



# Trade Hot Topics

## Energising Africa's Digital Economy: Cross-Border Data Flows and the African Continental FTA

Kyle de Klerk<sup>1</sup>

### 1. Introduction

The African Continental Free Trade Area (AfCFTA) is the largest free trade agreement in the world by number of members and geographical area covered. It spans 54 African countries,<sup>2</sup> with a combined gross domestic product (GDP) of US\$3.5 trillion and 1 billion consumers. Although initial trading under the agreement officially commenced in 2021, there are still ongoing negotiations on several outstanding protocols. One of these, known as the Digital Trade Protocol, has been pushed up the negotiating agenda as COVID-19-induced digitalisation offers African countries the opportunity to leapfrog traditional industrialisation and pursue a digital-led development strategy.

This is underpinned by the growing importance of data, both for the digital economy in general and for achieving the Sustainable Development Goals (SDGs), particularly targets 9.b and 9.c. The global proliferation of internet-connected devices, the decreasing costs of bandwidth and internet access, and the exponential growth in computing power and storage capacity are all causing data to be generated, collected, stored, processed and used at unprecedented levels. This has led to a corresponding increase in the amount of data that has

flowed between countries, known as 'cross-border data flows', and upon which the digital economy and digital trade depends. In 2022, it is estimated that the size of global cross-border data flows surpassed the cumulative volume of all internet traffic before 2016 (UNCTAD, 2021).

As the importance and quantity of cross-border data flows continue to grow, so do the regulatory interests of governments. Concerns about digital risks to national security and the privacy of citizens have led to a proliferation of cybersecurity and data protection regulations, many of which restrict the transfer of data to other countries. Governments are also increasingly looking towards such restrictions as a form of digital infant industry policy, or as a means of inducing foreign investment from digital multinational firms with small domestic asset investments. This has led to a rising number of trade agreements that include provisions prohibiting the restriction of cross-border data flows between their members, subject to privacy and security exemptions.

It is provisions such as these that are currently under negotiation, and that are due to be included in the forthcoming AfCFTA Digital Trade Protocol.<sup>3</sup> This issue of *Trade Hot Topics* provides an overview

1 Kyle de Klerk is an Assistant Research Officer in the International Trade Policy Section, Commonwealth Secretariat. Any views expressed are those of the author and do not necessarily represent those of the Commonwealth Secretariat

2 At the time of writing, 46 countries had deposited instruments of ratification.

3 While the exact scope of the Digital Trade Protocol remains confidential, the Secretary-General of the AfCFTA Secretariat has stated that the protocol will be 'comprehensive... and will cover very important areas such as data flows and transfer of data across regions of the African continent'. See: <https://youtu.be/UpCox4Njfc?t=1619>

of the ongoing debate regarding cross-border data flows and their restriction. It examines this debate in light of Africa's digital needs and explores how cross-border data flows are regulated in the multilateral trading system and other large regional trade agreements, as well as by different African countries. It concludes with some recommendations for the negotiations on the AfCFTA Digital Trade Protocol.

## 2. Cross-border data flows and Africa's digital economy

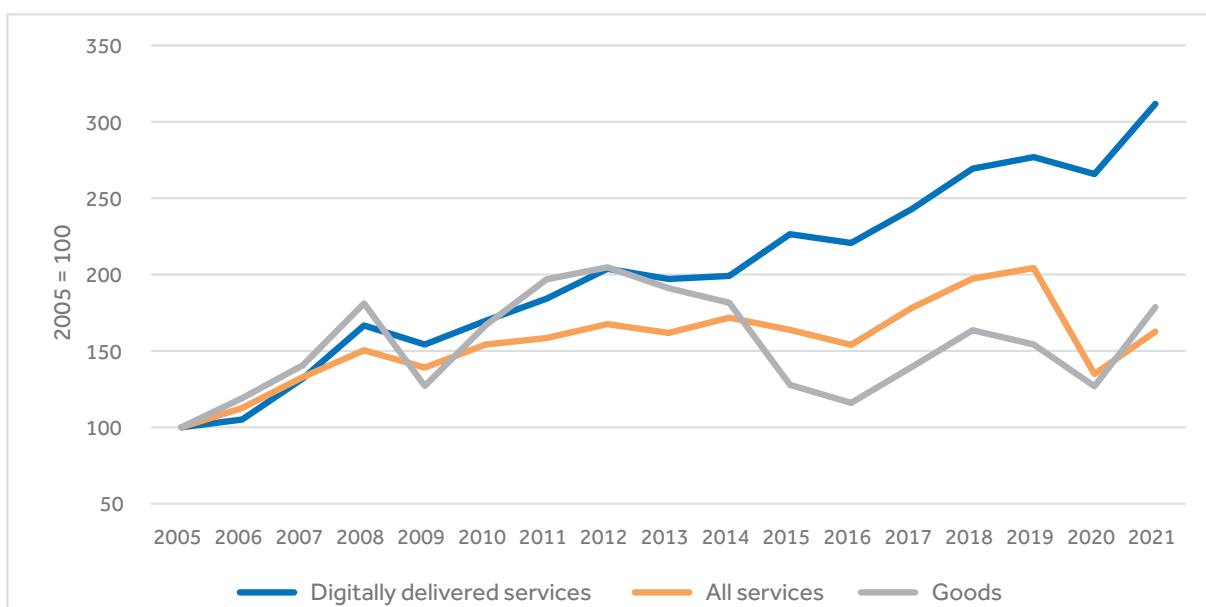
The value of Africa's collective digital economy, having tripled from US\$30 billion in 2012 to US\$99.7 billion in 2019, is expected to almost double to US\$180 billion by 2025 (IFC and Google, 2020). This is reflected by the growth in Africa's digital services exports from US\$9 billion in 2005 to US\$33 billion in 2022, far exceeding the growth rates of more traditional exports over this period (Figure 1).

This growth has been facilitated by rapid increases in bandwidth availability,<sup>4</sup> the growing adoption of more affordable internet-enabled mobile devices and expanding engagement with the digital economy. Since 2014, the number of e-commerce consumers within Africa has grown by an annual rate of 21 per cent, almost double that of the world average (Chivunga and Tempest, 2021). Africa's share of digitally deliverable services in total services exports grew from 17 per cent in 2005 to 33 per

cent in 2021, a faster rate than for any other region (Figure 2).<sup>5</sup> In total, the digital economy is expected to create 230 million new jobs in Africa by 2030 (AU, AfDB and UNECA, 2017).

Cross-border data flows are an integral part of this growth, serving as the medium through which digital services and goods are traded. They also hold great importance for the development of new 'disruptive' or 'frontier' technologies such as big data analytics and artificial intelligence (AI), where they are integral to what are known as the 'three Vs': volume (quantity of data), velocity (age/relevance of data) and variety (complimentary types of data). The eventual value of many of these technologies depends on the quality of input data used to generate insights, which in turn depends on maximising these three Vs, as well as the veracity (the accuracy) of data. As such without the ability to draw on data originating in different countries, the usefulness of these technologies will be limited. AI has recently been thrust into the spotlight with the release of publicly available large language models such as OpenAI's GPT-4 and Google's Bard, which are set to transform both Africa's and the global digital economy. The rapid diffusion and adoption of these technologies, along with their dependence on data's volume, variety and velocity, are likely to increase the size and importance of cross-border data flows significantly.

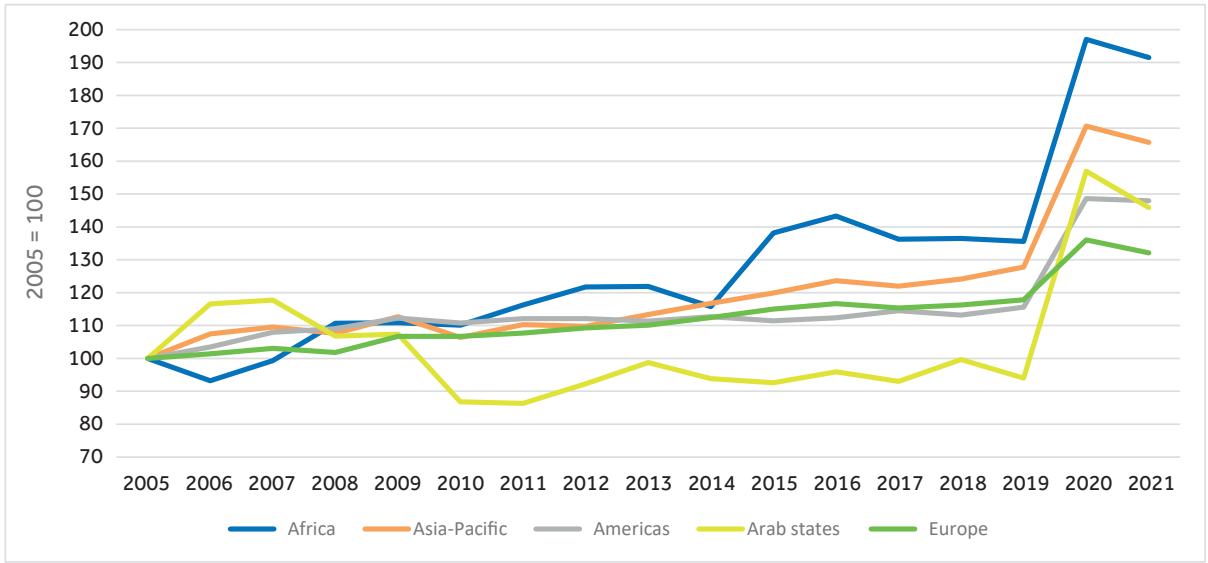
Figure 1. Growth of African exports (2005 baseline)



Source: Commonwealth Secretariat (using data from the World Trade Organization [WTO] and the UN Conference on Trade and Development [UNCTAD]).

4 Africa's inbound international bandwidth capacity grew by a factor of ten between 2009 and 2019 (African Union and OECD, 2022).  
 5 Although its absolute share still lags far behind other regions: 34 per cent compared to 71 per cent in the Americas, 65 per cent in Europe, 55 per cent in Asia and the Pacific, and 40 per cent in Arab countries.

**Figure 2. Growth in Africa’s digitally deliverable services as a share of total services exports**



Source: Commonwealth Secretariat (using data from UNCTADStat).

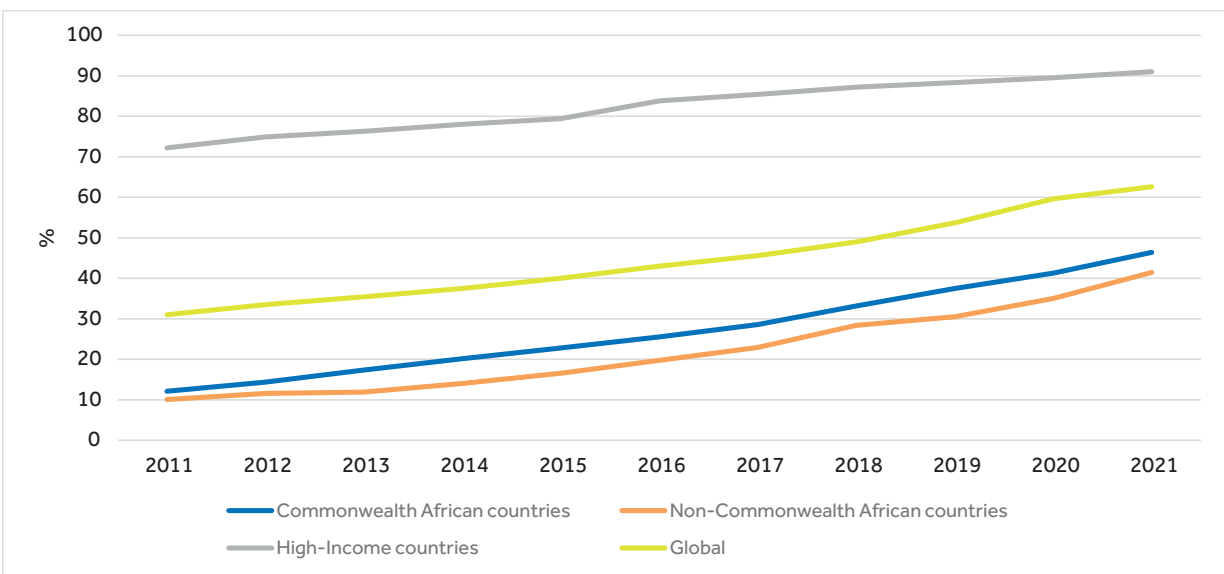
### 2.1 Africa’s digital divide

While digitalisation holds great promise for African development, its benefits will fail to materialise if the digital divide among Africa countries and between the continent and the world persists. Despite rapid increases in the penetration of mobile internet and the use of mobile devices, only 32.8 per cent of the African population consistently use the internet, the lowest proportion of internet users of any continent in the world (see Figure 3). This divide also applies between and within African countries, with least developed countries (LDCs) and rural areas generally having even lower levels of internet access and use (see the appendix for internet usage rates in individual African countries).

In addition, the relatively high penetration of mobile internet coverage is deceptive as it depends on outdated infrastructure that is only capable of providing limited bandwidth. As a result, 59 per cent of internet-enabled devices in Africa use 2G and only 49.2 per cent of the African population has access to long-term evolution (LTE)-enabled mobile networks (see Figure 4). While over 80 per cent of African mobile users can access the internet, they lack sufficient bandwidth capacity for full participation in the digital economy (Fajarnes et al., 2022).

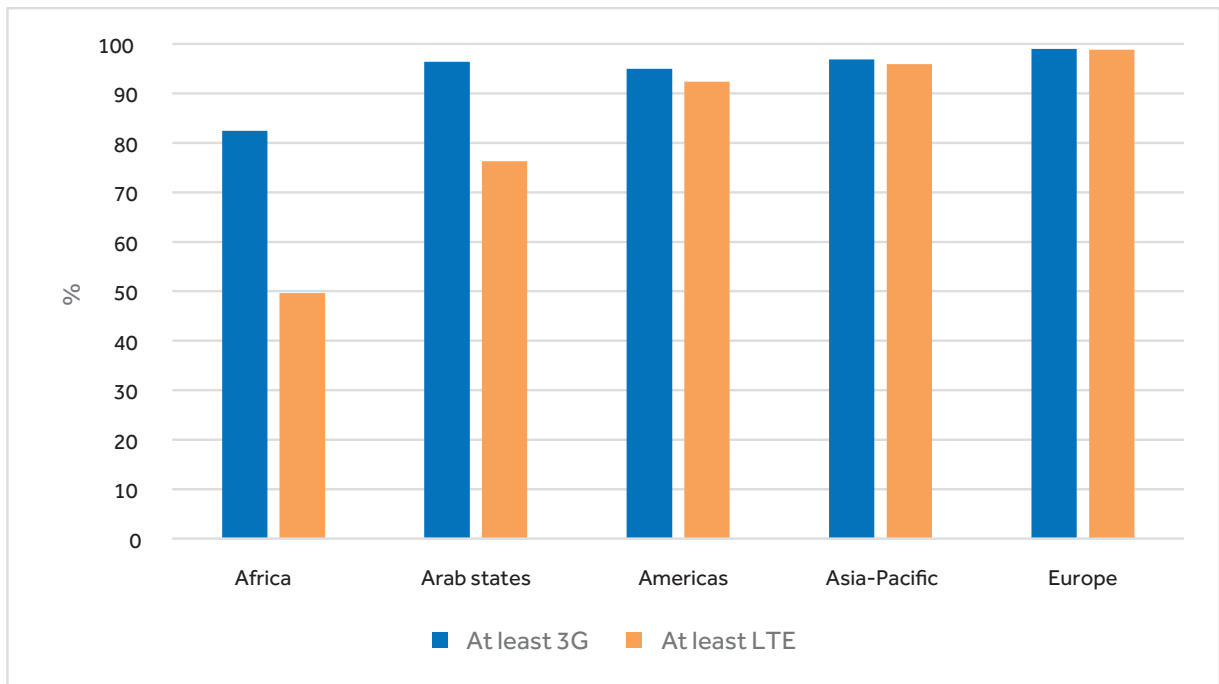
Those users in Africa who have access to LTE pay a high price due to a lack of competition and low economies of scale that inflate data prices. In absolute terms, Africa has the second-most expensive

**Figure 3. Percentage of the African population using the internet**



Source: Commonwealth Secretariat (using data from the International Telecommunication Union [ITU]).

**Figure 4. Percentage of the African population covered by mobile networks (2021)**



Source: Commonwealth Secretariat (using data from ITU).

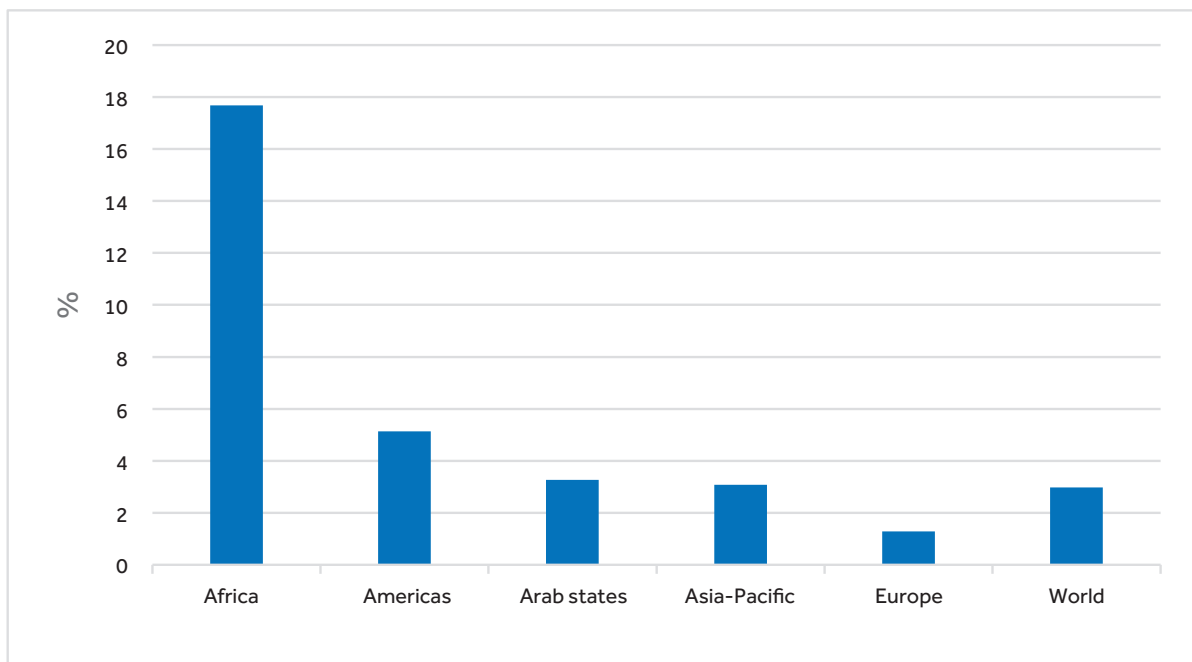
data among all regions, while in relative terms, it is by far the most expensive region. Only 12 African countries are considered to have affordable data, defined as being less than 2 per cent of gross national income (GNI) per capita (see the appendix) (A4AI, 2021).

The high prices, low penetration rates and limited economies of scale in Africa reflect the lack of information and communication technology (ICT) infrastructure, particularly data centres necessary for the provision of affordable mobile and cloud

computing services: Africa has 28 servers per million people, the lowest in the world and almost half that of Latin America (50) and Southeast Asia (54) (Lemma et al., 2022).

These digital capacity constraints must be addressed for the African digital economy to flourish. Part of the solution to this issue is increasing investment into and construction of ICT infrastructure, as well as facilitating the use of demand- and supply-side economies of scale by data service providers. Cross-border data flows are integral

**Figure 5. Price of fixed-broadband basket 5GB (2021, percentage of GNI per capita)**



Source: Commonwealth Secretariat (using data from ITU).

to both, fuelling digital integration that allows African countries with relatively developed ICT infrastructure to aggregate regional demand to levels sufficient to incentivise investment and construction of advanced ICT infrastructure, such as data centres (World Bank, 2023). Without allowing data to flow across borders, African countries will struggle to induce investment into small domestic markets with nascent digital sectors.

### 3. The regulation of cross-border data flows

While conventional economic logic suggests that data should flow freely, many countries impose restrictions on its movement in practice. Data localisation requirements,<sup>6</sup> which intend to balance the economic uses of data with its social, distributive and security implications, are imposed as restrictions on cross-border data flows in many countries. These may take a variety of forms, outlined in Table 1.

**Table 1. Typology of data localisation measures**

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

Source: Commonwealth Secretariat, drawing upon models developed by UNCTAD and the World Bank

Localisation requirements are motivated by various factors, including inducing foreign investment from digital multinational firms, maximising the gains of digitalisation for domestic firms, protecting the privacy of citizens, addressing threats to national and cyber security, and ensuring government regulatory oversight and accessibility of data for law enforcement purposes. This section will briefly examine some of these common policy objectives.

#### 3.1 The economic debate on data localisation

The economic impacts of data localisation and cross-border data flows are subject to intense debate. Opponents of data localisation point out that cross-border data flows are necessary for

the internet — and therefore the digital economy as a whole — to function in the most optimal and cost-effective way. The internet consists of an interconnected web of people, devices and businesses spread across the world. Typically, the sending and receiving of data from one part of this web to another relies on the 'client-server' model, whereby a server stores data that is accessed by 'clients', such as a smartphone. Importantly, given that the internet consists of several global networks containing millions of interlinked servers, any single request for data will require it to flow through numerous servers located in many different countries.

The result is that almost no activity on the internet involves purely domestic flows of data, and national borders are largely irrelevant to the efficiency of internet traffic. Consequently, digital service providers utilise business models that depend on cross-border data flows to cut costs, optimise their operations, raise the quality of their services and trade their services across borders (NFTC, 2011). For example, the cross-border provision of large-scale cloud computing services lowers costs for digital start-ups and reduces barriers to entry to both domestic and international markets, while cross-border data flows more generally are necessary for businesses to connect to the global digital marketplace. As such, the imposition of data localisation requirements is thought to have a net negative impact on the domestic digital economy, a view supported by several empirical studies.<sup>7</sup>

However, and inspired by China's strict localisation measures, many policy-makers in the developing world are considering using data localisation as a form of industrial policy in response to the following factors:

1. The unrestricted flow of data out of a country is often seen as benefiting only a few digital multinationals that dominate the global digital economy. This can come at the expense of local micro, small and medium-sized enterprises (MSMEs) that lack the skills, hardware and financial resources to compete on a level playing field.

6 While the scope of the term 'data localisation' is contested, this THT uses 'data localisation' to refer to all regulatory measures that directly or indirectly prevent data from flowing across borders.

7 Studies have shown that localisation requirements can: negatively impact on the import of digital services (Ferracane and van der Marel, 2019); significantly undermine the domestic FinTech industry (Aguerre, 2018); lead to substantial cross-sectoral productivity losses that outweigh any gains to local digital service providers (Ferracane and van der Marel, 2020); fail to increase employment or the number of digital jobs (Cory and Dascoli, 2021); and have negative spillover effects that harm the disposable income of consumers (Bauer et al., 2014).

2. Digital multinationals mostly do not need to establish large physical presences in the markets where they operate, leading to very small foreign direct investment (FDI) inflows compared to their earnings.
3. Domestic MSMEs lack the vast user bases and data processing capabilities of digital multinationals, leading to informational asymmetries that lock in the latter's advantage (WEF, 2020).

The rationale behind the imposition of localisation requirements is that the added regulatory burden can act as a form of digital infant industry protection, while also compelling digital multinationals to invest in the local digital infrastructure and human capital required for the domestic storage and processing of their data. This investment is believed to result in spillover effects for the wider domestic digital economy.<sup>8</sup>

### 3.2 Data localisation for national and cybersecurity

With the growing dependence of governance operations on digital tools, many governments stipulate that certain types of data, such as information relating to defence, intelligence, diplomatic, and other confidential and sensitive activities, must be stored within the country to safeguard national security. In addition to protecting these digital elements of traditional national security domains, state-level cybersecurity policy is also concerned with protecting the physical infrastructure that it considers essential for the functioning of the country. This is often referred to as 'critical infrastructure' and typically includes energy, transport, defence and ICT infrastructure, all of which are increasingly becoming digitalised and thus vulnerable to digital disruption. As a result, as part of their cybersecurity regulations, states may impose various localisation measures such as licensing, testing, registration, or domestic storage and processing requirements for data that relate to the operation of critical infrastructure. However, few African countries have imposed such requirements, particularly compared to data protection localisation discussed below.

### 3.3 Data localisation as data protection

In the digital context, the gathering, storage and processing of personal data to produce insights raises privacy concerns. These concerns have been exacerbated by the growing awareness of the

online mass surveillance practised by both governments and private actors (Aaronson, 2015; Zuboff, 2019). Governments have become increasingly suspicious of unrestricted and unmonitored transmission of personal data to other countries and have adopted various privacy and data protection regulations that impose localisation requirements. Notably the European Union's (EU's) General Data Protection Regulation (GDPR), which entered into force in 2018, imposes conditional transfer requirements for personal data and is widely recognised as the trailblazing framework for privacy protection. This has led to its global replication and use as a template for the development of other personal data protection frameworks, particularly within Africa.

The remainder of this THT will analyse data protection localisation regulations, as it is by far the most common policy rationale for localisation measures imposed by African countries.

#### Box 1. Defining personal data

There is no internationally agreed definition of personal data. However, the following commonly cited definition is found in the GDPR, which has seen wide replication across Africa:

*Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

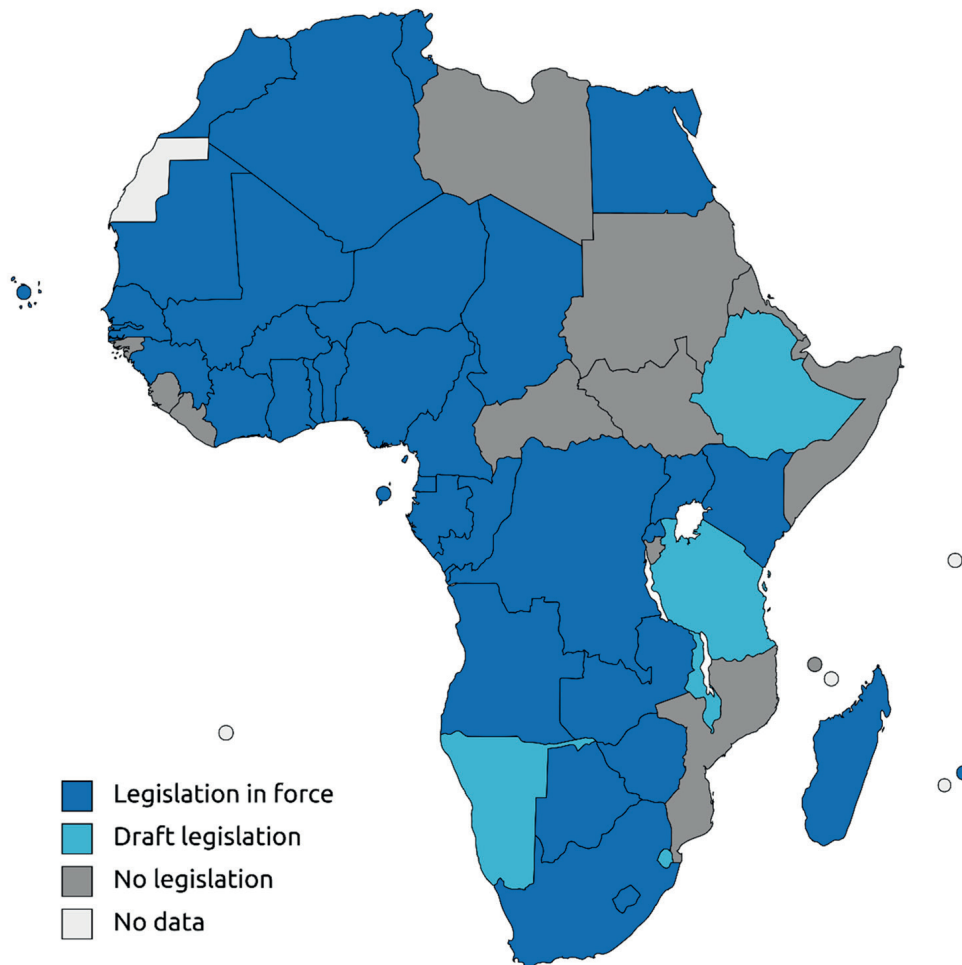
## 4. Data protection regulation in Africa

Africa currently has one of the lowest levels of digital integration in the world. A major reason for this is regulatory divergence between countries, particularly with respect to privacy and data protection regulations, which has resulted in limitations on cross-border data flows and digital trade more generally. Seventy-one (71) per cent of African countries have adopted privacy and data protection frameworks,<sup>9</sup> roughly half of which impose localisation requirements (Kugler, 2022). However, many of these regulatory frameworks are not yet in force or

8 Within Africa, Nigeria is the only country that imposes localisation requirements with this policy objective, though South Africa has signalled a similar regulatory intention with the release of its Draft National Data and Cloud Policy.

9 UNCTAD, 'Global Cyberlaw Tracker'. See: <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/global-cyberlaw-tracker>

Figure 6. Map of data protection and privacy legislation in Africa



Source: Commonwealth Secretariat using mapchart.net (Data from UNCTAD Cyberlaw Tracker, DLA Piper Data Protection Laws of the World, and ALT Data Protection Africa).

are woefully ineffective as they lack enforcement by a dedicated data protection authority (Banga et al., 2021). These regulations usually impose conditional localisation requirements that render the cross-border flow of personal data contingent upon the level of protection offered by the destination country. This indirectly discourages firms from attempting to expand into other African markets that lack the requisite level of personal data protection, as doing so may require the replication of data processing and storage infrastructure within countries with incompatible frameworks. This points to the need for harmonisation between conflicting regulations, something that several regional frameworks have looked to resolve.

#### 4.1 Regional data protection regulatory frameworks

At a continental level, the African Union Convention on Cyber Security and Personal Data Protection (referred to as the 'Malabo Convention') is the sole binding regulatory framework pertaining to cross-border data flows. Meanwhile, three African regional economic communities (RECs) have implemented frameworks that aim to harmonise data protection regulations and contain provisions on cross-border data flows (see Box 2).

In 2014, the African Union (AU) adopted the Malabo Convention, which aims to harmonise the personal data protection and cybersecurity laws of AU member states. The Malabo Convention includes a binding requirement that parties establish legal frameworks that protect personal data, punish violations of privacy and adhere to the principle of the

## Box 2. Data protection within regional economic communities

The East African Community (EAC), the Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC) have each developed regional data protection frameworks. These include the EAC Legal Framework for Cyberlaws (LFC), the ECOWAS Supplementary Act on Personal Data Protection (SAPDP) and the SADC Data Protection Model Law (DPML).

In 2009, the EAC adopted the LFC, making it the first REC to adopt a harmonisation framework that related to data issues. By contemporary standards its provisions are relatively primitive, with few modern implications for cross-border data flows. However, in 2010, a more comprehensive framework was adopted by ECOWAS: the SAPDP. This remains the only binding regional data protection act that is currently in force in Africa. It is largely identical to the Malabo Convention, having formed the basis of the latter.

Finally, SADC released the DPML in 2013. The DPML is a result of a long-term joint EU–ITU project that aimed to create a set of data protection and cybersecurity model laws for African RECs (the Economic Community of Central African States and the Economic and Monetary Community of Central Africa both adopted the same model law). First, it states that personal data may be freely transferred between those SADC member states that have transposed the DPML into domestic law. Second, it states that the transfer of personal data to non-SADC countries or to SADC members that have not transposed the DPML requires a prior finding of adequacy (a conditional localisation requirement) by the domestic data protection authority, and further clarifies the criteria that the data protection authority should examine when making this finding. Last, it states that transfers may still be made to countries that are judged to not provide an adequate level of protection if the user provides their consent.

free flow of personal data.<sup>10</sup> With respect to data localisation requirements, the Malabo Convention states that the collection and processing of personal data is prohibited, unless the user consents.<sup>11</sup> However, once consent has been granted, personal data is subject to conditional localisation measures that state that personal data may not be transferred to a *non-member state of the AU* unless the destination country provides an adequate level of personal data protection, or if the relevant national data protection authority of a member state authorises the cross-border transfer of personal data.<sup>12</sup> However, and somewhat surprisingly, the Malabo Convention does not clarify what criteria should be used when making adequacy assessments, nor how these localisation requirements apply to the transfer of personal data between AU member states (Greenleaf and Cottier, 2020). This ambiguity may render the cross-border transfer of personal data between AU members more difficult than the same transfer to a foreign non-AU member, defeating the original purpose of the convention. This perhaps underlies the fact that, since 2014, only 13 African countries have deposited their ratification notifications and thus the agreement has not secured the 15 ratifications required for its entry into force.

## 5. Cross-border data flows in the World Trade Organization and regional trade agreements

Currently, the World Trade Organization (WTO) does not have any agreements or rules that directly address the issue of cross-border data flows. Instead, existing 'technologically neutral' agreements regulate cross-border data flows indirectly by treating them as a medium through which goods and services may be traded. For example, the General Agreement on Trade in Services (GATS) will regulate cross-border data flows when they are used as the medium to purchase or provide a digital service in another country. However, this regulation varies depending on the commitments made by members within their individual services schedules. These rely on a sectoral taxonomy that was created in 1991, which makes it conceptually challenging to regulate digital services and data flows through a pre-internet services schedule. An additional complicating factor in this indirect form of regulation is the blurring of traditional goods/services silos due to digitalisation. This is leading to the provision of 'embedded' services within goods,

10 Malabo Convention, Article 8.

11 Malabo Convention, Article 14.1.

12 Malabo Convention, Article 14.6.



with the value of these goods largely dependent on the embedded service (e.g., the applications in smartphones) (Meltzer, 2015; Wu, 2017).

As a result of this legal uncertainty and ad hoc applicability, both scholars and WTO members consider the established WTO agreements as providing an insufficient global regulatory framework for cross-border data flows. Several governments have sought to expand the mandate of the E-Commerce Work Programme to include cross-border data flows, but have so far been unsuccessful.

At the 2017 Buenos Aires Ministerial Conference, some WTO members, led by Japan, Australia and Singapore, issued the Joint Statement on Electronic Commerce. The statement outlined their intentions to 'initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce', and led to the creation of the Joint Statement Initiative on Electronic Commerce ('the JSI') in 2019. At the time of writing, 88 members were participating in the ongoing JSI negotiations, which aim to create binding rules for participating states on a wide range of digital issues – including cross-border data flows, data localisation, privacy and personal data protection, and cybersecurity. To date, only seven African

countries are participating, four of which are members of the Commonwealth.<sup>13</sup>

As discussions on cross-border data flows have largely stalled within the WTO, many countries have instead turned to RTAs to further their digital trade interests. Since 2015, preferential trade agreements (PTAs) and RTAs have increasingly included 'e-commerce' or 'digital trade' chapters that contain binding provisions addressing issues relating to cross-border data flows. Eighty-two (82) countries (none of which are African) are involved in 99 different agreements that include such provisions (Elsig and Klotz, 2021). However, the cross-border data flow provisions in the RTAs outlined in Table 2 are of particular relevance for AfCFTA negotiators.

## 6. Way forward

The developmental potential of Africa's digital economy is immense, offering great scope to create jobs, stimulate economic growth, and enhance social and political inclusion. Growing e-commerce adoption and digital services exports are encouraging and point towards the importance of cross-border data flows in harnessing this potential, as well as ensuring African competitiveness in the development of new disruptive technologies.

**Table 2. Comparison of data flow-related provisions in selected RTAs**

	Cross-border data flows			Data protection	
	Liberalisation of data flows	Prohibition of localisation	Scope of exemptions	Minimal standards	Harmonisation
<b>CPTPP</b>	Binding	Binding	Narrow, with criteria	Binding, no criteria	Non-binding
<b>CUSMA</b>	Binding	Binding	Narrow, with criteria	Binding, with criteria	Non-binding, reference to international frameworks
<b>DEPA</b>	Binding	Binding	Narrow, with criteria	Binding, with criteria	Binding, reference to international frameworks
<b>RCEP</b>	Binding, with special and differential treatment	Binding, with special and differential treatment	Very broad, no criteria	Binding, no criteria	Binding <sup>14</sup>

Note: CPTPP = Comprehensive and Progressive Agreement for Trans-Pacific Partnership; CUSMA = Canada–United States–Mexico Agreement; DEPA = Digital Economy Partnership Agreement; RCEP = Regional Comprehensive Economic Partnership.

<sup>13</sup> Benin, Burkina Faso, Côte d'Ivoire, and Commonwealth members Cameroon, Kenya, Mauritius and Nigeria.

<sup>14</sup> Although the provision is binding, co-operation is only required 'to the extent possible' (Art. 12.8.5). This provides an easy opt-out from these obligations.

They are also important in tackling Africa's persistent digital divide, which threatens to impede the 67.2 per cent of offline Africans from participating in the digital economy. To bridge this gap, there is a need for rapid ICT infrastructure development and investment, as envisioned by SDG targets 9.b and 9.c. This becomes more viable when digital integration offers increasing returns through economies of scale and lower transaction costs.

As such, the AfCFTA Digital Trade Protocol is of great significance. Negotiators have an important task in finding the correct balance between regulatory freedom for states at different levels of development, while still encouraging cross-border data flows between them. As such, flexibility must be a cross-cutting attribute of the Digital Trade Protocol: as the largest RTA in the world by number of members, the AfCFTA cannot impose a 'one size fits all' approach that does not accommodate the varied levels of development and regulatory capabilities of different African countries. With this in mind, the following recommendations are offered, focusing on three key areas.

### 6.1 Defining concepts

In the context of the digital economy and given the multidimensional nature of data, it is particularly important that AfCFTA members have the same interpretation of provisions that relate to cross-border flows. Agreement on key definitions and concepts, as well as the relationship between them, is crucial for the interoperability of relevant domestic regulation, and ultimately to the success of the AfCFTA in growing Africa's digital economy. Comprehensive definitions must be provided for all relevant terms, including but not limited to 'data', 'personal data', 'data protection', 'digital trade', 'e-commerce' and 'cross-border data flows'. Doing so would ensure that members implement conceptually compatible domestic regulations, giving private actors certainty when operating across multiple jurisdictions and consumers greater trust in the efficacy of privacy and data protection regulations.

### 6.2 Facilitating cross-border data flows

The AfCFTA needs to find the right balance between enhancing digital integration and allowing members to address the distributional impacts of digitalisation and the digital divide. Here, it may be instructive for AfCFTA negotiators to examine how other trade agreements have sought to do the same thing. The CPTPP, CUSMA, DEPA and RCEP all prohibit the imposition of localisation require-

ments by default, but vary greatly according to the ease with which a measure may be exempt. On one side of the spectrum, the CPTPP, CUSMA and DEPA all adopt strict exceptions clauses similar to those found in the General Agreement on Tariffs and Trade (GATT) Article XX and GATS Article XIV. These allow members to impose localisation measures 'to achieve a legitimate public policy objective', which are implicitly those pertaining to data protection and security. On the other side of the spectrum, RCEP's exceptions clause allows member states to impose localisation requirements at their discretion. This has led some analysts to claim that RCEP is 'meaningless' regarding the liberalisation of cross-border data flows (Leblond, 2020).

Within the AfCFTA Digital Trade Protocol, relevant provisions could look to liberalise cross-border data flows, but with an exceptions clause that sits in the middle of the spectrum identified earlier. Localisation measures in the name of national security and cybersecurity and privacy and data protection may be exempt, as may be those measures that explicitly look to tackle domestic digital divides (Beyleveld and Sucker, 2022). Negotiators may also wish to take inspiration from RCEP, which includes several footnotes that provide for the timebound exemption of capacity-constrained LDCs and non-compliant member states from specific provisions. The inclusion of similar provisions in the AfCFTA for capacity-constrained African states may be prudent in finding this balance and securing political buy-in. This may be negotiated on a case-by-case basis, or by defining certain criteria (such as LDC status) that warrant exemption from a specific provision.

### 6.3 Harmonising data protection regulations

For the AfCFTA to promote intra-African cross-border data flows, it needs to address regulatory conflict between domestic data protection frameworks and across regional frameworks. Other RTAs have addressed this problem by including binding provisions that oblige their members to adopt domestic privacy laws and mandate their members to work towards harmonisation. These are initial solutions that the AfCFTA could emulate.

However, it is not sufficient to mandate the adoption of such frameworks by African countries without ensuring that they adhere to a set of minimum standards. This may be done in two ways. The first is to stipulate common principles that should inform each respective law, as done by CUSMA and DEPA. The second, and more ambitious option, is to

explicitly refer to the Malabo Convention as a best international standard that should be used when adopting domestic privacy laws and to encourage its ratification. This would mirror CUSMA's referral to the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Doing so could also allow the AfCFTA to address the deficiencies of the Malabo Convention, identified in Section 4.1, by specifying those criteria that should be used to make adequacy assessments between member states. However, adequacy assessments are usually an arduous and lengthy process and may be especially onerous for under-resourced African data protection authorities. So, another solution is for the AfCFTA to draw on SADC's DPML and include a provision that allows for the free transfer of personal data between those AfCFTA members that have ratified the Malabo Convention and encoded it into domestic law.<sup>15</sup>

Regardless of which approach is taken, the AfCFTA will need to accommodate the different capacities of members in adhering to these minimum standards, especially considering that many African countries do not have any domestic privacy laws. Therefore, and similarly to above, a time-bound exemption for non-compliant and capacity-constrained countries could be provided.

15 There is precedence for such an approach in Africa: Article 42 of Kenya's Data Protection Act states that any country that has ratified the Malabo Convention is assumed to have appropriate safeguards in place, and thus personal data may be freely transferred from Kenya to that country.

## 7. Appendix: Select ICT indicators for African countries (2021)

	% Population using the internet	% Covered by 3G network	% Covered by 4G/LTE network	Cost of 2GB mobile data (% of GNI per capita)
Algeria	70.8	98.2	79.9	0.9
Angola	32.6	87.2	33.0	3.6
Benin	34.0	80.0	46.0	6.5
Botswana	73.5	98.0	88.0	1.2
Burkina Faso	21.6	53.2	36.6	10.5
Burundi	5.8	50.6	32.2	13.7
Cabo Verde	69.8	93.8	80.0	3.3
Cameroon	45.6	25.8	13.5	4.0
Central African Rep.	10.6	47.6	0.3	41.0
Chad	17.9	59.0	22.0	24.1
Comoros	27.3	87.0	85.0	7.9
Congo (Rep. of the)	-	87.0	85.0	12.4
Côte d'Ivoire	45.4	96.4	64.5	2.6
Dem. Rep. of the Congo	22.9	55.0	40.0	10.9
Djibouti	68.9	90.0	90.0	6.1
Egypt	72.1	99.5	98.0	1.1
Equatorial Guinea	53.9	60.0	-	23.5
Eritrea	21.7	35.0	-	-
Eswatini	58.9	99.1	80.4	4.1
Ethiopia	16.7	85.0	10.0	5.3
Gabon	71.7	98.0	98.0	2.2
Gambia, The	33.0	88.0	7.5	12.2
Ghana	68.2	95.8	67.7	2.3
Guinea	34.7	40.0	29.0	5.7
Guinea-Bissau	35.2	43.0	23.0	8.5
Kenya	28.8	95.0	94.0	3.1
Lesotho	48.0	95.8	85.1	7.4
Liberia	33.6	63.0	35.0	18.1
Libya	-	98.0	40.0	3.6
Madagascar	19.7	67.1	27.1	13.2
Malawi	24.4	84.4	68.6	10.4
Mali	34.5	68.0	47.0	10.1
Mauritania	58.8	43.7	-	3.8
Mauritius	67.6	99.0	99.0	0.9
Morocco	88.1	99.3	99.1	1.3
Mozambique	17.4	85.0	50.0	11.9
Namibia	53.0	89.0	79.0	2.6
Niger	22.4	24.0	-	15.3

	% Population using the internet	% Covered by 3G network	% Covered by 4G/LTE network	Cost of 2GB mobile data (% of GNI per capita)
Nigeria	55.4	84.6	61.9	2.0
Rwanda	30.5	98.6	98.1	6.5
São Tomé and Príncipe	51.2	94.0	-	5.7
Senegal	58.1	99.4	83.1	2.9
Seychelles	81.6	99.0	98.5	2.5
Sierra Leone	-	79.9	48.6	14.4
Somalia	-	70.0	30.0	7.7
South Africa	72.3	99.9	97.9	2.3
South Sudan	-	15.0	15.0	-
Sudan	-	78.6	35.0	3.4
Tanzania	31.6	85.0	13.0	4.9
Togo	35.0	97.0	83.0	11.4
Tunisia	79.0	99.0	95.0	1.2
Uganda	10.3	85.0	31.0	8.0
Zambia	21.2	95.5	91.2	6.4
Zimbabwe	34.8	84.3	39.1	29.6

Source: Commonwealth Secretariat (using data from ITU)

## 8. References

A4AI (2021) *A4AI Mobile Broadband Pricing - GNICM 2021*. Available at: [https://adi.a4ai.org/extra/baskets/A4AI/2021/mobile\\_broadband\\_pricing\\_gni.php#](https://adi.a4ai.org/extra/baskets/A4AI/2021/mobile_broadband_pricing_gni.php#).

Aaronson, S. (2015) 'Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security', *World Trade Review*, 14(4), pp. 671–700.

AfricanUnionandOECD(2022)*Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs*. Available at: <https://www.oecd-ilibrary.org/deliver/0a5c9314-en.pdf?itemId=%2Fcontent%2Fpublication%2F0a5c9314-en&mimeType=pdf>.

Aguerre, C. (2018) 'Digital trade in Latin America: mapping issues and approaches', *Digital policy, regulation and governance* [Preprint].

AU, AfDB and UNECA (2017) 'Assessing Regional Integration in Africa VIII'. Available at: <https://uneca.org/assessing-regional-integration-africa-viii>.

Banga, K., Macleod, J. and Mendez-Parra, M. (2021) 'Digital trade provisions in the AfCFTA: What can

we learn from South–South trade agreements?' Available at: <https://set.odi.org/wp-content/uploads/2021/04/Digital-trade-provisions-in-the-AfCFTA.pdf>.

Bauer, M. et al. (2014) *The costs of data localisation: Friendly fire on economic recovery*. ECIPE Occasional Paper.

Beyleveld, A. and Sucker, F. (2022) *Cross-border data flows in Africa: Policy considerations for the AfCFTA Protocol on Digital Trade*. Available at: <https://doi.org/10.13140/RG.2.2.17512.34562>.

Chivunga, M. and Tempest, A. (2021) 'Digital Disruption in Africa: Mapping Innovations for the AfCFTA in Post-COVID Times', *Occasional Paper*, 317. Available at: <https://www.africaportal.org/documents/22228/Occasional-Paper-317-chivunga-tempest.pdf>.

Cory, N. and Dascoli, L. (2021) *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. Information Technology and Innovation Foundation. Available at: <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>.

Elsig, M. and Klotz, S. (2021) *Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion*. Cambridge University Press.

Fajarnes, P., Samarajiva, R. and Adeniran, A. (2022) 'Creating a Level Playing Field for Digital Trade'. *ECommerce Week*, UNCTAD, Geneva, 25 April. Available at: <https://unctadeweek2022.pathable.co/meetings/virtual/GEeaNturgfvJLh9i>.

Ferracane, M. and Marel, E. van der (2019) 'Do data policy restrictions inhibit trade in services?', *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS*, 29.

Ferracane, M.F. and van der Marel, E. (2020) 'The costs of data protectionism', *Big data and global trade law*. Cambridge University Press, Cambridge [Preprint].

Greenleaf, G. and Cottier, B. (2020) 'Comparing African data privacy laws: International, African and regional commitments', *University of New South Wales Law Research Series* [Preprint].

IFC and Google (2020) *e-Conomy Africa 2020*. Available at: <https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2>.

Kugler, K. (2022) 'The Impact of Data Localization Laws on Trade in Africa'. Available at: <https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf>.

Leblond, P. (2020) *Digital Trade: Is RCEP the WTO's Future?*, Centre for International Governance Innovation. Available at: <https://www.cigionline>.

[org/articles/digital-trade-rcep-wtos-future/](https://www.wto.org/articles/digital-trade-rcep-wtos-future/) (Accessed: 12 June 2022).

Lemma, A., Mendez-Parra, M. and Naliaka, L. (2022) *The AfCFTA: unlocking the potential of the digital economy in Africa*. London: ODI. Available at: [https://cdn.odi.org/media/documents/Digital\\_trade\\_report\\_AfCFTA\\_\\_\\_A7wsHot.pdf](https://cdn.odi.org/media/documents/Digital_trade_report_AfCFTA___A7wsHot.pdf).

Meltzer, J.P. (2015) 'The Internet, Cross-Border Data Flows and International Trade', *Asia & the Pacific Policy Studies*, 2(1): 90–102.

NFTC (2011) 'Promoting Cross-Border Data Flows: Priorities for the Business Community'. Available at: [www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf](http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf).

UNCTAD (2021) *Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow*. Geneva: UNCTAD.

World Bank (2023) *Digital Africa: Technological Transformation for Jobs*. Available at: <https://openknowledge.worldbank.org/bitstream/handle/10986/39491/9781464817373.pdf>.

World Economic Forum (2020) 'Accelerating Digital Inclusion in the New Normal'. World Economic Forum. Available at: [http://www3.weforum.org/docs/WEF\\_Accelerating\\_Digital\\_Inclusion\\_in\\_the\\_New\\_Normal\\_Report\\_2020.pdf](http://www3.weforum.org/docs/WEF_Accelerating_Digital_Inclusion_in_the_New_Normal_Report_2020.pdf).

Wu, M. (2017) 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System'. Available at: [e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final.pdf](http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final.pdf).

Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.

# International Trade Policy Section at the Commonwealth Secretariat

This *Trade Hot Topic* is brought out by the International Trade Policy (ITP) Section of the Trade Division of the Commonwealth Secretariat, which is the main intergovernmental agency of the Commonwealth – an association of 56 independent countries, comprising large and small, developed and developing, landlocked and island economies – facilitating consultation and co-operation among member governments and countries in the common interest of their peoples and in the promotion of international consensus-building.

ITP is entrusted with the responsibilities of undertaking policy-oriented research and advocacy on trade and development issues and providing informed inputs into the related discourses involving Commonwealth members. The ITP approach is to scan the trade and development landscape for areas where orthodox approaches are ineffective or where there are public policy failures or gaps, and to seek heterodox approaches to address those. Its work plan is flexible to enable quick response to emerging issues in the international trading environment that impact particularly on highly vulnerable Commonwealth constituencies – least developed countries (LDCs), small states and sub-Saharan Africa.

## Scope of ITP Work

ITP undertakes activities principally in three broad areas:

- It supports Commonwealth developing members in their negotiation of multilateral and regional trade agreements that promote development friendly outcomes, notably their economic growth through expanded trade.
- It conducts policy research, consultations and advocacy to increase understanding of the changing international trading environment and of policy options for successful adaptation.
- It contributes to the processes involving the multilateral and bilateral trade regimes that advance more beneficial participation of Commonwealth developing country members, particularly, small states and LDCs and sub-Saharan Africa.

## ITP Recent Activities

ITP's most recent activities focus on assisting member countries in their negotiations in the World Trade Organization and various regional trading arrangements, undertaking analytical research on a range of trade policy, emerging trade-related development issues, and supporting workshops/dialogues for facilitating exchange of ideas, disseminating informed inputs, and consensus-building on issues of interest to Commonwealth members.

## Selected Recent Meetings/Workshops Supported by ITP

21 March 2023: Public event on Assessing the Business and Trade Dimensions of the 2022 Birmingham Commonwealth Games, in partnership with the UK's Department for Business and Trade. The event reflected on the legacy of the Commonwealth Games and explored how businesses can capitalise on the trade and investment relationships established during the Games.

16 November 2022: Public event on Enabling Climate Smart Trade and Investment: From Policies to Actions, organised for the ICC's Make Climate Action Everyone's Business Forum. The event examined how trade and trade policies can support climate action and how countries can integrate environmental and social considerations into trade agreements to achieve the SDGs.

2 November 2022: Public event on Maximising the Gains from Digital Trade: Solutions and Priorities for Developing Countries and LDCs, organised jointly with the Enhanced Integrated Framework (EIF) and hosted at the WTO in Geneva. The event reflected on lessons from country experiences and EIF projects, explored the concept of Aid for Digital Trade and identified innovative new ways to support LDCs, and particularly their MSMEs, to build capacity for digital trade.

31 October 2022: Joint Commonwealth Secretariat-UNCTAD workshop on Understanding the IPR-related Landscape for Graduating LDCs: Issues and Challenges. The workshop, hosted at the United Nations in Geneva, was attended by technical experts from the Centre for Policy Dialogue, United Nations Committee for Development Policy, ODI, South Centre, UNCTAD, WIPO and WTO, who discussed issues, challenges and opportunities related to intellectual property rights for graduating LDCs.

## Previous Ten Issues of the Commonwealth Trade Hot Topics Series

Issue 187: Enhancing Intra-Commonwealth Trade and Investment: An International Business Research Agenda

Issue 186: Beyond Trade and GDP: Exploring the Wealth of the Commonwealth

Issue 185: Deepening Intra-Commonwealth Trade and Investment between the UK and Africa

Issue 184: Realising the Trade Ambitions of the Doha Programme of Action for LDCs: A Commonwealth Perspective

Issue 183: Embedding Development in WTO Plurilateralism: A Commonwealth Developing Country Perspective

Issue 182: The Russia-Ukraine Conflict: Implications for Food Security in the Commonwealth

Issue 181: Beyond the Pandemic: Commonwealth Trade and Investment Prospects

Issue 180: Capacity-Building in Digital Economy Agreements – the Missing Link?

Issue 179: Towards a Commonwealth 10-point programme of action for LDCs

Issue 178: The EU's Carbon Border Adjustment Mechanism: Implications for Commonwealth Countries



# Trade Hot Topics

ISSN: 2071-8527 (print) ISSN: 2071-9914 (online)

Commonwealth Trade Hot Topics is a peer-reviewed publication which provides concise and informative analyses on trade and related issues, prepared both by Commonwealth Secretariat and international experts.

Series editor: Brendan Vickers

Produced by the Trade, Oceans and Natural Resources Directorate of the Commonwealth Secretariat

For further information or to contribute to the Series, please email [b.vickers@commonwealth.int](mailto:b.vickers@commonwealth.int)