THE IMPACT OF DATA PROTECTION RULES ON THE DIGITAL ECONOMY ASPECT OF THE AFRICAN CONTINENTAL FREE TRADE AGREEMENT (AfCFTA)

Solagbade Sogbetun

Ibrahim Moshood

ALP NG & CO.
AFRICA LAW PRACTICE NG & COMPANY
WWW.ALP.COMPANY

THE IMPACT OF DATA PROTECTION RULES ON THE DIGITAL ECONOMY ASPECT OF THE AFRICAN CONTINENTAL FREE TRADE AGREEMENT (AfCFTA)

BACKGROUND

The AfCFTA ("the Agreement") is a regional agreement to enhance industrialization in Africa. It covers a market of 1.2 billion people and a gross domestic product of USD 2.5 Trillion across all 55 member states. AfCFTA is the world's largest free trade area since the formation of the World Trade Organization (WTO).[1] The agreement is to be implemented in phases and some of the phases are still under negotiation. Generally, these phases include but are not limited to intellectual property, competition, schedule of tariff concessions, dispute resolution and investment.

Since the population of Africa is expected to reach 2.5 billion by 2050, and about 26% of the world's working population. It has also been estimated that AfCFTA will boost intra African trade by 52.3 % by 2020.[2]

The objectives of the AfCFTA are:

- Consolidation of the region into one trade area.
- Removal of tariffs on 90% of goods and services exported within Africa.
- Fostering economic integration of the continent.
- Production of more jobs for African youths.
- Driving industrialization of Africa.

The gravamen of the AfCFTA is to improve international economic relations and cross-border trading. The Agreement also covers the free flow of tangible and intangible goods and services both of which thrive on the collection and use of data. Unfortunately, many member states do not have adequate data protection regimes to help govern and control how data flows, its security and usage in the region. The Agreement fails to address these gaps.

This article examines the relevance of data privacy rules to international trade/ digital economy considering the recent implementation of AFCFTA, and the strides the Agreement must cover to create space for a robust digital economy aspect of regional and international trade.

---

[1] The United Nations Economic Commission for Africa (UNECA) January 2020 AfCFTA Q&A.

[2] https://www.globalafricanetwork.com/2020/02/13/company-news/the-african-continental-free-trade-area-whowill-benefit/

DATA PROTECTION IN THE AFCFTA

McKinsey in its report on Africa business growth, noted that Africa has over 400 Million internet users in Nigeria[3], the second largest behind China. The implication of this is that there are a vast amount of e-commercial activities occurring in the continent. For every trade possibility AfCFTA brings, there are lot of considerations to be given to what would happen to the data submitted by customers to international trading counterparts. If A in Lagos decides to pay his tuition to a university in Cape Town through a financial technology company based in Durban, what is purely a financial service would involve the dissemination of personal and financial information required to conclude the transaction.

In the first quarter of 2017, **Forbes** had predicted that the data market will surpass USD 200 billion by the end of 2020[4]. This imputes that data flows cannot be removed from the economy especially the digital economy as it relates to communications and financial services. For instance, Nigeria's recent adoption of Organization for Economic Co-operation and Development (OECD) "Significant Economic Presence" rule in its Finance Act 2020 is heavily based on data. It expands the tax net to cover multinationals using its citizens' data.

It is germane to consider that no country wants to give another country unfettered/unregulated access to its data. Invariably, data issues have become a matter of disputes for sovereign states. Although, AfCFTA has made such free flow of services and information possible, what has it done to protect that information? For member states to benefit fully from the digital economy aspect of international trade, they must recognize the fact that data is power and create effective regimes for data protection.

[3] https://www.mckinsey.com/featured-insights/middle-east-and-africa/how-ecommerce-supports-african-businessgrowth
[4] https://www.forbes.com/sites/gilpress/2017/01/20/6-predictions-for-the-203-billion-big-data-analyticsmarket/#6ac966642083

The African reality and challenges

United Nations Conference on Trade and Development (UNCTAD) on the importance of data protection in 2016 noted that:

> *"Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative market effects by reducing consumer confidence."*

For an agreement contemplating so much international data flows, data protection should be core considerations of the agreement. However, by virtue of the reality of the African business environment, which is harsh and myopic on various fronts. In the case of Africa, our realities are our challenges. For instance, there are no common enforceable data protection laws or regulations applicable across Africa. Specifically, countries like Ethiopia, Guinea- Bissau, Sudan, Mozambique, Botswana, Congo, Djibouti, Liberia and some other African member-states to this agreement have no data protection laws.[5] This leaves data exchanged between countries open to misuse, hacks and threats.

AfCFTA Efforts

The two major efforts made by Africa in a creating a regional data protection regime are the African Union Convention on Cyber Security and Personal Data and Article 15 of the AFCFTA.

i. AfCFTA Protocol on Trade in Services

This was modelled on the World Trade Organization's (WTO) General Agreement on Trade in Services (GATS). Article 15(C) ii of Protocol on Trade in Services provides that:

> *"privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and account"*

[5] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Compared to the data protection regimes contained in the free trade agreements of other regions, this provision simply does not do enough for data protection. It merely allows state parties to adopt measures necessary to comply with their national data laws.

The provision is restraint on trade operating to exempt about member-states from the many benefits of the AfCFTA. This is because, over 23 out of 54 [6] countries in Africa do not have data protection laws. The above provision in effect restrains trading with the other 23 countries without data protection laws. In the same vein, it would be unfair to have the rest of the region wait for

---

the other countries to implement data protection laws before the Agreement can take full effect. It appears more reasonable for the Agreement to incorporate data protection provisions to be complied with by all member states ratifying the Agreement. Essentially, the function and focus of Article 15 should be extended to cover for situations where member states without data privacy laws can still receive data from another member state subject to robust provisions of the AfCFTA on data protection.

Moreover, Article 15 appears to be a mere proliferation of the provisions of most countries' data protection laws. For instance, in Nigeria, the Nigeria Data Protection Regulation (NDPR)[7] already provides that National Information Technology Development Agency (NITDA) would not permit international data flows where the affected country has no adequate data protection regime.

ii. The African Union Convention on Cyber Security and Personal Data Protection (*The Malabo Convention*) 2014.

This convention is a comprehensive document covering electronic transactions, privacy and cybersecurity. Unfortunately, till date, the Malabo Convention has been signed by only 14 states and ratified by five countries out of 55 member states. This further emphasizes the fact that the data protection needs of the AfCFTA must be enshrined in the Agreement or annexed with it, to function effectively.

How does this affect Africa?

---

[6] https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-championsdigital-privacy/

[7] Section 2.11 of the Nigeria Data Protection Regulation 2019

The whole world is becoming more integrated with the advent of digital economy in international trade. Without a robust data privacy regime, Africa stands to lose billions in revenue and jobs as external entities that ought to set up businesses in Africa would rather just set up shop in a region with more developed data protection laws.

Recommendations

Globally, regional international trade agreements have annexures and other types of subsidiary regulation on data protection. For example, in Europe there is the Annexure XI to the European Free Trade Agreement (EFTA)[8] which has been ratified by many countries that are signatories to the agreement. This annexure covers data protection in relation to electronic communication, audiovisual services and information services within European member states.

Like other free trade agreements, the AfCFTA must consider incorporating specific data protection provisions to maintain international best practices in data protection. Doing this would ensure that:

i. Africa remains competitive in international trade as this would increase the confidence of member states and external trade partners.
ii. Safe conduct is maintained during transactions involving personal data exchange.
iii. There are clear-cut data protection standards, ensuring that data flows within control and alongside rights. Whilst also maintaining confidence between states with data protection laws and those without. Ultimately, this allows for true inclusiveness by allowing all African countries take full benefits of AfCFTA.

[8] https://www.efta.int/legal-texts/eea/annexes-to-the-agreement

Authors

Solagbade Sogbetun
Senior Associate
ssogbetun@alp.company