localisation of data in the State Party's territory for storage or processing;
c. Prohibiting storage or processing in the territory of other State Parties;
d. Making the cross-border transfer of data contingent upon the use of computing facilities or network elements in the State Party's territory or upon localisation requirements in the State Party's territory.

34 Based on Article 12.15.3(a), RCEP
35 Based on Article 4.3.3, DEPA; Article 19.11.2, USMCA; Article 14.11.3, CPTPP; Paragraph 6, Section B.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
36 Based on paragraph 26, Section 4, EU-Singapore Digital Partnership.
37 Based on Article 19.11.1, USMCA; Article 12.15.2, RCEP; Paragraph 5, Section B.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations. Article 4.3.2, DEPA and Article 14.11.2, CPTPP express the same notion in affirmative, instead of negative, covenant: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."
38 Paragraph 5, Section B.2.1, Draft Negotiating Text of the WTO E-Commerce Negotiations; Article 201, EU-UKTCA.

3.2.3. DATA LOCALISATION

Similar to the cross-border transfer of data, data localisation, often termed as "location of computing facilities" requirements, is often discussed in connection with data sovereignty. Data localisation involves the legislative barriers to data flows, such as through compulsory local data storage requirements (Cory, 2017). Data localisation is motivated not only by the need to protect data subjects but also to support public policy and domestic regulation purposes, especially in critical sectors such as tax, accounting, finance, or telecommunication.

Generally, data localisation rules mandate the retention of data or a copy thereof within a country's territory. Strict data localisation rules require the storage of all data locally, and not merely a copy. Data localisation rules are often intended to prevent cybercrimes (such as identity theft), promote local economies (via creating jobs), and address rising concerns about privacy (McKinsey, 2022). However, where the local data infrastructures are not secure enough, they can become susceptible to security threats, such as cyber-attacks and foreign surveillance. Furthermore, the requirements for duplicate copies of data may place undue financial obligations on companies. Some African countries face acute technological capacity constraints, and therefore, data localisation requirements could, in fact, burden the domestic capacity of the current digital infrastructure (such as the national data centres) (African Union, 2022). This is why it is essential for the AU Member States to assess the application of data localisation on a cost-benefit basis, with the incorporation of public value, to ensure facilitating technology innovation while not overburdening the domestic infrastructure capacity.

The first rule of data localisation was included in the Japan–Mongolia FTA in 2015. Since then, an increasing number of trade agreements have incorporated this rule under their e-commerce chapter. However, similar to the rules on cross-border transfer of data, the current scope of data localisation rules under RTAs has also been limited to data protection, giving the need to reconcile the differentiated approaches and the emphasis on data sovereignty of countries.

Generally, three types of provisions on data localisation can be found in the existing RTAs, including those with the most extensive scope, such as the DEPA or the UK-Singapore DEA. These include provisions citing the right to regulate, the prohibition of using data localisation requirements as a condition for conducting business in a country's territory, and the non-discrimination treatment.[39] Similar to the rule on cross-border transfer, the specific conditions for the mandatory location of computing facilities are left to be regulated at the domestic level. Financial services have a separate data transfer requirement, whereby certain restrictions on data flows may apply for the protection of privacy or confidentiality of individual records, or for prudential reasons. Therefore, options for this type of provision are also provided below.

(I) RECOGNITION OF RIGHTS TO REGULATE

Generic right to regulate: The State Parties recognise that each State Party may have its own [regulatory requirements/measures] regarding the use or location of computing facilities, including [regulatory requirements/measures] that seek to ensure the security and confidentiality of communications. [40]

39 The non-discriminatory rule also emphasis a Party's power to regulate to serve public policy objectives, and therefore, in this guide, we include this type of provision under the same 'right to regulate' cohort.

40 Based on Article 4.4.1, DEPA; Article 12.14.1, RCEP; Article 14.13.1, CPTPP; Paragraph 4, Section B.2.2, Draft Negotiating Text of the WTO E-Commerce Negotiations.

Right to regulate in line with essential security interest: Nothing in this Article shall prevent a State Party from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests. [41]

Right to regulate without discrimination or inhibiting trade: Nothing in this Article shall prevent a State Party from adopting or maintaining measures inconsistent with [*the prohibition in data localisation in a State Party's territory*] that it considers necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[42] and (b) does not impose restrictions on the use or location of computing facilities greater than are [necessary/required] to achieve the objective.[43]

(II) PROHIBITION OF DATA LOCALISATION

No State Party shall require a covered person to use or locate computing facilities in that State Party's territory as a condition for conducting business in that State Party's territory.[44]

(III) LOCATION OF FINANCIAL COMPUTING FACILITIES FOR COVERED FINANCIAL SERVICE SUPPLIER

[Option 1] Recognise the need for access to information for financial regulation and supervision: The State Parties recognise that immediate, direct, complete, and ongoing access by a State Party's financial regulatory authorities to information of covered financial service suppliers, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognise the need to eliminate any potential limitations on that access. [45]

[Option 2] No requirement of data localisation subject to conditions: No State Party shall require a covered financial service supplier to use or locate financial service computing facilities in the State Party's territory as a condition for conducting business in that territory, so long as the State Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on financial service computing facilities that the covered financial service supplier uses or locates outside the State Party's territory. [46]

3.2.4. DIGITAL IDENTITIES

Digital identity is not only closely linked to the issue of personal data, but also can have a major distributional impact. Ensuring that everyone has access to identification is one of the Sustainable Development Goal (SDG) Targets, Target 16.9—to "provide legal identity for all, including birth registration" by 2030. Furthermore, identification enabled access to financial and economic opportunities, social protection, healthcare, education, etc. (World Bank, 2023).

41 Based on Article 12.14.3(b), RCEP; Paragraph 7, Section B.2.2, Draft Negotiating Text of the WTO E-Commerce Negotiations.
42 Based on Article 12.14.3(a), RCEP
43 Based on Article 4.4.3, DEPA; Article 14.13.3, CPTPP; Paragraph 6, Section B.2.2, Draft Negotiating Text of the WTO E-Commerce Negotiations.
44 Based on Article 4.4.2, DEPA; Article 19.12, USMCA; Article 14.13.2, CPTPP; Article 12.14.2, RCEP; Paragraph 5, Section B.2.2, Draft Negotiating Text of the WTO E-Commerce Negotiations.
45 Paragraph 10, Section B.2.3, Draft Negotiating Text of the WTO E-Commerce Negotiations.
46 Paragraph 10, Section B.2.3, Draft Negotiating Text of the WTO E-Commerce Negotiations.

Digital identity systems can support the currently laggard paper-based identity system. This is even more instrumental in the context of Sub-Saharan Africa, which accounts for nearly 500 million people, or almost half of the global unregistered population (World Bank, 2023).

Building a digital identity system is a challenging task as it requires tackling both the potential risks of privacy, inclusivity, and sustainability of the traditional ID system (World Bank, 2023), as well as the cybersecurity risk of a digital system (Kanwar, Reddy, Kedia, & Manish, 2022). Therefore, the nuances of the system design and operation should be situated within the government (thus the right to regulate in the context of the regional agreement). However, to ensure the broad-based benefits of the digital identity system, mutual recognition of digital identities should be emphasised as this can enable regional economic integration and cooperation. This is even more crucial to realise the African Economic Community goals with the free movements of persons, goods, services and capital.[47] The AU Interoperability Framework on Digital ID and AU Data Policy Framework recognise that and aim to achieve a high level of interoperability and coherence of digital ID and data Systems across the continent while several African countries have been introducing digital identification systems, pervasive and interoperable digital identification systems remain a major social and economic challenge on the continent. To support mutual recognition, the Digital Identity Interoperability Framework will be key in facilitating the generation of datasets that can support the development of public and private services in Africa.

The above consideration is reflected in the existing rules regarding digital identities within RTA frameworks. Digital identity provisions generally affirm the State Party's right to regulate when it comes to the domestic implementation of digital identity systems, while promoting mechanisms to support interoperability and mutual recognition among Parties. The below options for provisions are therefore provided for digital identity provisions of the AfCFTA Protocol on Digital trade.

(I) ASPIRATION TO PROMOTE INTEROPERABILITY FOR DIGITAL IDENTITY REGIMES

Recognising that the cooperation of the State Parties on digital identities, individual or corporate, will increase regional and global connectivity, and recognising that each State Party may have different implementations of, and legal approaches to, digital identities, each State Party shall endeavour to promote the interoperability between their respective regimes for digital identities. [48]

(II) MEASURES TO PROMOTE INTEROPERABILITY FOR DIGITAL IDENTITY

The State Parties shall endeavour to facilitate initiatives to promote such compatibility and interoperability [between digital identity regimes], which may include:

a. the establishment or maintenance of appropriate frameworks to foster technical interoperability or common standards between each State Party's implementation of digital identities;
b. comparable protection of digital identities afforded by each State Party's respective legal frameworks, or the recognition of their legal and regulatory effects, whether accorded autonomously or by mutual agreement;

47 Article 4.2.1, *Abuja treaty.*
48 Based on Article 7.1, DEPA; Article 8.61-S (1), UK-Singapore DEA.

c. the establishment or maintenance of broader continental and international frameworks [on digital identity regimes];
d. identifying and implementing use cases for the mutual recognition of digital identities and
e. exchanging knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and the promotion of the use of digital identities.[49]

(III) CARVE-OUT FOR PUBLIC POLICY OBJECTIVES

For greater certainty, nothing in this Article shall prevent a State Party from adopting or maintaining measures inconsistent with [measures promoting the interoperability between regimes for digital identities] to achieve a legitimate public policy objective.[50]

3.2.5. OPEN GOVERNMENT DATA

Big data and open data are the two major developments shaping the trajectory of the data-driven economy. Big Data is most useful, and has the greatest economic and social value, when it is also Open Data (Gurin, 2014). Open government data, whether being big data or not, can contribute to building a transparent society, building trust, and allowing smarter use of data by enabling individuals, organisations and even governments themselves to innovate and collaborate in new ways (World Bank, 2019; HM Government, 2013). For example, government data can be used in the development of applications to improve access and use of local services, such as public transport (Gurin, 2014). McKinsey (2013) estimates that open data can help unlock up to US$5 trillion in economic value annually across seven sectors (education, transportation, consumer products, electricity, oil and gas, healthcare, and consumer finance).

The AU Data Policy Framework encourages the establishment of open government data initiatives by government agencies in support of creating integrated and interoperable national data systems. The AU Data Policy Framework emphasises that '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." In fact, several successful open data-based innovations have been carried out in Africa to improve performance in the areas of agriculture production, social and governance, and access to medicines.

Open data would entail substantial changes in legal, social and technical aspects (such as change in mindset, governance approach, and legal framework) (Open Data Handbook, 2023). Furthermore, it should not be presumed that open data practice will automatically take root throughout government. Resistance to change would likely happen, and in this case, advocacy and awareness raising about open data for all institutional actors will be beneficial (Schalkwyk, Willmers, & Schonwetter, 2015).

As a result, at the bilateral levels, most open government data provisions in existing RTAs are weakly binding. Already, they represent a 'truly innovative and very relevant' step in the domain of domestic regimes for data governance (Burri, 2021). Usually, open government data provisions cover recognition of the benefits conferred by public access to and use of government data, possible criteria for open government data to support access and use,

49 Based on Article 7.1, DEPA; Article 8.61-S (2), UK-Singapore DEA.
50 Based on Article 7.2, DEPA.

encouraging bilateral/regional cooperation, and areas for cooperation. Among these, the criteria for open government data can support the creation of integrated and interoperable national data systems to foster a strong data economy, as envisioned in the AU Data Policy Framework. Based on the consideration of the current practices, the below provides some options for these types of open government data provisions of the AfCFTA Protocol on Digital trade.

(I) ENCOURAGING PUBLIC ACCESS TO AND USE OF GOVERNMENT DATA

The State Parties recognise that facilitating public access to and use of government data fosters economic and social development, competitiveness, and innovation.[51] To this end, the State Parties [are encouraged to/shall strive to/shall] expand the coverage of such data, such as through engagement and consultation with interested stakeholders.[52]

(II) CRITERIA FOR OPEN GOVERNMENT DATA

To the extent that a State Party chooses to make government data digitally available for public access and use, a State Party [shall endeavour to/shall], to the extent practicable, ensure that such data:

a. is made available in a machine-readable and open format;

b. can be searched, retrieved, used, reused and redistributed;

c. is updated, as applicable, in a timely manner;

d. is accompanied by metadata that is, to the extent possible, based on commonly used formats that allow the user to understand and utilise the data;

e. is made available in a spatially enabled format with reliable, easy to use and freely available Application Programming Interfaces ("APIs")

f. is generally available at no or reasonable cost to the user.

g. can be used for commercial and non-commercial purposes, including in the process of production of a new product or service. [53]

(III) ENCOURAGE COOPERATION TO FACILITATE USE OF GOVERNMENT DATA

The State Parties [*shall endeavour to/shall*] cooperate in matters that facilitate and expand public access to and use of government data, including exchanging information and experiences on practices and policies, with a view to encouraging the development of electronic commerce and creating business opportunities, especially for small and medium-sized enterprises.[54]

51 Based on Article 19.18.1, USMCA; Article 9.5.1, DEPA; Article 8.61-H (1), UK-Singapore DEA.
52 Paragraph 2, Section B.4.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
53 Consolidated from several text of Article 8.61-H (2), UK-Singapore DEA; Paragraphs 3 & 4, Section B.4.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.
54 Based on Article 8.61-H (3), UK-Singapore DEA; Article 9.5.3, DEPA; Article 19.18.3, USMCA; Paragraph 5, Section B.4.1, Draft Negotiating Text of the WTO E-Commerce Negotiations.

(IV) AREAS OF COOPERATION

Cooperation under this Article may include activities such as:

a. jointly identifying sectors where open data sets, particularly those with global value, can be used to facilitate technology transfer, talent formation and innovation, among other things;
b. encouraging the development of new products and services based on open data sets; and
c. fostering the use and development of open data licensing models in the form of standardised public licences available online, which will allow open data to be freely accessed, used, modified and shared by anyone for any purpose permitted by the State Parties' respective laws and regulations, and which rely on open data formats.[55]

3.2.6. DATA-DRIVEN INNOVATION

Technology advancement being embedded in modern society has given rise to more and better datasets for use and analysis, which in turn support better decision-making in both public and private sectors. Furthermore, data can also be used to support further innovation, such as in machine learning, automation, and Artificial Intelligence (AI) (Borne, 2021). Besides the opportunities brought about by applying AI to large-scale data, there have been rising concerns about their socio-economic impacts. These concerns range from possible job losses, expansion of monopoly with exclusive access to technology, fundamental human rights, and political stability impacts to ethical concerns related to algorithm errors and bias (Mittelstadt, 2021; Bossmann, 2016; Smart Africa Alliance, 2021; Adams, 2022).[56] Probably due to these concerns, as well as the fact that countries are at different stages of data-driven innovation development, data-driven innovation provisions in existing regional and bilateral frameworks are mostly framed as 'best endeavour' and cooperation, without being legally binding (as discussed below). Within Africa, the AU Data Policy Framework also highlight the policy significance of economic regulation necessary to redress the uneven distribution of opportunities related to data value creation and innovation (African Union, 2022).

While the private sector, being the more agile and active sector, is expected to drive much of the progress, governments have an important role in supporting data-driven innovation for economic growth and improving quality of life. In particular, governments have an important role in collecting and disseminating data, creating the appropriate legal frameworks to foster data sharing, and raising public awareness about the importance of sharing data (Castro & Korte, 2013). The AU Data Policy Framework recommends the establishment of "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." This calls for cooperative actions among all stakeholders, governments and businesses alike, to steer the data-driven innovative economy forward.

The same notion is reflected in the structure of data-driven innovation provisions in RTAs. Generally, data-driven innovation provisions recognise the role of data and data-driven innovation in the economy and call for cooperative activities to support data innovation.

55 Article 9.5, DEPA.
56 This topic is out of scope of this guide, and will not be explored here as it has been dealt with in other pan-African initiatives, such as the African Union Artificial Intelligence (AU-AI) Continental Strategy for Africa, which is under development (AUDA-NEPAD, 2023), or the Blueprint on Artificial Intelligence for Africa, jointly developed by the Smart Africa Alliance and the South African government (Smart Africa Alliance, 2021).

It should be noted that at this stage, as in other data-related areas, given the different approaches to data governance, the commitments for data innovation are mainly at best endeavour. Based on the consideration of the current practices, the below provides some options for data innovation provisions of the AfCFTA Protocol on Digital trade.

(I) RECOGNISE THE ROLE OF DATA IN THE ECONOMY:

[Option 1] The State Parties recognise that digitalisation and the use of data promote economic growth.[57]

[Option 2] The State Parties recognise that cross-border data flows and data sharing enable data-driven innovation.

(II) RECOGNISING THE NEED FOR ENABLING ENVIRONMENT AND MECHANISMS FOR DATA INNOVATION

[Option 1] To support the cross-border transfer of information by electronic means and promote data-driven innovation, the State Parties recognise the need to create an environment that enables, supports, and is conducive to, experimentation and innovation, including through the use of regulatory sandboxes where applicable.[58]

[Option 2] The State Parties recognise that innovation may be enhanced within the context of regulatory data sandboxes where data, including personal information, is shared amongst businesses in accordance with the State Parties' respective laws and regulations.[59]

[Option 3] The State Parties recognise that data sharing mechanisms, such as trusted data sharing frameworks and open licensing agreements, facilitate data sharing and promote its use in the digital environment to: (a) promote innovation and creativity; (b) facilitate the diffusion of information, knowledge, technology, culture and the arts; and (c) foster competition and open and efficient markets. [60]

(III) COLLABORATION ON DATA INNOVATION

The State Parties shall endeavour to support data innovation through:[61]

a. Collaborating on data-sharing projects, including projects involving researchers, academics and industry, using regulatory sandboxes as required to demonstrate the benefits of the cross-border transfer of information by electronic means;[62]
b. Cooperating on the development of policies and standards for data mobility, including consumer data portability; and
c. Sharing policy approaches and industry practices related to data sharing, such as data trusts.[63]

57 Article 8.61 I(1), UK Singapore DEA.
58 Article 8.61 I (2), UK Singapore DEA.
59 Based on Article 9.4.1, DEPA.
60 Based on Article 9.4.2, DEPA.
61 Article 8.61 I (3), UK Singapore DEA.
62 Similar provision can be found in Article 9.4.3, DEPA.
63 A data trust can be defined as a steward mechanism that manages someone's data on their behalf. See (Artyushina, 2021).

3.2.7. DIGITAL INCLUSION

Digital inclusion is defined as "equitable, meaningful, and safe access to use, lead, and design of digital technologies, services, and associated opportunities for everyone, everywhere" (United Nations, 2023). It is arguably appropriate to discuss digital inclusion in the context of data-related issues, as digital inclusion presents both a challenge and an expected outcome of the data-driven economy. The UN emphasises the factors of access, affordability, and participation to contribute to digital inclusion (United Nations, 2023). These factors are inter-related as access and affordability will provide the means for individuals to raise their voices and participate.

In the context of Africa, ensuring digital inclusion is even more critical to ensure that the continent can reap the benefit of the data-driven economy. IFC and Google estimate that the Africa's internet economy has the potential to reach US$180 billion by 2025 and US$712 billion by 2050 (Google & IFC, 2020). In fact, the Digital Transformation Strategy for Africa (2020-2030) and the AU Data Policy Framework emphasise equitable inclusion as an important condition for the data economy. However, in order to realise that potential, the continent needs to overcome several challenges related to infrastructure, human resources, and regulatory framework.

Digital inclusion provisions in RTAs aim to address some of the challenges in access and participation in the digital and data-driven economy through a mainly cooperative approach. This includes, among others, sharing experiences and best practices, addressing barriers to access, and developing digital skills. Furthermore, for better monitoring and steering policies toward digital inclusion, the role of data collection in disaggregated forms is also emphasised to provide an evidential basis in the formulation of policies supporting digital inclusions.

Based on the consideration of the current practices, the below provides some options for data innovation provisions of the AfCFTA Protocol on Digital trade.

(I) RECOGNISE THE IMPORTANCE OF DIGITAL INCLUSION

The State Parties acknowledge the importance of digital inclusion to ensure that all people and businesses have what they need to participate in, contribute to, and benefit from the digital economy.[64]

The State Parties recognise the importance of expanding and facilitating opportunities in the digital economy by removing barriers to participation in the digital economy, and that this may require tailored approaches, developed in consultation with juridical persons, individuals and other groups that disproportionately face such barriers, including between Indigenous Peoples, women, rural populations and low socio-economic groups. [65]

(II) AREAS FOR COOPERATION TO SUPPORT DIGITAL INCLUSION

To this end, the State Parties shall cooperate on matters relating to digital inclusion, including the participation of women, rural populations, low socio-economic groups and Indigenous Peoples in the digital economy. Cooperation may include:

64 Based on Article 11.1.1, DEPA.
65 Consolidated based on Article 11.1.2, DEPA; Article 8.61-P (1), UK-Singapore DEA.

a. Sharing of experiences and best practices, including the exchange of experts, with respect to digital inclusion;

b. Promoting inclusive and sustainable economic growth to help ensure that the benefits of the digital economy are more widely shared;

c. Identifying and addressing barriers to accessing digital economy opportunities;

d. Developing programmes to promote the participation of all groups in the digital economy;

e. Improving digital skills and access to online business tools;

f. Promoting labour protection for workers who are engaged in or support digital trade;

g. Sharing methods and procedures for the collection of disaggregated data, the use of indicators, and the analysis of statistics related to participation in the digital economy;

h. Sharing best practices, collaborating on capacity-building initiatives, active engagement in international fora and promoting countries' participation in, and contribution to, the global development of rules on digital trade; and

i. Other areas as jointly agreed by the State Parties.[66]

(III) MECHANISM FOR COOPERATION

Cooperation activities relating to digital inclusion may be carried out through the coordination, as appropriate, of the State Parties' respective agencies, enterprises, labour unions, civil society, academic institutions and non-governmental organisations, among others. [67]

3.2.8. COOPERATION

While cooperative actions have been covered in some of the above provisions, there is an option to have a separate provision that cross-cut all areas supporting the larger digital trade development objectives, including data issues. As discussed, data governance remains a sensitive policy area, especially for personal data, and therefore, it calls for a sensible approach to reconcile the benefits of various stakeholders. Furthermore, data security and trust building are important elements in persuading businesses and individuals to participate in the digital economy. While technological solutions provide the answer to data security, trust building requires a gradual approach based on cooperation and awareness raising.

Cooperative provisions are commonly stated in the form of "*best endeavour*" commitments in all RTAs, as indicated in the use of the expression "*The Parties shall endeavour to […].*" This indicates the weak binding characteristics of this type of provisions, and the dependence on Parties to carry out the activities anticipated in the provisions. The variables among different RTAs in this type of provision are the areas for cooperation identified in the agreement, and the mechanism for cooperation. Below is the consolidation of areas of cooperation found in the most comprehensive trade agreement with digital trade chapter/provisions for consideration under the AfCFTA Protocol on Digital trade. State Parties can then add or remove areas that they deem fit for their aspiration.

66 Based on Article 11.1.3, DEPA; Article 8.61-P (2) & (4), UK-Singapore DEA.
67 Based on Article 11.1.4, DEPA; Article 8.61-P (3), UK-Singapore DEA.

(I) AREAS FOR COOPERATION

The State Parties shall endeavour to:

a. Exchange information and share experiences on regulations, policies, enforcement and compliance relating to personal information protection with a view to strengthening existing international mechanisms for cooperation in enforcing laws protecting privacy;
b. Cooperate and maintain a dialogue on the promotion and development of mechanisms that further continental interoperability of privacy regimes;
c. Promote, through international cross-border cooperation initiatives, the development of mechanisms to assist users in submitting cross-border complaints regarding personal information protection.[68]
d. Jointly identify sectors where open data sets, particularly those with global value, can be used to facilitate technology transfer, talent formation and innovation, among other things;
e. Encourage the development of new products and services based on open data sets; and
f. Foster the use and develop open data licensing models in the form of standardised public licences available online, which will allow open data to be freely accessed, used, modified and shared by anyone for any purpose permitted by the State Parties' respective laws and regulations, and which rely on open data formats.[69]

(II) MECHANISM FOR COOPERATION

The State Parties shall [consider establishing/establish] a [forum/technical working group/ sub-committee under digital trade committee/other choices for cooperative mechanism] to address any of the issues listed above or any other matter pertaining to the operation of this Chapter.[70]

3.2.9. GENERAL EXCEPTIONS

Besides creating an enabling environment for innovation and digital technology to strive, other core tasks of governments cover the promotion and protection of public health, consumer safety, public morals, public order, national security, etc. In order to protect and promote these societal values and interests, governments usually retain the power to adopt legislation or take other measures that are inconsistent with the above-mentioned commitments. These are often provided under the 'General Exceptions' clause in trade agreements, which have applicability across the whole agreement or a specific chapter.

[Option 1] Incorporating GATT and GATS General Exception: For the purposes of this Agreement, Article XX of GATT 1994 and its interpretative note and Article XIV of the General Agreement on Trade in Services in Annex 1B to the WTO Agreement shall apply to the extent applicable. To this end, the provisions above shall be incorporated into and made an integral part of this Agreement, mutatis mutandis. State Parties further agree that, in view of the challenges brought by the global nature of the internet, this Agreement shall not prevent Members from adopting or maintaining any measures for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, protecting the lawful rights and interests

68 Based on Article 19.14, USMCA (partly).
69 Based on Article 9.5.4, DEPA.
70 Based on Article 19.14, USMCA.

of its citizens, juridical persons and other organisations and achieving other legitimate public policy objectives, provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and are no more than necessary to achieve the objectives.[71]

[Option 2] Specifying the exceptions: Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade and cross-border transfer of information by electronic means, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any State Party of measures: (a) necessary to protect public morals or to maintain public order; (b) necessary to ensure the equitable or effective imposition or collection of direct taxes in respect of trade through electronic means; (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the prevention of deceptive and fraudulent practices; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; and (iii) safety.[72]

3.2.10. DISPUTE AVOIDANCE AND DISPUTE SETTLEMENT

The State Parties can choose to apply or not apply a dispute settlement mechanism (DSM) to data provisions, and the whole Protocol on Digital Trade. The enforceability of data provisions will differ depending on the way the data provisions are structured in combination with the applicability of the DSM. Figure 9 below illustrate the different level of enforceability on RTA provisions in increasing order. For example, a provision with aspirational language (e.g., State Parties 'should', 'shall strive to', 'shall endeavour to', etc.) will be less binding on State Parties than a provision with more strongly committed language (e.g., State Parties 'shall', 'shall commit to', 'shall not fail to', etc.). A provision subject to DSM is more strongly enforceable than a provision which is not [subject to DSM]. This requires reading the provisions in context and in connection with other provisions/chapters of the agreement.

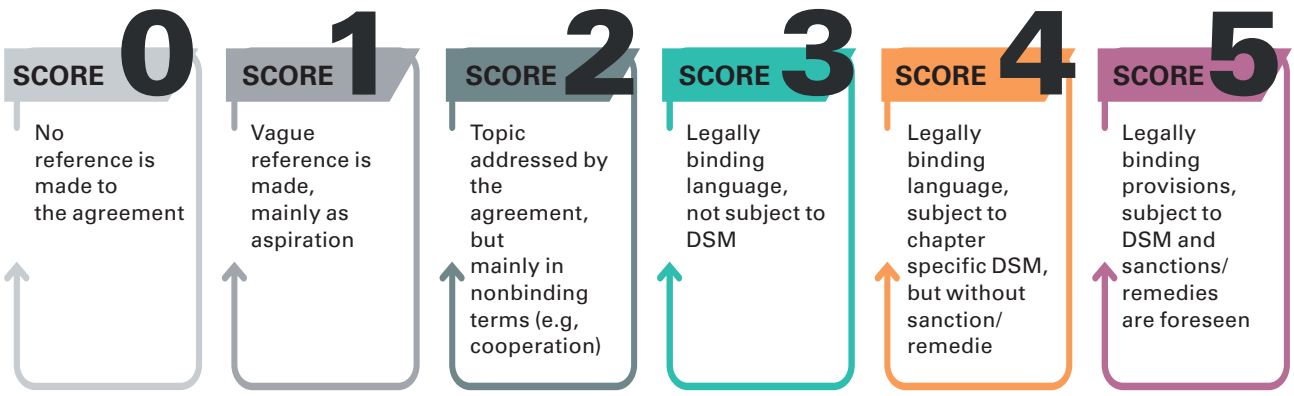
Current RTAs have different approaches to DSM with regard to data provisions. The RCEP, for example, currently excludes all matters arising under its E-Commerce Chapter from dispute settlement. The CPTPP, on the other hand, provides a transitional period for specific members to allow them 'breathing' time to adjust domestic regulations. The DEPA provides a full framework for dispute avoidance and dispute resolution under the Digital Trade chapter, including all procedural steps for conducting mediation and arbitration. This DSM, however, explicitly exclude its application to some of the 'sensitive' provisions, including the cross-border transfer of information by electronic means and the location of computing facilities.

Where DSM is applied, DSM provisions often allow the application of a multi-tier dispute resolution mechanism, whereby Parties go step-by-step through a layered process of dispute resolution. The process usually starts with bilateral consultations, followed by other alternative dispute resolution (ADR) methods, and ends with arbitration/panel with either a binding ruling or non-binding report on findings. Below are the different options for applying DSM to data provisions, as well as for Protocol on Digital Trade. Where DSM is selected to apply (Option 3 of provision type (i)), other types of provisions (from provision (ii) onward) can be referred

71 Based on Article 6, Annex 1: Scope and general provisions, Draft Negotiating Text of the WTO E-Commerce Negotiations.
72 Based on Article 6, Annex 1: Scope and general provisions, Draft Negotiating Text of the WTO E-Commerce Negotiations.

to for consideration. A provision on the objective of the DSM is also provided to emphasise that mutually agreed solutions are the best possible outcome that should guide the action of all State Parties in case any matter of disagreement arises during the implementation of the Agreement.

Figure 9. Example of the levels of enforceability of provisions



Source: Based on (Baker, 2022; Baker, 2021)

(I) APPLICABILITY OF DISPUTE SETTLEMENT MECHANISM:

[Option 1] Excluded from DSM: No State Party shall have recourse to dispute settlement under Chapter [*indicate chapter no.*] (Dispute Settlement) for any matter arising under this Chapter.[73]

[Option 2] Build-in review mechanism for inclusion of data provisions under DSM: As part of any general review of this Agreement, the State Parties shall review the application of the Dispute Settlement Chapter to this Chapter <*identify chapter number*> [*Digital Trade, including data provision*]. Following the completion of the review, the Dispute Settlement Chapter shall apply to this Chapter between those Parties that have agreed to its application. [74]

[Option 3] Application of specific DSM for Digital Trade Chapter (including for data provisions)/ general DSM: Except for <*specify provisions to be excluded from dispute settlement, if any*>, the Dispute Settlement Mechanism provided in <*specify the Annex/ Chapter on Dispute Settlement*> shall apply:

a. With respect to the avoidance or settlement of disputes between the State Parties regarding the interpretation or application of this Agreement; or

b. When a State Party considers that an actual or proposed measure of another State Party is or would be inconsistent with an obligation of this Agreement, or that another State Party has otherwise failed to carry out an obligation under this Agreement.[75]

73 Based (partly) on Article 12.17.3, RCEP.
74 Based (partly) on Article 12.17.3, RCEP.
75 Adapted from Article 14.3, DEPA.

(II) OBJECTIVES

The State Parties shall at all times endeavour to agree on the interpretation and application of this Agreement and shall make every attempt through cooperation and consultations to arrive at a mutually satisfactory resolution of any matter that might affect its operation.

The objective of this [*Dispute Avoidance and Dispute Settlement chapter/provision*] is to provide an effective, efficient and transparent process for consultations and settlement of disputes among the State Parties concerning their rights and obligations under this Agreement.

(III) TRANSITIONAL PERIOD FOR CERTAIN STATE PARTIES

<*Specify State Party/State Parties*> shall not be subject to dispute settlement under Chapter <*specify chapter number*> (*Dispute Settlement*) regarding its obligations under Article <specify article number> for a period of <*specify number of transitional years*> years after the date of entry into force of this Agreement for <*specify State Party/State Parties*>.[76]

(IV) CONSULTATION

In the event of any differences between State Parties regarding the interpretation and application of this Chapter, the State Parties concerned shall first engage in consultations in good faith and make every effort to reach a mutually satisfactory solution. A State Party (*requesting State Party*) may, at any time, request consultations with another State Party (responding State Party) regarding any matter arising under this Chapter by delivering a written request to the responding State Party's contact point. In the event that the consultations fail to resolve the differences, any State Party engaged in the consultations may refer the matter to the [Institutional setting of the Agreement].[77]

(V) GOOD OFFICE AND CONCILIATION

The State Parties may at any time agree to voluntarily undertake any alternative methods of dispute resolution, such as good offices or conciliation. Proceedings that involve good offices or conciliation shall be confidential and without prejudice to the rights of the Parties in any other proceedings. The State Parties participating in proceedings under this [*Good Office and Conciliation*] article may suspend or terminate those proceedings at any time. If the disputing State Parties agree, good offices or conciliation may continue while the dispute proceeds for resolution before an arbitral tribunal established under Article <*identify article number*> (Arbitral Tribunals).[78]

(VI) ARBITRATION/PANEL

If the consulting State Parties have failed to resolve the matter no later than <*indicating number of days*> days after the date of receipt of a request for consultation, the requesting State Party may request the establishment of a [arbitration tribunal/panel] under Article <*indicating article number*> (Establishment of [*an arbitration tribunal/a Panel*]) and, as provided in Chapter <indicating chapter number> (Dispute Settlement).

76 Based on Article 14.18, CPTPP.
77 Based (partly) on Article 12.17.2, RCEP.
78 Based on Article 14.4, DEPA.

(VII) CHOICE OF FORUM

If a dispute regarding any matter arises under this Agreement and under another international trade agreement to which the disputing State Parties are party, including the WTO Agreement, the complaining State Party may select the forum in which to settle the dispute. Once a complaining State Party has requested the establishment of, or referred a matter to, a panel or other tribunal under an agreement [*as mentioned above*], the forum selected shall be used to the exclusion of other fora.[79]

Further readings

- Draft Negotiating Text of the WTO E-Commerce Negotiations. INF/ECOM/62/Rev.2. 8 September 2021.
- Digital Economy Partnership Agreement (DEPA) between New Zealand, Chile and Singapore.
- Digital Economy Agreement (DEA) between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore.
- Chapter 14 (Electronic Commerce), Comprehensive and Progressive Agreement for Trans-Pacific Partnership.
- Chapter 19 (Digital Trade), Agreement between the United States of America, the United Mexican States, and Canada (USMCA).
- Title III (Digital Trade), Trade and Cooperation Agreement (TCA) between the European Union and the European Atomic Energy Community and the United Kingdom of Great Britain and Northern Ireland.
- Section F (Electronic Commerce), Chapter 8 (Services, Establishment, and Electronic Commerce), European Union-Singapore FTA.
- Chapter 12 (Electronic Commerce), Regional Comprehensive Economic Partnership.
- Burri, M. (Ed.). (2021). Big Data and Global Trade Law. Cambridge: Cambridge University Press. doi:10.1017/9781108919234

79 Based on Article 14.7, DEPA.

3.3 GUIDELINES FOR NEGOTIATORS ON CONSIDERING DATA PROVISION IN AFCFTA PROTOCOLS ON DIGITAL TRADE

3.3.1. GENERAL INSTITUTIONAL FRAMEWORK

GENERAL APPROACH

Countries have different models of institutional frameworks to mandate the responsibility of the lead ministry in charge of trade negotiation and other line ministries. For example, while some countries assign the Ministry of Foreign Affairs to be the lead ministry, taking advantage of its worldwide network and diplomacy skills, others assign the Ministry of Trade to take advantage of its specialised knowledge of trade (Baker P. R., Le, Vanzetti, & Ngov, 2022). Specific to data provisions (including data protection, data flow, open government data, etc.), the ministries of information and communication technology (ICT) should lead in technical aspects. Data Protection Agencies, where established, should also be closely engaged during the process. For digital identities, the relevant national identification authority should be involved. For legal text scrubbing, the Ministry of Justice or Department of Legal Affairs in the relevant ministries in charge should be consulted. In short, any institutional framework for trade policy must fit into the overall domestic economic agenda and the delegated authority in the country.

In any trade negotiation, internal coordination and consultation among related government agencies and the private sector are critical for its success. Consultations should be carried out on a regular basis. They should be conducted before the start of the negotiation to gather necessary information such as the potential benefits, concerns by private sectors, challenges in implementation, etc. It can also be used to decide whether a certain agreement is worth pursuing and to set red-lines (which will help to form the Zone of Possible Agreement (ZOPA) and Best Alternative to a Negotiated Agreement (BATNA) for negotiating team). After the negotiations have been concluded, proper internal consultations can help related parties effectively implement those policies and reap the benefits to their full potential.

THE IMPORTANCE OF INTER-MINISTERIAL COORDINATION AND CONSULTATIONS

The objective of consultations among government agencies is to make sure that they are well-coordinated in their respective mandate and that they serve the "broader" development objective of the country. Without this proper internal consultation, negotiators might not have sufficient information they need to negotiate with their foreign counterparts and risk deviating from the core interest of the country. In addition, it might also affect the ability to earn political support at home (UNCTAD, 2018).

Consultation should be done regularly before the start of the negotiations to search for important facts that affect certain areas of the agreement in order to achieve the overall negotiating objectives. This can also be used to respond to the negotiating partner's proposal and adjust one's negotiating position without losing much of the advantages.

THE IMPORTANCE OF CONSULTATION WITH THE PRIVATE SECTOR

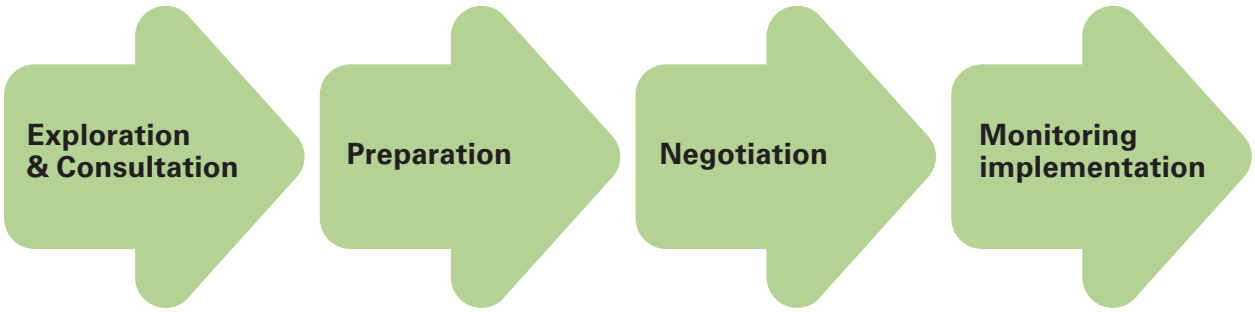
Civil society and consumer protection groups should be involved in shaping the national position, while private sector operators, with a better knowledge of the market and technology underpinning data markets, need to be consulted and engaged in this process, as ultimately, it is the operators and regulators who will be the primary 'users' of the data provisions contained in trade agreements. The private sector, including the individual consumers – especially in the case of data protection, are the ultimate beneficiaries of trade agreements. Therefore, they should be engaged as much as possible from the beginning of any trade negotiation. The private sector and representatives of consumer associations are the primary sources of information on the ground. They can provide negotiators with information on the benefits and challenges in the utilisation of trade agreements, among other matters. Timely and regular consultation with the private sector can also provide them ample time to equip themselves in order to get ready for the potential agreement to be concluded by the government. Conversely, it would be meaningless if an agreed issue cannot be effectively implemented by the private sector at home.

3.3.2. ANALYTICAL FRAMEWORK FOR NEGOTIATING DATA PROVISIONS

This section provides a suggested approach for the analytical framework in preparation for trade negotiation, with suggestions on the tools that can be used for each step of the process (Table 2). However, it should be noted that these should be seen as primary analytical steps, while more sophisticated analysis (like conducting a full-scale Sustainable Impact Assessment and domestic stakeholder consultation) should be done to ensure more holistic insights into the potential impact of a negotiated agreement (Baker & Le, 2022) (European Commission, 2016). Results coming from these tools should be read and interpreted in combination with the observations and practical experience, the potential influence of political-economic forces, and the country's visions in building the strategic partnership with the counterparts under consideration.

As discussed above, different government agencies can be involved in this process. It would be beneficial if all agencies could agree at an early stage on the communication and coordination mechanism. For example, the Ministry of Trade can be in charge of negotiating the whole digital trade chapter, while the technical team will comprise delegates from the Ministry of ICT and DPA to ensure technical inputs.

Table 2. Analytical framework in preparation for negotiation of data provisions



Stage	Analytical work	Purpose	Analytical tool
Stage 1 Exploration & Consultation	Taking stock of the current data regulatory frameworks	• Taking stock of domestic data regulatory frameworks and/or any possible development/changes in the near future (at the policy level) • Identify priorities and areas of concern of domestic businesses and individuals for trading/transferring data across borders • Parties' general regulatory profile on data governance: whether laws/regulations on data governance exist, general approach • The current commitments offered by other parties in the negotiated areas in existing RTAs (if any)	UNCTAD Cyber Law Trackers Legal text analysis Consultations
Stage 2 Preparation	Proposals of Legal Text for data provisions	Prepare options for the legal text of data provisions depending on the analysis in the exploration step	Data policy brief Legal text analysis
Stage 3 Negotiation	Revision of the documents prepared in Stage 2	Revise to reflect changes and new information obtained during negotiations.	Legal text analysis
Stage 4 Monitoring implementation	Assess compliance and monitoring	• Assess compliance with domestic regulations vis-à-vis the negotiated provisions • Identify any areas for changes in domestic regulations • Implement changes • Assess any challenges to implementation that need addressing	Reports by stakeholders Consultations Monitoring framework

4. CONCLUSIONS

The growth in the global economy is increasingly driven by data-driven sectors of the economy. In this trend, data has become a key asset that has been commodified and monetised to create a new stream of revenues for big companies (WEF, 2011; Sadowski, 2016). Data is now at the core of many frontier technologies that are propelling the digital economy. It does not only serve as an input for the production of goods and services, but it also possesses unique characteristics that allow firms to generate new streams of revenues and contribute to their competitiveness (Hagiu & Wright, 2020). However, it should be highlighted, that there is unevenness in the access and growth of data markets, which can be addressed through trade negotiations and effective data governance (African Union, 2022)

While the value of data is indisputable, there are critical divergences in regulatory approaches. As data becomes an increasingly important input to the provision of goods and services, using imperfect analogies of longstanding production inputs could provide some suggestions for how to regulate it. However, even among scholars, there have been different views on how to treat data, whether as labour, capital, individual properties, or even infrastructure (Aaronson, 2021). These different views, combined with different regulatory incentives, have spurred divergence in data governance approaches. The three largest digital markets – the United States, the EU and China – have different approaches to data governance. The United States focuses on control of the data by the private sector, China emphasises control of data by the Government, meanwhile the European Union favours control of data by individuals on the basis of fundamental rights and values (UNCTAD, 2021). Under any views, there is no denial in the roles the government plays in providing a just regulatory framework to promote responsible, secure and equitable use of data. These considerations are relevant in the context of Africa, where weaknesses in institutional frameworks, human development, and digital readiness are preventing countries from making advantage from the huge amount of data being generated by their institutions, private sector and citizens. The potential size of the market and the benefits arising from harmonisation efforts, has been recognised in the AU Data Policy Framework where key policy interventions to foster data flow across borders are identified and in the process of being implemented .

New uses for data require new ways of thinking about data. The unique characteristics of data suggest that they need to be treated differently from conventional goods and services, including in their international transfers. In the new context of the data-driven digital economy, UNCTAD (2021) suggests that rather than trying to determine who “owns” the data, policy efforts should focus on the right to access, control and use of data (UNCTAD, 2021). In addition to the data used in the private sector, creating value from public data is also important to enhance public interests through enhancing secure and equitable service delivery.

To better develop the rules regulating data, policymakers should acknowledge and agree on the special characteristics of data. Currently, there is no single agreed definition or taxonomy of data. Depending on differently chosen criteria, data can be categorised as personal or non-personal data; sensitive or non-sensitive data; private or public data; etc. (UNCTAD, 2021). In their purest form, i.e., many types of data have the characteristics of public goods (World Bank, 2021), which would then require government’s interventions to ensure the effective elimination of externalities.

Among these, personal data arguably has become an important asset that requires special attention (Ciuriak, 2018; WEF, 2011). As the use of personal data is closely associated with the privacy and safety of individuals, citizens should have the opportunity to provide their input in the rule-making process to ensure the transparency, participation, and accountability of the rules. This will contribute to the 'trust' element underpinning the growth of the digital economy and focus first on creating an effective enabling environment, then building trust in that new economy by empowering people around the world to control their data.

There are two desirable characteristics of data governance rules: to enable data access and engender trust. An enabling environment for data usage and flow would undoubtedly support innovation and create more value for the society than the sum of every single data point. However, the critical element of trust would be impaired where there is no mechanism for detecting and preventing misuse, identity theft, or other violations. Therefore, it is important to keep in mind that data helps to drive innovation, but there should be some limits to ensure the privacy of citizens and the state's security interests. A balance in approach is the most desirable but also challenging to reach. This would require consideration of all conditions and interests in the domestic environment. In this context, the AU Data Policy Framework highlights the importance of creating legitimate and trustworthy data systems via a wide range of measures, including not only cybersecurity and data protection but also promoting data justice and data ethics.

While it would be challenging to adopt one single rule book to all, AU Member States should strive to reach shared norms and rules based on the recommendations of the AU Data policy Framework and provisions of the Malabo Convention when it comes to personal data protection. This will help to create a digital environment which is less fragmented, where "more people would have greater access to information, and individuals could create and share more information" (Aaronson, 2016). This is where digital trade rules, and specifically data provisions, come into play. As discussed earlier in this guide, while data provisions in RTAs do not elaborate on the detail level that is provided in domestic data regulations, they set the minimum standards while allowing State Parties the discretion to determine the appropriate method of implementing the provisions of the Agreement within their own legal system and practice. Further, special considerations such as transitional periods and capacity building should be provided for the less digitally advanced State Parties to allow them sufficient policy space to develop data regulation in accordance with the commitments while still meeting their domestic needs.

As countries are at different stages of developing data governance frameworks, there will be a need for collaborative actions. Developing countries might benefit from engaging early on in regional and plurilateral discussions on data flows to ensure their voices are heard, and interests are well taken into consideration. The early, proactive participation will give developing economies greater leverage in the rule-making process, instead of the ordinary rule-taking position. This approach could accommodate national differences regarding ethics of data usage, disinformation, and other regulatory issues to ensure that data and the data-driven economy will be achieved together with just and equitable growth.

This reference guide on how to consider and integrate data provisions in the negotiation of digital trade protocols within the AfCFTA has been prepared with these characteristics of data, best practices from global experiences, and the previously mentioned core principles in line with the AU Data Policy Framework and Africa Digital Transformation Strategy. The guideline serves to help negotiating teams consider core data-related provisions contained in free trade agreements, and also consider the wider economic and societal implications of taking commitments in nine core areas to advance intra-Africa digital trade and regional integration in line with Agenda 2023 objectives, as well as the binding language in such provisions. As the nature of data governance is evolving and dynamic, the information in the reference guide should be considered in parallel with evolving new developments in data markets and data regulations.

REFERENCES

Aaronson, S. A. (2016). *The Digital Trade Imbalance and Its Implications for Internet Governance.* The Digital Trade Imbalance and Its Implications for Internet Governance. Retrieved from *https://www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance/*

Aaronson, S. A. (2021). Data Is Different, So Policymakers Should Pay Close Attention to Its Governance. In M. Buri, *Big Data and Global Trade Law* (pp. 340-360). Cambridge University Press.

Adams, R. (2022, May 30). *AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent*. Retrieved from Africa Policy Research Institute: *https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent*

African Union. (2020). *The Digital Transformation Strategy for Africa (2020-2030).*

African Union. (2022). *AU Data Policy Framework.*

African Union. (2022). *Decision on the Reports of the Sub-Committees of the Permanent Representatives' Committee (PRC). 40th Ordinary Session of the Executive Council (02-03 February 2022).* Retrieved from *https://au.int/sites/default/files/decisions/41584-EX_CL_Dec_1143-1167_XL_E.pdf*

African Union. (2023). *List of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection.*

African Union Commission. (2018). *African Forum on Cybercrime: African Union Convention on Cybersecurity and Personal Data Protection.*

African Union. (forthcoming). *Draft Continental Harmonisation Strategy on Policy and Regulatory Environment for Africa's Digital Single Market.*

APEC. (2005). *APEC Privacy Framework.* APEC Secretariat. Retrieved from *https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf*

APEC. (2019). *What is the Cross-Border Privacy Rules System?* Asia-Pacific Economic Cooperation. Retrieved from *https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015*

Arasasingham, A., & Goodman, M. P. (2023, April 13). Operationalizing Data Free Flow with Trust (DFFT). *CSIS*.

Artyushina, A. (2021, June 10). *The future of data trusts and the global race to dominate AI*. Retrieved from Bennett Institute for Public Policy of Cambridge: *https://www.bennettinstitute.cam.ac.uk/blog/data-trusts1/*

AUDA-NEPAD. (2023, March 29). *Artificial Intelligence is at the core of discussions in Rwanda as the AU High-Level Panel on Emerging Technologies convenes experts to draft the AU-AI Continental Strategy*. Retrieved from African Union Development Agency (AUDA-NEPAD): *https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging*

Ayalew, Y. E. (2023, June 15). *The African Union's Malabo Convention on Cyber Security and Personal Data Protection entered into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* Retrieved from European Journal of International Law Blog: *https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/*

Babalola, O. (2022). *Data Protection Legal Regime and Data Governance in Africa: An Overview.* AERC Africa.

Baker McKenzie. (2023, January 28). *Data Protection Day - Key developments and trends for 2023*. Retrieved from Lexology: *https://www.lexology.com/library/detail.aspx?g=e4ead5f0-ccd4-4762-8e06-7dd84c8341ff*

Baker, P. (2022). Trade and Sustainable Development in EU Economic Partnership Agreement. *Cross-Regional Exchange on Trade and Sustainable Development in EU Economic Partnership Agreement.*

Baker, P. R. (2021). *Handbook on Negotiating Sustainable Development Provisions in Preferential Trade Agreements.* Retrieved from UNESCAP: *https://repository.unescap.org/bitstream/handle/20.500.12870/4285/ESCAP-2021-MN-Handbook-negotiating-sustainable-development.pdf?sequence=1&isAllowed=y*

Baker, P. R., Le, L., Vanzetti, D., & Ngov, P. (2022). *Handbook on Trade Analysis.* Sept: GIZ.

Baker, P., & Le, L. (2022). *Digital Trade under CPTPP and its implications for the UK.* Retrieved from UK Parliament: *https://committees.parliament.uk/writtenevidence/110995/pdf/*

Baker, P., & Le, L. (2022). *Guidebook on Trade Impact Assessments.* Retrieved from www.unctad.org: *https://unctad.org/system/files/official-document/ditctncd2021d4_en.pdf*

Banga, K., Macleod, J., & Mendez-Parra, M. (2021). *Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?* Retrieved from *https://set.odi.org/wp-content/uploads/2021/04/Digital-trade-provisions-in-the-AfCFTA.pdf*

Berka, W. (2017). CETA, TTIP, TiSA, and Data Protection. In S. Griller, W. Obwexer, & E. Vranes, *Mega-Regional Trade Agreements: CETA, TTIP, and TiSA: New Orientations for EU External Economic Relations.* Oxford. Retrieved from *https://academic.oup.com/book/26602/chapter/195266134*

Borne, K. (2021, July 6). *Top 10 Data Innovation Trends During 2020*. Retrieved from Rocket-Powered Data Science: *http://rocketdatascience.org/?p=1589*

Bossmann, J. (2016, October 21). *Top 9 ethical issues in artificial intelligence*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/?*

Bracy, J. (2023, March 8). UK introduces draft data protection reform. *International Association of Privacy Professionals*.

Bryant, J. (2021, May 25). Three years in, GDPR highlights privacy in global landscape. *International Association of Privacy Professionals*.

Bukht, R., & Heeks, R. (2017). *Defining, Conceptualising and Measuring the Digital Economy.* Development Informatics Working Paper no. 68. Retrieved from *https://ssrn.com/abstract=3431732 or http://dx.doi.org/10.2139/ssrn.3431732*

Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law, Vol. 48, No. 1, 2017*. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3028137*

Burri, M. (2021). *Big Data and Global Trade Law.* Cambridge: Cambridge University Press.

Burri, M., Callo-Müller, M. V., & Kugler, K. (2022). *TAPED: Trade Agreement Provisions on Electronic Commerce and Data*. Retrieved from *https://unilu.ch/taped*

Castro, D., & Korte, T. (2013, November 3). *Data Innovation 101*. Retrieved from Center for Data Innovation: *https://datainnovation.org/2013/11/data-innovation-101/*

Chenaoui, H. (2018, September 11). Moroccan data protection law: Moving to align with EU data protection? *International Association of Privacy Professionals*.

CIGI. (2018). *Data Governance in the Digital Age.* Centre for International Governance Innovation. Retrieved from *https://www.cigionline.org/static/documents/documents/Data%20Series%20Special%20Reportweb.pdf*

Ciuriak, D. (2018). *The Economics of Data: Implications for the Data-Driven Economy.* Centre for International Governance Innovation.

CloudSufi. (2021, November 16). *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*. Retrieved from CloudSufi: *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*

Cory, N. (2017, May 1). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Retrieved from Information Technology & Innovation Foundation: *https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/*

Cory, N., & Dascoli, L. (2021, July 19). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology and Information Foundation*.

Crocetti, P., Peterson, S., & Hefner, K. (n.d.). *What is data protection and why is it important?* Retrieved from *https://www.techtarget.com/searchdatabackup/definition/data-protection*

Daigle, B. (2021). Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. *Journal of International Commerce and Economics*.

data.gov.uk. (n.d.). *data.gov.uk*. Retrieved from *https://www.data.gov.uk/*

de la Cruz, R., & Hau, S. (2022, March). *UK: Requirements for international data transfers under UK and EU data protection regimes.* Retrieved from Data Guidance: *https://www.dataguidance.com/opinion/uk-requirements-international-data-transfers-under*

DLA Piper. (2023). Retrieved from *https://www.dlapiperdataprotection.com/*

DLA Piper. (2023, January 29). *Data Protection Laws around the World - United States*. Retrieved from *https://www.dlapiperdataprotection.com/index.html?t=law&c=US*

Dür, A., Baccini, L., & Elsig, M. (2022). *The Design of International Trade Agreements: Introducing a New Database*. Retrieved from *https://www.designoftradeagreements.org/*

European Commission. (2016, April). *Handbook for Trade Sustainability Impact Assessment.* Retrieved from trade.ec.europa.eu: *https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154464.PDF*

European Commission. (2023, March 24). *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*. Retrieved from European Commission: *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*

European Commission. (n.d.). *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.* Retrieved from European Commission: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

European Commission. (n.d.). *Shaping Europe's digital future: Free flow of non-personal data*. Retrieved from *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in%20Europe*.

European Parliament. (2016, January 25). *Report 25 January 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)' (2015/2233(INI), [A8-0009/2016])*. Retrieved from *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0009+0+DOC+XML+V0//EN*

Gao, H. (2022, January 18). Data sovereignty and trade agreements: Three digital kingdoms. *Hinrich Foundation*.

Gawen, E., Hirschfeld, A., Kenny, A., Stewart, J., & Middleton, E. (2021). *Open source in government: creating the conditions for success.* London: Public Digital. Retrieved from *https://assets.public.digital/Open_Source_Report.pdf*

GDPR.EU. (n.d.). *hat is GDPR, the EU's new data protection law?* Retrieved from GDPR.EU: *https://gdpr.eu/what-is-gdpr/*

Giddings, A., Islam, E., Kao, K., & Kopp, E. (2021). *Towards a Global Approach to Data in the Digital Age.* IMF. Retrieved from *https://www.elibrary.imf.org/view/journals/006/2021/005/article-A001-en.xml*

Githaiga, J., & Kurji, J. A. (2023, February 6). *Kenya: Data Privacy Comparative Guide*. Retrieved from Mondaq: *https://www.mondaq.com/privacy/1190020/data-privacy-comparative-guide*

González, J. L., Casalini, F., & Porras, J. (2022). *A Preliminary Mapping of Data Localisation Measures.* OECD Publishing.

Google & IFC. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future.* Retrieved from *https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy*

GovTech Singapore. (2018, October 03). *ABCD: not as easy as you might think*. Retrieved from GovTech Singapore: *https://www.tech.gov.sg/media/technews/stack-18-abcd-ot-as-easy-as-you-might-think*

Greenberg, B. A. (2016). Rethinking Technology Neutrality. *Minnesota Law Review. 207*. Retrieved from *https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1206&context=mlr*

Greenleaf, G. (2018). Looming Free Trade Agreements Pose Threats to Privacy. 152 Privacy Laws & Business International Report. *152 Privacy Laws & Business International Report*, 23-27. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199889*

Greenleaf, G., & Cottier, B. (2022). International and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review, 44*.

GSMA. (2022). *The State of Mobile Internet Connectivity Report 2022.* Retrieved from *https://www.gsma.com/r/somic/*

GSMA. (2023). *The Mobile Economy 2023.* Retrieved from *https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf*

Gurin, J. (2014). Big Data and Open Data: How open will the future be? *Journal of Law and Policy for the Information Society Vol 10:3*, 691-704. Retrieved from *https://core.ac.uk/download/pdf/159607722.pdf*

Gurin, J. (2014, April 15). *Big data and open data: what's what and why does it matter?* Retrieved from The Guardian: *https://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government*

Hagiu, A., & Wright, J. (2020, February). *When Data Creates Competitive Advantage and When It Doesn't*. Retrieved from Harvard Business Review: *https://hbr.org/2020/01/when-data-creates-competitive-advantage*

Harvard Business Review. (2021). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*.

Hinrich Foundation. (2019, February 21). Data localisation and other barriers to digital trade.

HM Government. (2013). *Open Data White Paper. Unleashing the Potential.* Retrieved from *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf*

Huawei & Oxford Economics. (2017). *Digital Spillover. Measuring the true impact of the digital economy.* Retrieved from *https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf*

Hulme, M. H. (2016). Preamble in Treaty Interpretation. *University of Pennsylvania Law Review Vol 164*, 1281-1343. Retrieved from *https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9527&context=penn_law_review&httpsredir=1&referer=*

IBM. (n.d.). *What is artificial intelligence?* Retrieved from IBM: *https://www.ibm.com/topics/artificial-intelligence*

IBM. (n.d.). *What is machine learning?* Retrieved from IBM: *https://www.ibm.com/topics/machine-learning*

ICC. (2022). *ICC White Paper on Delivering Universal Meaningful Connectivity.* Retrieved from *https://iccwbo.org/wp-content/uploads/sites/3/2022/05/2022-icc-white-paper-delivering-connectivity.pdf*

IIF. (2020). *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy.* Institute of International Finance. Retrieved from *https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf*

ITU. (2013). *HIPSSA –Data Protection: SADC Model Law.*

ITU. (2021). *Measuring digital development Facts and Figures 2021.* Retrieved from *https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf*

ITU. (2022). *Measuring digital development: Facts and Figures 2022.* International Telecommunication Union. Retrieved from *https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2022-pdf-e.pdf*

Kanwar, S., Reddy, A., Kedia, M., & Manish, M. (2022). *The Emerging Era of Digital Identities: Challenges and Opportunities for the G20.* ADBI Institute. Retrieved from *https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf*

Kennedy, G., & Lee, K. H. (2021). *Finding Harmony - ASEAN Model Contractual Clauses and Data Management Framework Launched.* Retrieved from *https://www.lexology.com/library/detail.aspx?g=be41251e-f5f0-4062-a02b-5bffbb8f16ad*

Koigi, B. (2020, 08 10). *Africa data centre market to reach $3 billion by 2025.* Retrieved from Africa Tech: *https://africabusinesscommunities.com/tech/tech-news/africa-data-center-market-to-reach-$3-billion-by-2025-report/*

Kudo, F., & Soble, J. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

Kuo, M. (2022, September 26). Trafficking Data: China's Pursuit of Digital Sovereignty: Insights from Aynne Kokas. *The Diplomat*.

Mattoo, A., & Schuknecht, L. (1999). *Trade Policies for Electronic Commerce.* World Bank. Retrieved from *https://elibrary.worldbank.org/doi/10.1596/1813-9450-2380*

Mbengue, M. M. (2006, September). *Preamble.* Retrieved from Oxford Public International Law: *https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1456*

McKinsey. (2013, October 1). *Open data: Unlocking innovation and performance with liquid information*. Retrieved from *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information*

McKinsey. (2022, June 30). *Localisation of data privacy regulations creates competitive opportunities*. Retrieved from McKinsey: *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities*

McKinsey. (2022, August 17). *What is the Internet of Things?* Retrieved from McKinsey: *https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things*

Meddin, E. (2020). The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and Article XVII of the General Agreement on Trade in Services. *American University International Law Review, 35*(4).

Mitchell, A. D., & Hepburn, J. (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *19 Yale Journal of Law and Technology 182 (2017)*, 182-237. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2846830*

Mittelstadt, B. (2021). *The impact of Artificial Intelligence on the Doctor-Patent Relationship.* Council of Europe. Retrieved from *https://rm.coe.int/inf-2022-5-report-impact-of-ai-on-doctor-patient-relations-e/1680a68859*

Nordhaug, L. M., & Harris, L. (2021). Digital public goods: Enablers of digital sovereignty. In OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation.* Retrieved from *https://www.oecd-ilibrary.org/sites/c023cb2e-en/index.html?itemId=/content/component/c023cb2e-en*

OAG California. (2023, April 24). *California Consumer Privacy Act (CCPA)*. Retrieved from Office of the Attorney General - State of California Department of Justice: *https://oag.ca.gov/privacy/ccpa*

OECD. (2011). *OECD Guide to Measuring the Information Society 2011.*

OECD. (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (2013). *The OECD Privacy Framework.* Retrieved from *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2020). *OECD Open, Useful and Re-usable Data (OURdata) Index: 2019.*

OECD. (2022). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188.* Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (n.d.). *Data-driven innovation for growth and well-being*. Retrieved from OECD: *https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm*

OECD. (n.d.). *Digital trade*. Retrieved from Organisation for Economic Co-operation and Development: *https://www.oecd.org/trade/topics/digital-trade/*

OECD. (n.d.). *Why data governance matters*. Retrieved from Organisation for Economic Cooperation and Development: *https://search.oecd.org/digital/data-governance/*

OECD. (n.d.). *Personal Data Protection at the OECD*. Retrieved from *https://www.oecd.org/general/data-protection.htm*

OECD, WTO & IMF. (2020). *Handbook on Measuring Digital Trade.* Retrieved from *https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf*

Okwara, E. (2022, September 27). A privacy pro's odyssey in Africa. *International Association of Privacy Professionals*.

One Trust Data Guidance. (2022, December 22). *Morocco: CNDP reminds controllers of data breach procedure*. Retrieved from Data Guidance: *https://www.dataguidance.com/news/morocco-cndp-reminds-controllers-data-breach-procedure*

One Trust Data Guidance. (n.d.). *Morocco*. Retrieved from Data Guidance: *https://www.dataguidance.com/jurisdiction/morocco*

OneTrust. (2022, September 16). *ECOWAS Act on Personal Data Protection*. Retrieved from OneTrust DataGuidance: *https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection*

Onuoha, R. (2022, November 29). *Africa's Leading Lights: Regional Network Readiness for Digital Transformation*. Retrieved from Portulans Institute: *https://portulansinstitute.org/africas-leading-lights/*

Open Data Handbook. (2023). *The Open Data Handbook*. Retrieved from *https://opendatahandbook.org/guide/en/*

POPIA. (n.d.). *POPIA*. Retrieved from POPIA: *https://popia.co.za/*

Redman, T. C. (2015, May 20). *4 Business Models for the Data Age*. Retrieved from Harvard Business Review: *https://hbr.org/2015/05/4-business-models-for-the-data-age*

Research and Markets. (2022). *Africa Data Center Market - Industry Outlook & Forecast 2022-2027.*

Rotella, P. (2012, April 2). *Is Data The New Oil?* Retrieved from Forbes: *https://www.forbes.com/sites/perryrotella/*

SADC. (2021). *Selection of Individual Consultant: Consultancy for Revision and Modernisation of the SADC Data Protection Model Law.*

Sadowski, J. (2016, August 31). *Companies Are Making Money from Our Personal Data, but at What Cost?* Retrieved from The Guardian: *https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon*

Satariano, A. (2018, May 6). *What the G.D.P.R., Europe's Tough New Data Law, Means for You*. Retrieved from The New York Times: *https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html*

Schalkwyk, F. v., Willmers, M., & Schonwetter, T. (2015). *Embedding Open Data Practice: Developing Indicators on the Institutionalisation of Open Data Practices in two African Government.* World Wide Web Foundation. Retrieved from *http://webfoundation.org/docs/2015/08/ODDC-2-Embedding-Open-Data-Practice-FINAL.pdf*

Schenker, C. (2015). *Practice Guide to International Treaties.* Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera .

Simmons, D. (2022, January 13). *17 Countries with GDPR-like Data Privacy Laws*. Retrieved from Comforte: *https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws*

Smart Africa Alliance. (2021). *Artificial Intelligence for Africa Blueprint.* Smart Africa Alliance. Retrieved from *https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf*

Smart Africa Alliance. (2021). *Blueprint for e-Payments for the Facilitation of Digital Trade across Africa.* Retrieved from *https://smartafrica.org/knowledge/blueprint-for-e-payments-for-the-facilitation-of-digital-trade-across-africa/*

Stanford University. (2020). *Artificial Intelligence Definitions*. Retrieved from Stanford University Human-Centered Artificial Intelligence: *https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf*

Thirani, V., & Gupta, A. (2017, September 22). *The value of data*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2017/09/the-value-of-data/*

UK Parliament. (2023, March 8). *British Businesses to Save Billions Under New UK Version of GDPR*. Retrieved from *https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr*

UK Parliament. (2023, April 18). *Parliamentary Bills: Data Protection and Digital Information (No. 2) Bill*. Retrieved from *https://bills.parliament.uk/bills/3430*

UN Global Pulse. (n.d.). *UN Global Pulse Principles on Data Protection and Privacy*. Retrieved from UN Global Pulse: *https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/*

UNCTAD. (2012). *Harmonising Cyberlaws and Regulations: The Experience of the East African Community.* New York and Geneva: United Nations Conference on Trade and Development. Retrieved from *https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf*

UNCTAD. (2016). *Data protection regulations and international data flow: Implications for trade and development.*

UNCTAD. (2018). *Trade Policy Frameworks for Developing Countries: A Manual of Best Practice.*

UNCTAD. (2019). *Digital Economy Report 2019. Value creation and capture: Implications for Developing Countries.* New York: United Nations Conference in Trade and Development. Retrieved from *https://unctad.org/system/files/official-document/der2019_en.pdf*

UNCTAD. (2021). *Covid-19 and E-Commerce. A Global view.* New York: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf*

UNCTAD. (2021, December 14). *Data Protection and Privacy Legislation Worldwide*. Retrieved from *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.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/der2021_en.pdf*

UNCTAD. (2021). *Estimates of global e-commerce 2019 and preliminary assessment of COVID-19 impact on online retail 2020. UNCTAD Technical Notes on ICT for Development No. 18.* United Nations. Retrieved from *https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf*

UNCTAD. (2021). *Global E-Commerce Jumps to $26.7 Trillion, Covid-19 Boosts Online Retail Sales*. Retrieved from UNCTAD: *https://unctad.org/press-material/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-retail-sales*

UNCTAD. (2023). *G20 Members' Regulations of Cross-Border Data Flows.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf*

UNDG. (2017). *United Nations Sustainable Development Goals Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection.* United Nations Development Group.

United Nations. (2018). *Personal Data Protection and Privacy Principles.* Retrieved from *https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf*

United Nations. (2023). *Digital Inclusion.* Retrieved from *https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf*

WEF. (2011). *Personal Data: The Emergence of a New Asset Class.* Geneva: World Economic Forum.

WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.* World Economic Forum.

WEF. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

WEF. (2023). *Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows.*

World Bank. (2019). *Starting an Open Data Initiative*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021, May 13). *http://opendatatoolkit.worldbank.org/en/starting.html*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021). *World Development Report 2021: Data for Better Lives.* Retrieved from *https://www.worldbank.org/en/publication/wdr2021*

World Bank. (2023). *Identification for Development (ID4D) Practitioner's Guide*. Retrieved from *https://id4d.worldbank.org/guide/*

World Bank. (n.d.). *Starting an Open Data Initiative*. Retrieved from *http://opendatatoolkit.worldbank.org/en/starting.html*

WTO. (1999). *Council for Trade in Services – Report of the Meeting Held on 14 and 15 December 1998 – Note by the Secretariat, Doc. S/C/M/32.*

WTO. (1999). *Work Programme on Electronic Commerce – Progress Report to the General Council – Adopted by the Council for Trade in Services on 19 July 1999, Doc. S/L/74, 27 July 1999.*

WTO. (2016). *GATS 3 Article XIV (DS reports).*

WTO. (2021). *WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore.*

WTO. (2023, March 30). *E-commerce negotiators advance work, discuss development and data issues*. Retrieved from World Trade Organisation: *https://www.wto.org/english/news_e/news23_e/jsec_30mar23_e.htm*

WTO. (n.d.). *Joint Initiative on E-commerce*. Retrieved from World Trade Organisation: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*

WTO Plurilaterals. (n.d.). *Joint Statement Initiative on Electronic Commerce*. Retrieved from WTO Plurilaterals: *https://wtoplurilaterals.info/plural_initiative/e-commerce/*

Yayboke, E., & Ramos, C. G. (2021, July 23). The Real National Security Concerns over Data Localization. *CSIS*.

Zillner, S., & Neururer, S. (2016). Big Data in the Health Sector (Chapter 10). In J. M. Cavanillas, E. Curry, & W. Wahlster, *New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe* (pp. 179-194). Springer Open.

ANNEXES

ANNEX 1. GLOSSARY

As the digital realm is still under evolution, there have been no agreed definitions for many of the terms related to digital trade and digital economy. Therefore, the definitions below are provided with the aim to facilitate discussion rather than dictating a fixed interpretation of the terms.

Artificial Intelligence (AI) was termed by emeritus Stanford Professor John McCarthy in 1955 as "the science and engineering of making intelligent machines" (Stanford University, 2020). AI is intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals, which involves consciousness and emotionality. As a technology, AI is a field that combines computer science and robust datasets, to enable problem-solving. It also encompasses sub-fields of machine learning and deep learning, which are frequently mentioned in conjunction with artificial intelligence (IBM, n.d.).

Data governance refers to diverse arrangements, including technical, policy, regulatory or institutional provisions, that affect data and their cycle (creation, collection, storage, use, protection, access, sharing and deletion) across policy domains and organisational and national borders (OECD, n.d.). While the scope can be interpreted broadly, the central questions around data governance boil down to four key themes: who owns the data and what these data rights entail; who is allowed to collect what data; the rules for data aggregation; and the rules for data rights transfer (CIGI, 2018).

Data localisation is used to refer to requirements that data be stored and/or processed within the domestic territory (González, Casalini, & Porras, 2022). Some go further to require all processing and derivative use of data to remain within national boundaries (IIF, 2020). In the context of trade agreements, data localisation tends to fall under the provision of 'location of computing facilities', which requires "use or locate computing facilities in [a] Party's territory as a condition for conducting business in that territory".

Data ownership refers to both the possession of and responsibility for information (Zillner & Neururer, 2016). In other words, data ownership can be understood as a form of property or as a form of control. It is, however, difficult to fit 'data ownership' into the traditional property law, as being intangible assets, data typically involve complex assignment of different rights across different data stakeholders, requiring "the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others" (OECD, 2015).

Data sovereignty refers to a policy approach which advocates that data should be subject to the laws and regulations of the country in which it is generated. The demand for data sovereignty is driven by concerns about the control and ownership of data, particularly in the context of cloud computing and cross-border data flows (Gao, 2022). See also 'digital sovereignty.'

Data-driven innovation (DDI) refers to the use of data and analytics to improve or foster new products, processes, organisational methods and markets (OECD, 2015). This is often associated with the generation and use of huge volumes of data – commonly referred to as "big

data" – to foster new industries, processes and products and create significant competitive advantages (OECD, n.d.).

Digital economy was termed for almost 30 years since the typically-cited origin of the term in Don Tapscott's 1996 book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence". Since then, several definitions have emerged with different approaches to define the digital economy (Bukht & Heeks, 2017). One approach is to refer to the digital economy as "that part of economic output derived solely or primarily from digital technologies with a business model based on digital goods or services" (UNCTAD, 2019; Bukht & Heeks, 2017).

Digital sovereignty refers to the power and authority of a national government to make free decisions affecting citizens and businesses within the digital domain – with broad coverage encompassing data, software, standards and protocols, infrastructure, and public services (Gawen, Hirschfeld, Kenny, Stewart, & Middleton, 2021; Nordhaug & Harris, 2021)

Digital trade covers all trade that is digitally ordered and/or digitally delivered (OECD, WTO & IMF, 2020). The OECD further clarifies that digital trade "encompasses digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments" (OECD, n.d.)

E-commerce refers to the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders". This definition of e-commerce covers orders made on web pages, extranet or EDI while excluding orders made by telephone calls, facsimiles, or manually typed e-mails (OECD, 2011). The WTO E-Commerce JSI consolidated negotiating text as of September 2021 proposes that "[Digital trade/e-commerce] means the production, distribution, marketing, sale or delivery of goods and services by electronic means". This provides a broader definition compared to that of the OECD, as it covers all transactions whereby at least one stage of commerce is done using electronic means.

Internet of Things (IoT) describes physical objects embedded with sensors and actuators that communicate with computing systems via wired or wireless networks—allowing the physical world to be digitally monitored or even controlled (McKinsey, 2022).

Location of computing facilities refers to the requirements of domestic regulations to locate computer servers and storage devices for processing or storing information for commercial use within a country's territory as a condition for conducting business in that territory (Article 4.4, DEPA).

Machine Learning, as a field of study, refers to the field of study of how computer agents can improve their perception, knowledge, thinking, or actions based on experience or data. For this, machine learning draws from computer science, statistics, psychology, neuroscience, economics and control theory (Stanford University, 2020). In terms of application, machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy (IBM, n.d.).

Open data refers to digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed (Article 9.1, DEPA).

Personal data means any information relating to an identified or identifiable individual (OECD, 2022). Some frameworks use a similar term, 'personal information', which refers to "information, including data, about an identified or identifiable natural person" (Article 1.3, DEPA).

Personal data protection refers to the area of law that provides administrative or technical measures which are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness (OECD, 2013). This can also be referred to as "data protection laws" or "privacy laws".

ANNEX 2. EXAMPLES OF INTERNATIONAL FRAMEWORKS ON DATA GUIDELINES

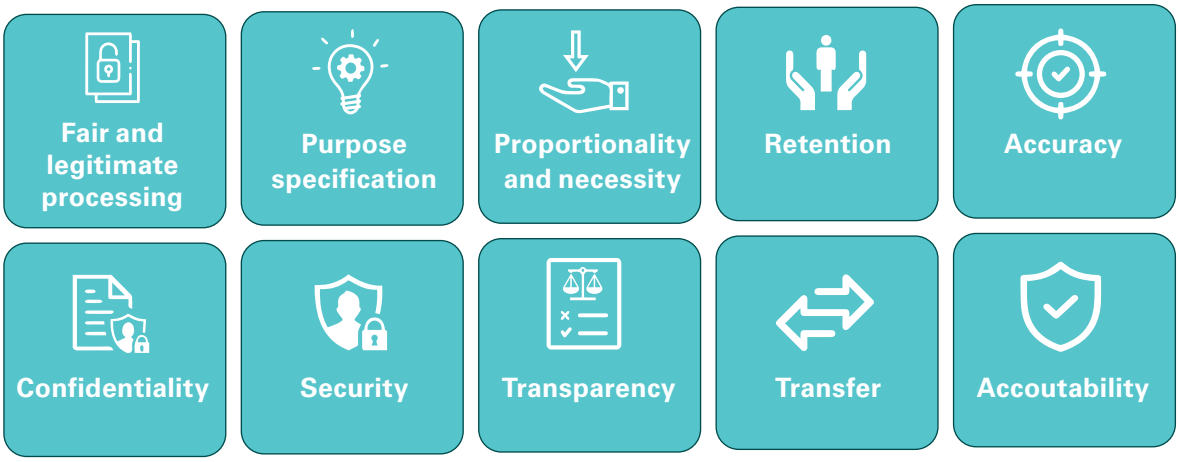
Some of the most notable international frameworks are discussed in this annex as an examination of the good practices, while some domestic regulatory frameworks are also briefly discussed as to how jurisdictions correspond to data issues.

(I) UN PRINCIPLES AND GUIDELINES

The United Nations (UN) has developed a set of data privacy principles that aim to promote the responsible use of data for sustainable development while also safeguarding privacy and protecting human rights (UN Global Pulse, n.d.). These include the UN Principles on Personal Data Protection and Privacy 2018 (the 'Principles') and the UN's Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection (the 'Guidance').

The Principles, comprising ten rules, set out a basic framework for the processing of "personal data" by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities. These principles aim to: (i) harmonise standards for the protection of personal data across the UN System; (ii) facilitate the accountable processing of personal data; and (iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy. These Principles may also be used as a benchmark for the processing of non-personal data (United Nations, 2018).

Figure 10. Ten UN Principles on Personal Data Protection and Privacy



Source: (United Nations, 2018)

The Guidance is centred around nine principles **(Error! Reference source not found.)** designed to support members and partners of the United Nations Development Group in establishing an efficient and coherent framework on data privacy, data protection and data ethics for the United Nations Development Group (UNDG) concerning the use of big data. It should be noted that the Guidance is not a legal document; instead, it provides only a minimum basis for self-regulation that could be further expanded and elaborated on by the implementing organisations (UNDG, 2017). Given its broader scope, the Guidance principles for data also provide more elaborated guidance on the expected standards of data processing and use, as well as on risk management and data quality control. A summary of the principles is provided in Annex 4.

Figure 11. Nine Principles of the UN Guidance Note on Big Data

(II) THE OECD PRIVACY GUIDELINES

The Organization for Economic Cooperation and Development (OECD) Privacy Guidelines are also an important international framework for data protection. The OECD Privacy Guidelines were first adopted in 1980 to guide the responsible handling of personal data and have since been updated and revised to conform with the rapidly changing landscape of data privacy (OECD, n.d.). The OECD's Privacy Guidelines are based on certain fundamental principles centred around the importance of data quality, purpose specification, accountability, and individual rights (OECD, 2013). Thus, the principles require, among other obligations, that organisations obtain the consent of individuals prior to collecting or using their personal data and that appropriate measures are in place to safeguard personal data from unauthorised access or use (OECD, 2013).

One of the key characteristics of the OECD Privacy Guidelines is their emphasis on cross-border data flows. The OECD Privacy Guidelines emphasise the importance of adopting comprehensive data protection laws that include provisions for cross-border data transfers whereby adequate safeguards need to be maintained in such transfers. Moreover, the Guidelines state that any limitations imposed on the transborder flow of data must be proportional to the risks (OECD, 2013). The Guidelines also emphasise the importance of international cooperation and interoperability.

(III) APEC PRIVACY FRAMEWORK & APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

Among the well-established initiatives to promote international standards for data governance rule-making are the APEC Privacy Framework, the APEC Cross-Border Privacy Rules (CBPR) System, and the Association of Southeast Asian Nations (ASEAN) Data Management Framework (DMF) and Model Contractual Clauses (MCCs) for Cross Border Data Flows.

- The APEC Privacy Framework provides principles for the collection, holding, processing, use, transfer or disclosure of personal information applied to persons or organisations in the public and private sectors who control each of the afore-mentioned processes. This Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows (APEC, 2005).
- The APEC Cross-Border Privacy Rules (CBPR) System is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognised data privacy protections (APEC, 2019). The CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework.
- The ASEAN DMF is designed to provide practical guidance for all private sector businesses in the implementation of a data management system based on good management practices and fundamental principles, using a risk-based methodology.
- The MCCs are standard contractual terms and conditions that are recommended in agreements relating to the cross-border transfer of personal data between businesses in the region, and which are meant to encapsulate key data protection obligations and reduce negotiation and compliance costs (Kennedy & Lee, 2021).

While all of these initiatives are far from archiving their full scope and impact, they provide examples of good practices in building up regional and international data governance standards towards an open digital economy.

(IV) DATA FREE FLOW WITH TRUST INITIATIVE

A more recent initiative, the World Economic Forum (WEF) Data Free Flow with Trust, equally aims to facilitate the free flow of data while ensuring trust in data privacy and security. Pitched by the former Japanese Prime Minister, Abe Shinzo, in 2019, the WEF Data Free Flow with Trust (DFFT) initiative is founded on the premise that the free flow of data is crucial for economic growth and innovation and that data protection and privacy is key to maintaining trust in the digital economy (WEF, 2020). Hence, the initiative seeks to find a balance between promoting the free flow of data and the protection of personal information.

The principles outlined in the WEF Data Free Flow with Trust initiative are intended to provide a framework for policymakers and industry leaders to develop enabling regulatory frameworks (WEF, 2022). A roadmap for cooperation was adopted in 2021, focusing on four areas of cooperation, namely data localisation; regulatory cooperation; government access to data; and data sharing for priority sectors (Arasasingham & Goodman, 2023). An action plan was further designed in 2022, and it extends cooperation on future digital regulatory interoperability and the sharing of knowledge on international data spaces (Arasasingham & Goodman, 2023). Given its international scope and the focus of the private sector, the initiative could help to reduce regulatory fragmentation globally, which would ease businesses' accessibility and use of data across borders. However, a common caveat with the initiative, as well as with the other frameworks discussed, is that it is difficult for countries to develop a common regulatory framework as different jurisdictions have different legal and regulatory frameworks and understandings of data protection and privacy that renders it difficult to develop a common set of principles and guidelines that can apply everywhere (WEF, 2023).

The EU GDPR as comprehensive and robust regulations on data protection. Given its depth and broad scope of coverage, the GDPR has served as an inspiration for many legislations around the world. This includes Brazil's General Law for the Protection of Personal Data, data protection legislation in California and Virginia, as well as India's proposed Digital Personal Data Protection Bill (Bryant, 2021). Some of the distinctive provisions of the EU GDPR that have earned the law its reputation include:

- Extra-territorial application: While the EU GDPR has been adopted by the EU, it is applicable to any entity that processes or collects data pertaining to EU subjects, irrespective of whether the entity is located within the EU or not (GDPR.EU, n.d.).
- Consent: In processing, collecting, or using the information of EU subjects, the GDPR requires that all entities procure the unambiguous consent of individuals concerned. Moreover, data subjects can withdraw previously given consent at any given time.
- Data subject rights: The GDPR recognises numerous privacy rights for data subjects, which give individuals greater control over the data that organisations may collect, store, or process on them.
- Enforcement and sanctions: Non-compliance with the GDPR can result in penalties amounting to up to EUR 20 million or 4% of global annual revenue, whichever is higher.

The EU GDPR also imposes certain restrictions on the transborder flow of personal data. As per the provisions of the GDPR, personal data can only be transferred to territories where an adequate level of protection is guaranteed under domestic laws. The European Commission is responsible for determining the adequacy of the level of data protection in non-EU countries.

Only a few countries are recognised as having adequate laws (European Commission, n.d.).[80] Where there is no adequacy, organisations have recourse to other legal mechanisms to transfer personal data outside of the EU. These can include standard contractual clauses, binding corporate rules, codes of conduct and certification mechanisms (European Commission, n.d.).

The EU has also adopted legislation with regard to the flow of non-personal data. One of the aims of the EU is to facilitate the movement of data within Europe, enabling organisations and governments to collect and manage non-personal data at any location of their choice within the bloc (European Commission, n.d.). The Regulation on a framework for the free flow of non-personal data thus aims to eliminate any hurdles that hinder the free flow of non-personal data between different EU countries. The Regulation supplements the GDPR and ensures a consistent and coherent approach to the free movement of all data in the EU. Some of the key obligations that arise under the Regulation include data availability for regulatory control, data portability between cloud service providers for professional users, and better consistency and coherence with cybersecurity concerns (European Commission, n.d.).

ANNEX 3. UN'S PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES

1. FAIR AND LEGITIMATE PROCESSING

The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations System Organization concerned; (iii) the mandates and governing instruments of the United Nations System Organization concerned; or (iv) any other legal basis specifically identified by the United Nations System Organization concerned.

2. PURPOSE SPECIFICATION

Personal data should be processed for specified purposes which are consistent with the mandates of the United Nations System Organization concerned and take into account the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.

3. PROPORTIONALITY AND NECESSITY

The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

80 The countries that have been recognized as having adequate data protection laws by the EU Commission include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom, and Uruguay.

4. RETENTION

Personal data should only be retained for the time that is necessary for the specified purposes.

5. ACCURACY

Personal data should be accurate and, where necessary, up to date to fulfil the specified purposes.

6. CONFIDENTIALITY

Personal data should be processed with due regard to confidentiality.

7. SECURITY

Appropriate organisational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorised or accidental access, damage, loss or other risks presented by data processing.

8. TRANSPARENCY

Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, the provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data insofar as the specified purpose for which personal data is processed is not frustrated.

9. TRANSFERS

In carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfies itself that the third party affords appropriate protection for the personal data.

10. ACCOUNTABILITY

United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles.

ANNEX 4. UN'S GUIDANCE NOTE ON BIG DATA: KEY PRINCIPLES

1. LAWFUL, LEGITIMATE AND FAIR USE

Data must be collected and used in a lawful, legitimate, and fair manner, either directly or through a contract with a third-party data provider. Data access, analysis, or other uses should comply with applicable laws, including data privacy and data protection laws, as well as the highest standards of confidentiality and moral and ethical conduct. Adequate consent from the individual whose data is being used is also emphasised. The legitimate interests of individuals whose data is being used should be taken into account when accessing, analysing, or using data to ensure that data use is fair. Data should not be used in a manner that violates human rights, or that is likely to cause unjustified or adverse effects. Hence, to ensure that data use is legitimate and fair, risks, harms, and benefits should always be assessed.

2. PURPOSE SPECIFICATION, USE LIMITATION AND PURPOSE COMPATIBILITY

Data use must align with the purpose for which it was obtained. The purpose cannot be altered unless there is a legitimate basis. Moreover, the purpose must be lawful, and it should be as narrowly defined and precise as possible. Additionally, the purpose of data access and collection should be clearly stated at the time of access or collection.

3. RISK MITIGATION AND RISKS, HARMS AND BENEFITS ASSESSMENT

Data should be collected and used in compliance with applicable laws, respecting individuals' privacy and protecting their rights. The use of sensitive data should involve consultation with the concerned groups or their representatives to mitigate associated risks. Any potential risks and harms should not be excessive in relation to the benefits of data use.

4. SENSITIVE DATA AND SENSITIVE CONTEXTS

When collecting, accessing or analysing data related to vulnerable groups or that is classified as sensitive, stricter data protection measures should be enforced. Furthermore, it's important to take into account that non-sensitive data can become sensitive depending on the context in which it is used, such as cultural or political factors, and how it affects individuals or groups.

5. DATA SECURITY

Robust technical and organisational safeguards must be implemented to ascertain proper management of data and prevent any unauthorised use or disclosure of personal data. Privacy-enhancing technologies should be used throughout the data lifecycle to this end. Moreover, wherever applicable, personal data should be de-identified in an attempt to mitigate any risks to privacy.

6. DATA RETENTION AND DATA MINIMISATION

The access, analysis and use of data access should be kept to the minimum amount necessary so that it only fulfils its intended purpose. Moreover, the amount of data collected should be restricted to the minimum required as well. In order to ensure that these are adhered to, the use of data should be subject to monitoring. Moreover, following the use of data, it should be permanently deleted unless its retention is warranted.

7. DATA QUALITY

Data should be checked for accuracy, relevance, integrity, completeness, and usability, and kept up-to-date. Low-quality data entail risks and must be assessed for biases that can result in unlawful and arbitrary discrimination. Automatic processing of data should be avoided, especially when it can have an impact on individuals or groups. Moreover, periodic assessments of data quality should be conducted during the data life cycle.

8. OPEN DATA, TRANSPARENCY AND ACCOUNTABILITY

Open data is important for driving innovation, transparency, and accountability, and data should be made open whenever possible unless the risks outweigh the benefits or there are other legitimate reasons not to do so. It is also important to establish appropriate governance and accountability mechanisms to ensure compliance with relevant laws. Transparency is crucial for accountability. It is recommended to publicly disclose information about the use of data, including the nature, purpose, and retention period, as well as the algorithms used for processing data, in clear and simple language understandable by the general public.

9. DUE DILIGENCE FOR THIRD-PARTY COLLABORATORS

In working with third-party collaborators who use data should follow relevant laws, including privacy laws, and adhere to high standards of confidentiality, morality, and ethics. To ensure compliance, a due diligence process should be conducted to evaluate the data practices of potential third-party collaborators. Additionally, legally binding agreements should be established that outline the parameters for accessing and handling data.

African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
www.au.int