International Economic Law Clinic

LIBERALISING CROSS-BORDER DATA FLOWS IN AFRICA TO UNLOCK THE CONTINENT'S DIGITAL ECONOMY - AN ANALYSIS OF DATA FLOW RESTRICTIONS IN THE EAC AND ECOWAS ECONOMIC COMMUNITIES.

07/11/2022

Submitted by:

Gladys Anne Nyangweso

Jude Oundo

Mitchelle Oriedo

James Kanjeru

Raphael Gitau

Sumaya Hussein

Bernadette Mulyungi

Natasha Oduor

To : Mandela Institute of the University of Witwatersrand

Dr. Alexander Beyleveld

Ms Kholofelo Kugler

TradeLab

International rules on cross-border trade and investment are increasingly complex. There is the WTO, World Bank and UNCTAD, but also hundreds of bilateral investment treaties (BITs) and free trade arrangements ranging from GSP, EU EPAs and COMESA to ASEAN, CAFTA and TPP. Each has its own negotiation, implementation and dispute settlement system. Everyone is affected but few have the time and resources to fully engage. TradeLab aims to empower countries and smaller stakeholders to reap the full development benefits of global trade and investment rules. Through pro bono legal clinics and practica, TradeLab connects students and experienced legal professionals to public officials especially in developing countries, small and medium-sized enterprises and civil society to build lasting legal capacity. Through 'learning by doing' we want to train and promote the next generation of trade and investment lawyers. By providing information and support on negotiations, compliance and litigation, we strive to make WTO, preferential trade and bilateral investment treaties work for everyone.

More at: https://www.tradelab.org

What are Legal Practica

Legal practica are composed of small groups of highly qualified and carefully selected students. Faculty and other professionals with longstanding experience in the field act as Academic Supervisors and Mentors for the Practica and closely supervise the work. Practica are win-win for all involved: beneficiaries get expert work done for free and build capacity; students learn by doing, obtain academic credits and expand their network; faculty and expert mentors share their knowledge on cutting-edge issues and are able to attract or hire top students with proven skills. Practicum projects are selected on the basis of need, available resources and practical relevance. Two to four students are assigned to each project. Students are teamed up with expert mentors from law firms or other organizations and carefully prepped and supervised by Academic Supervisors and Teaching Assistants. Students benefit from skills and expert sessions, do detailed legal research and work on several drafts shared with supervisors, mentors and the beneficiary for comments and feedback. The Practicum culminates in a polished legal memorandum, brief, draft law or treaty text or other output tailored to the project's needs. Practica deliver in three to four months. Work and output can be public or fully confidential, for example, when preparing legislative or treaty proposals or briefs in actual disputes.

Kenyatta University

Kenyatta University, located in Nairobi, Kenya, runs an interdisciplinary clinic, in partnership with Strathmore University. Kenyatta University is the first TradeLab clinic to be run jointly by two different departments - School of Law and School of Economics - with law and economics students collaborating on all projects. Kenyatta School of Law delivers innovative legal education which is student-focused and research-led. It embraces an integrated philosophy of teaching, research and community service. Strathmore University holds a peerless reputation for quality in academic and professional education, as well as personal formation.[1]

CONTENTS

[1] It is with great pleasure that we would like to express our gratitude to our coordinators Professor Tomasz Milej, Mrs. Caroline Kago, and Mrs. Beatrice Ngunyi. We are also grateful to our mentors Professor Alex Boniface Mukulilo and Professor Amaka Vanni for their guidance. We thank them for organizing workshops that gave us the necessary skills and for their support. We truly wouldn't have done this without them.

EXECUTIVE SUMMARY

Cross-border data flows have become an integral aspect of globalisation in the 21st century. Almost every type of cross-border transaction has a digital component the global economy has become increasingly data dependent. However, cross-border data flows are not consistently orderly and safe. They may pose serious challenges to national security interests, regulatory frameworks, and even law enforcement. Furthermore, as we become increasingly reliant on data for daily activities, new concerns arise including privacy and economic development.

Accordingly, these concerns necessitate effective regulation for cross border data flows. As a result, governments have started updating and adapting data-related policies to the digital including restrictions on the cross-border flow of data. Reasons for introducing restrictions differ from country to country, but typically include one or more of the following justifications such as data privacy, protection, national sovereignty integrity, and security. Leading actors such as the European Union (EU), the United States of America and China have created regulatory regimes replicated across the globe.

African countries have also adopted differing approaches to cross-border data restrictions. This study will analyse the regulatory trends in the ECOWAS and EAC regional economic communities while drawing comparisons with the established models of the developed world. It will discuss the type of restrictions at the national level, the types of data regulated and their underlying rationale.

DEFINITION OF TERMS

Data Flow- movement of data across borders.

Data Storage- the recording and maintenance of data in a storage medium for accessibility once requested by users.

Data Transfer- the transmission or copying of electronic data/ information from one location to another.

Data localization/ residency- the collection, processing and storage of data within a country's borders.

Data Processing- the gathering and use of personal data by a processor

Data Subject- An individual/entity to whom data relates.

1.0 INTRODUCTION

The internet has revolutionized international trade by presenting a new platform for trade for various categories of traders ranging from states, international companies and firms and independent sellers.[2] This was especially evident at the onset of and during the covid-19 pandemic.[3] The United Nations Conference on Trade and Development (UNCTAD) reports that e-commerce firms such as Amazon, Alibaba, eBay among others reported an average of 10%-15% in profits for the year 2020 in trading online during the pandemic.[4] It has thus become an unspoken requirement for firms, industries and companies to establish an online presence. Traditional companies and industries have also had to result in e-commerce as well. These measures have proved beneficial to these companies. An online presence for these companies means a wider market access across borders.[5] Such development means that it is necessary to have data on the consumers in order to facilitate the trade. These companies rely on data in their businesses for a number of purposes: monitoring production systems, monitoring supply chains, understanding consumer preferences (their willingness to pay and reaction to new products) and to manage global workforces.[6] From the foregoing, it is evident that cross border data flows are important in the facilitation of international trade.

Some states have implemented strict laws and regulations to protect the data privacy of their citizens, a measure that has consequently impeded the growth of cross-border data flows. The measures are particularly strict in states in the ECOWAS and EAC regions. This is because, as the document will show, both regions are based on the EU approach and the Chinese approach, or a hybrid of the two. The EU approach allows the transfer of data to countries that have an adequate level of protection accorded to personal data and the data subject must consent to having their

[2] Assan Jallow, 'Why the Internet has resulted in more International Business and What Factors are Responsible for the Increase in the Volume in International Trade?' (13 October 2019)
[3] Nigel Cory and Luke Dascoli, ' How Barriers to Cross-Border Data Flows are spreading Globally, What they Cost, and How to Address them' (July 19 2021), Information Technology and Innovation Foundation < https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost > accessed 7 April 2022
[4] United Nations Conference on Trade and Development, 'Global e-Commerce Jumps to $26.7 Trillion, Covid-19 boosts Online Sales' (3 May 2021) < https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales > accessed 7 April 2022
[5] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (February 2013) Issues in Technology Innovation Number 22 < https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf > accessed 7 April 2022
[6] Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?' (1 May 2017) Information Technology and Innovation Foundation < https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost > accessed 7 April 2022.

data transferred cross-border.[7] The Chinese approach requires local storage within the state's servers and an assessment of the data that will be sent to the third-party state by a data authority .[8] Policy makers in both regions argue that these measures are meant to pursue legitimate objectives while others see it as a form of data protectionism limiting the market access for new companies within countries' jurisdictions.[9]

1.1 Cross Border Data Flow Restrictions

Cross-border data flows refer to the flow of data across borders with the aim of facilitating provision of cross-border communication, trade and services.[10] Cross-border restrictions, therefore, refer to regulatory measures pursuing certain objectives whose consequence is the hindrance of the free flow of data across state borders.[11] Companies are through these restrictions required to process data locally, assess data before transferring it, seek the approval of a relevant data authority before transferring data among other measures.[12] These measures present a barrier to international trade by slowing productivity of companies and increasing prices for affected industries and consumers.[13] They may be direct and explicit or indirect.[14]

1.2 Types of Data Flow Restrictions

1.2.1 Direct/Explicit Restrictions

a) Explicit Local Storage Requirements.

This type of restriction requires the company that intends to transfer data across borders to store a copy of the transferred data within the borders of the jurisdiction of the state imposing the law.

---

[7] Svetlana Yakovleva and Kristina Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade" International Data Privacy Law, 2020, Vol. 10, No. 3

[8] Jinhe Liu, 'China's Data Localization' (August, 2019) < https://www.researchgate.net/figure/Dynamic-system-of-Chinas-cross-border-data-flow-institutionalization-created-by-the_fig2_335290331 > accessed 11 June 2022

[9] *Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?'* (n 5)

[10] Francesca Casalini & Javier López González, 'Trade and Cross-Border Data Flows' (2019) OECD Trade Policy Papers No.220 OECD Publishing, Paris < http://dx.doi.org/10.1787/b2023a47-en > accessed 11 June 2022

[11] Martina F. Ferracane, 'Restrictions on Cross-Border data flows: a taxonomy' (2017) European Centre for International Political Economy ECIPE Working Paper -No.1 of 2017 < https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf > accessed 7 April 2022

[12] Francesca Casalini & Javier López González, 'Trade and Cross-Border Data Flows' (n.10)

[13] *Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?'* (n 4)

[14] *Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows are spreading Globally, what they Cost, and How to Address them'* (n 2)

These restrictions allow the receiving state to store and process data within their borders as long as a copy is left in the sending state.[15]

b) Explicit local Processing and Storage Requirements.

These types of restrictions require the company to process all data that is intended to be transferred within the jurisdiction of the sending state. The company will, therefore, be required to invest in local processing systems or the incorporating within their systems of local processing operators. The company may then transfer the data to the parent company after processing.[16]

c) Ban on Transfer of data.

This type of restriction completely bans the transfer of data to the receiving state. This restriction therefore requires the company to store, process and access data within the jurisdiction of the country imposing the restrictions. These types of bans are mostly sector specific for example, health, ICT and telecommunications and personal data.[17]

1.2.2 Indirect/ implicit restrictions.

a) Conditional Data Transfer

These restrictions may take the form of conditions that have to be fulfilled by the company before data is transferred. The state imposing the regulation may prescribe for certain authorization by the Data protection agency[18] or maybe the Attorney General.[19]Therefore, the transfer of data is subject to such authorization.

1.3. Objectives of Data Restrictions

1.3.1 Data Privacy or Cybersecurity

Policy makers place restrictive measures in place in a bid to protect the data of their subjects. Regulators believe that they are best placed to protect the data of their subjects within their

[15] *Martina F. Ferracane, 'Restrictions on Cross-Border data flows: a taxonomy'* (n 11)
[16] Ibid, pg.4
[17] An example is National Information Technology Development Agency's mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (2019)
[18] Article 6, Supplementary Act A/SA. 1/01/10 on Personal Data Protection Within ECOWAS
[19] Part 2.11, Nigeria Data Protection Regulation (2019)

jurisdiction.[20] Allowing the free flow of data outside their jurisdiction, according to regulators, is dangerous because the optimal level of security has not been achieved globally.[21] The security justifications are as follows: adequate cyber security builds consumer trust and free flow of data may lead to abuse or misuse of consumer data that would lead to loss of money if the data subject was involved in an online transaction or emotional and psychological harm.[22]

1.3.2 Law Enforcement and Regulatory Reasons.

Regulators enact restrictive measures to ensure that there is accountability from companies within their jurisdiction. The companies have to account for data within their possession and protect such data.[23] Regulators need to have the power and evidence to address data concerns that arise within their territories such as threat to national security when confidential information is leaked to third party states. This would ensure that local courts can adjudicate in case of any data breaches.[24] Examples of data breaches include the use, acquisition of, disclosure and accessing of data through illegal or unauthorized means.[25] Storing data locally or at least storing a copy of the data is a restriction put in place to avoid the challenges that come with retrieving data that has already been transferred to a foreign country.[26] An example can be sourced from the United States Case of: ***United States v Microsoft Corporation,***[27] the case concerned a warrant that had been issued by a United States District Court to Microsoft Corporation to disclose all emails and all other information of one of its clients suspected of engaging in illegal activities. The client's information was stored in Dublin, Ireland. Microsoft moved to Court to challenge the validity of the warrant. At appeal level, the court found that the arrest warrant would be an unauthorized extraterritorial

[20] Nigel Cory and Luke Dascoli, ' How Barriers to Cross-Border Data Flows are spreading Globally, What they Cost, and How to Address them' (July 19 2021), Information Technology and Innovation Foundation < https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost > accessed 7 April 2022

[21] Svetlana Yakovleva and Kristina Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade" (2020) International Data Privacy Law, Vol. 10, No. 3 pg. 207.

[22] Ibid, pg.207.

[23] Ibid

[24] Martín Molinuevo and Simon Gaillard, ' Trade, Cross-Border Data, and the Next Regulatory Frontier: Law enforcement and data localization requirements' (2018) World Bank Group Number 3 < https://documents1.worldbank.org/curated/en/903261543589829872/pdf/132606-BRI-PUBLIC-add-series-MTI-Practice-Note-3.pdf > accessed 8 April 2022; United States v Microsoft Corporation [2018] 584 U. S. ____ (2018)

[25] Global Investigations Review, 'Regulatory Compliance in the Context of a Cross-Border Data Breach' (8 June 2021)

[26] Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?' (1 May 2017) Information Technology and Innovation Foundation < https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost > accessed 7 April 2022.

[27] United States v Microsoft Corporation, 584 U.S 2018 [SC]

application and quashed the warrant. This encouraged the creation of the Cloud Act in the United States because of its inability to investigate the instant case concerning the client suspected of engaging in illegal activities. The Act encourages the storage of information within the United State's territory. Further, in Kenya during the 2017 presidential elections, OT-Morpho was the French company that had been outsourced by IEBC to man the server and to ensure the correct transmission of votes. The French firm was controversially awarded Sh6.8 billion to supply the Kiems kits used in the General Election. However, the kits failed on the election day and this was one of the reasons the Supreme Court relied on to nullify the presidential polls. The Supreme Court gave an order that it had to open its servers used in the 2017 presidential election for scrutiny.

1.3.3 Economic Reasons

Data localization, some regulators believe, is a quick way to force high-tech economic activity to take place within their borders—a new type of "digital mercantilism"—similar to how countries utilize tariffs to protect local manufacturing enterprises. Traditional trade-protectionism measures like tariffs are ineffective when it comes to digital economic activity, countries seeking digital mercantilism are turning to data localization regulations.[28] A number of recent papers have shown that the unilateral imposition of customs duties on electronic transmissions will:

- have distortive effects on growth of the digital economy
- be cost-prohibitive and technologically unfeasible
- likely fall foul of several existing free trade agreements under the most favoured nation principle.

Rather than impose customs duties, we think that a combination of internal taxation and international tax reform, undertaken by the OECD, is the best path forward for governments seeking to protect national revenue bases in the context of the digital economy.

Regulators believe that restricting data flows will give their countries a net economic advantage by forcing corporations to shift data-related jobs to their country. Companies may be required to

[28] Nigel Cory and Luke Dascoli, ' How Barriers to Cross-Border Data Flows are spreading Globally, What they Cost, and How to Address them' (July 19 2021), Information Technology and Innovation Foundation < https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost > accessed 7 April 2022

process and store data within the jurisdiction of the imposing state. The effect of this is that local processing firms are economically boosted and further, the imposing state benefits from technological innovation and development.[29]

1.3.4 Data Sovereignty

States use this justification because it allows them to carry out surveillance of their citizens and control the data access of their subjects. States use this justification to maintain control over data flows, data and digital technologies within their jurisdictions.[30] This can be tied with another justification provided for data residency. Some states argue that data localization requirements protect them from foreign surveillance which they would be easily susceptible to if they allowed for free flow of data.

1.3 Data Use and Misuse

The use of data and digital technologies is important to international trade. Data is used in global trade for the following: concluding contracts between parties to an agreement, communication on customer's addresses, monitoring consumer preferences, monitoring global value chains among others.[31] There are also certain ways in which data is susceptible to abuse that usually motivates policy makers and regulators to come up with localization requirements. Abuse encompasses conduct whereby a dominant firm takes advantage of its market power to exploit its trading parties or consumers (exploitative abuses) and conduct by which a dominant firm prevents or hinders competition on the market (exclusionary abuses).

Excessive data collection is one of the methods of data abuse. This is because it is an abuse of the dominant position held by a service provider or data regulator. The European Union (EU), whose data regulations Kenya has modelled, posits that under competition law, this kind of action is illegal.[32]

---

[29] *Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows are spreading Globally, what they Cost, and How to Address them'*

[30] n 30

[31] Nigel Cory, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?' (1 May 2017) Information Technology and Innovation Foundation < https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost > accessed 7 April 2022.

[32] Emma Fröderberg Shaiek, *Excessive Data Collection as an Abuse of Dominant Position; The Implications of the Digital Data Era on EU Competition Law and Policy*, Stockholm University, 2021, 3

Data abuse is also indicated in the following practices: excessive pricing, unfair trading conditions, breach of data protection values and restrictions on consumer choice.[33]

[33] Case 6/72, Europemballage Corporation and Continental Can Company Inc. v Commission, EU:C:1973:22

2.0 REGULATORY APPROACHES IN EU, CHINA, AND USA

2.1 Europe's geographically based approach

European Union (EU) has adopted a geographically based approach in order to govern cross-border data flow. That is, obstructing the free movement of cross-border data on the basis of data protection is prohibited within EU member states. Furthermore, non-EU member states must have proper data flow protection in place in order for EU member states to share data with them..[34]

2.1.1. Personal Data as Fundamental Rights

The EU considers communication privacy and personal data protection to be fundamental rights. Articles 7 and 8 of the European Union's 2000 Charter of Fundamental Rights make these rights binding on all EU members, and the 2009 Instrument of Lisbon (the EU's most recent institutional reform treaty) made them so. Furthermore, Article 52 of the Charter states that any restrictions on such rights must adhere to the proportionality principle, while Article 47 guarantees the right to seek judicial recourse for violations.

2.1.2. Unrestricted data flow inside the territory

Article 12 of the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (hereinafter the Convention), adopted in January 1981, states that state parties cannot restrict cross-border data flows solely on the basis of protecting privacy within EU member-states. That is, data can be transferred across EU member states as long as each member state adhere to the level of data protection provided for in the EU.

The EU adopted the "Directive on the protection of people with regard to the processing of personal data and on the free movement of such data" (hereafter referred to as "the Directive") in October 1995, which is the basic norm of EU data protection. Based on "the Convention," "the Directive" improved data mobility within the EU by removing barriers to data flow caused by local laws in member countries.

Furthermore, "the Directive" draws on and incorporates the legal practice of several European countries in terms of data controller rights and obligations, data oversight, and other topics. The practices of lowering obstacles and promoting free flow reflect the needs of the EU's political and

[34] Liu Hongsong and Cheng Haiye. (2020) Global governance of transborder data flow: progress, trends, and China's path[J]. Global Review,12(6):65-88.

economic integration, as well as the fact that the EU's internal regulatory position is heavily skewed toward encouraging data flow.[35]

2.1.3. The principle of "sufficient protection" for data transfer beyond the region

When data is moved outside of the EU, the EU follows the "adequate protection" standard. According to The Directive, which has been repealed by the General Data Protection Regulation (GDPR), data can be transferred only when third countries provide "similar," "equal," or "sufficient" protection to the EU or meet EU requirements. Furthermore, the EU's (GDPR)" adopted in May 2018 sets three factors for determining whether third nations provide specific appropriate protection: (1) the rule of law, including the degree of respect for human rights and fundamental freedoms, as well as relevant comprehensive and specialized legislation and their implementation; (2) the existence of an effective specialized regulatory organization; and (3) accession to international treaties or multilateral agreements on the protection of personal data, thereby assuming obligations under international law in that field.[36] Furthermore, GDPR applies if data organizations in the EU use or process personal data in the course of providing products and services. In terms of data flow outside the EU, the EU might be considered strongly inclined toward data limitation and control.

The EU's "geographically based" difference between internal and external data flows is an effective endeavor to find ways to guarantee data security while boosting data flows.[37] The EU law provides for uniform standards of data protection within the EU member states, while ensuring that external data flows into non-member states happen only, if those states have a proper standard of data protection. This regulatory road unifies standards, sets fair expectations for data rights realization, and makes it easier to prevent third nations from evading their own data protection rules.[38]

---

[35] Yang Xi. (2019) Intergenerational development and experience of EU's personal data protection system —a model of internal regulation and external expansion[J]. International Business, (5):145-156.
[36] Article 45(2) of the 2016 General Data Protection Regulation.
[37] Kuner C. (2010) Regulation of transborder data flows under data protection and privacy law: past, present, and future[R]. OECD Digital Economy Papers,20-21.
[38] LI Yanhua. (2019) Regulation path and China's choice on global cross-border data[J]. Present day Law Science,17(5):106-116

The GDPR is a component of the EU's digital data plan. In addition, European Commission is developing regulatory frameworks for data sharing, artificial intelligence, and other areas.[39]

The GDPR provides a consistent set of standards for personal data protection across the EU. It aims to protect people's fundamental rights in the digital era while also making business easier by ensuring that rules are applied consistently across the EU. Individual rights and corporation obligations surrounding data collection and processing are outlined in the GDPR. It applies to all enterprises and organizations in the EU that process personal data about individuals, regardless of where the data is processed. The GDPR, like the previous Data Protection Directiveonly allows the transfer of personal data outside the EU to countries that the EU considers to have an appropriate level of protection.[40]

2.2 The USA's Principle of accountability approach

There is no general federal legislation impacting on data protection and more particularly cross border data flows in the USA. While the United States Supreme Court has interpreted the Constitution to grant individuals a right to privacy, this right normally only protects them from government interference. The federal government's handling of personal information is governed by the Privacy Act of 1974,[41] while the Electronic Communications Privacy Act of 1986[42] expanded government limits on telephone wiretaps to include computer transfers of electronic data. Guidance on its approach towards cross border data flows can however be found in different federal and state laws that are sector specific as well as trade agreements the United States is party to.

For instance, in recent years, the United States has imposed strong restrictions on the cross-border transfer of technical and sensitive data affecting important science and technology disciplines. The US Export Administration Regulations (EAR), for example, mandate that export control is not confined to "hardware" shipments but also encompasses "software." That is, the transfer of scientific and technological data to servers outside the United States, as well as data out of the United States, requires an export license from the Department of Commerce Bureau of Industry and Security. The Foreign Investment Risk Review Modernization Act (FIRRMA) another example states that some non-controlled foreign investments undertaken by US corporations

[39] European Commission, Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence.
[40] GDPR Articles 44-50
[41] 5 U.S.C. §552a. The Privacy Act covers personal records maintained by federal agencies
[42] 18 U.S.C. §2510

involving "critical technology," "critical infrastructure," and "critical or sensitive data" will be subject to security reviews. Furthermore, the United States has broadened the scope of data control through "long-arm jurisdiction." The United States passed the "Clarifying Lawful Overseas Use of Data Act (Cloud Act)" in March 2018, establishing the premise that "whoever owns the Data controls the Control of the Data." This approach abandons the previous "server" standard in favour of the "data controller" standard, allowing the government to access and monitor data in foreign jurisdictions. The CLOUD Act primarily amends the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

On the other hand, the United States is a global leader in the digital economy and information technology. Both of which are sectors that rely heavily on access to cross-border data flows. This serves as an objective basis and premise for pushing for the free flow of global data.[43] Such commitment for free cross border data flows can be evidenced in trade agreements the US is party to such as the United-States-Mexico-Canada Agreement (USMCA)[44] that expressly prohibits restrictions to cross border data flows including transfer of personal data.[45] The only acceptable restrictions are those that pursue legitimate objectives and are not either disguised trade restrictions or more than is necessary to achieve the intended objective. This provision is almost a cut and paste from the then Trans Pacific Partnership Agreement between the US and 11 other nations in the Pacific[46] which, while the US later withdrew from, supports the notion that it is a strong supporter of free cross-border data flows..

Although the United States aims to foster free data flow and establish a barrier-free global Internet system, it is also concerned about the possible danger to its dominant position posed by the emergence of Internet companies in China and India such as TikTok that has been accused of massive data breaches.[47] These developments as well as public demand have led to active debates

[43] Zhang Monan. (2020) Cross-border data flow: global situation and the countermeasures for China[J]. China Opening Journal, (2):44-50.
[44] A free trade agreement between the three countries that was intended to modernise NAFTA. It entered into force on July 1,2020
[45] Chapter 19, Article 11
[46] Chapter 14, Article 11
[47] < https://www.washingtonpost.com/business/2022/06/29/fcc-tiktok-ban-apple-google/ > accessed on 7/28/2022

in congress for a potential comprehensive national policy on data privacy, and several laws on data protection and security have been submitted.[48]

The upshot is that the US approach to cross border data flows though not as clear cut as the EU GDPR puts global trade on a pedestal and is thus more skewed towards free cross border data flows including transfer of personal data. Protection of the fundamental right to privacy as well as other legitimate objectives that may require restrictions on the same such as national security are treated as exceptions and only permitted when necessary.

2.3 China's Security first approach

China's commerce and internet policies reflect official direction and industrial policy, limiting information flow and individual privacy. For example, requiring all internet traffic to transit via a national firewall can stymie cross-border data transmission.[49] China's counterterrorism law, enacted in 2015, requires telecommunications and internet service companies to aid the government, which might involve sharing individuals' data. Citing national security concerns, China's Internet Sovereignty policies, Cybersecurity Law, and Personal Information Security Specification impose stringent requirements on businesses, such as storing data domestically, limiting access to, use of, or transfer of data internationally, and mandating security assessments that give Chinese authorities access to proprietary information.

China launched a new social credit system in 2014, a centralized big-data-enabled system for monitoring and regulating the behavior of businesses and residents that functions as a self-enforcing regulatory mechanism. China's government says it wants to make people more "sincere" and "trustworthy," while also gathering credible data on the creditworthiness of firms and individuals. The degree of government services and possibilities available to an individual would be determined by his or her score. [50]

China released its Personal Information Protection Law (PIPL), a draft collection of laws aiming at regulating privacy law, in October 2020. The PIPL is intended to complete China's privacy legal framework, which began with the 2016 Cybersecurity Law (CSL). China, like other major

[48] 117th Congress, S. 224, H.R. 1816, H.R. 4801, S. 2499, CRS Legal Sidebar LSB10441, Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress, by Jonathan M. Gaffney.
[49] USTR, "2018 USTR Report to Congress on China's WTO Compliance," February 2019, p. 156.
[50] Kelsey Munro, "China's social credit system 'could interfere in other nations' sovereignty'," *The Guardian*, June 27, 2018.

international powers, understands that "knowledge is power," and that being up to speed on current events allows them to not only react fast but also influence the information's character.[51]

The PIPL establishes China's personal data protection regime, which is modelled in part after the GDPR. Personal information, sensitive personal information, and processing are among the key ideas introduced. The PIPL specifies its extraterritorial jurisdiction and includes standard data protection features such as personal information processing principles, consent and non-consent reasons for processing, cross-border transfer procedures, and data subject rights. Some provisions are still awaiting clarification from implementing rules as of the time of writing this note.

China passed the CSL on November 7, 2016, and it went into effect on June 1, 2017. Personal information protection obligations are included in the CSL, which apply to all businesses that use a computerized information network system. The CSL is the primary law governing cyberspace, with a focus on multi-level cybersecurity protection, important information infrastructure protection, cybersecurity reviews and inspections, and certification of key network equipment and unique cybersecurity goods.[52]

The Data Security Law (DSL) introduces a new data protection regime for China. The DSL is the foundational law for data security, and it establishes a set of policies to ensure data development and use, as well as industry development. These policies include data categorization and classification, data risk controls, data security contingency responses, data security reviews, export controls, and anti-discrimination. Specific rules for putting these ideas into action are expected in the future, and may include supporting laws, regulations, and recommendations.[53]

China aims to have all of its residents covered by the social credit system by 2020, requiring some US enterprises that do business in China, such as airlines, to join.[54] As of 2018, the portal receives data from a variety of government departments and financial firms. In several provinces, pilot initiatives are underway to apply various rewards and penalties in response to data collected. The

[51] Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? ITIF (May 1, 2017), https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost.
[52] Eric Rosenbach & Shu Min Chong, Governing Cyberspace: State Control vs. The Multistakeholder Model, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (2019)
[53] Ren Jiayu and Beijing Baidu Netcom Technology Co., Ltd.Beijing Haidian District First Interm People's Ct. Dec. 25, 2015). See Ren Jiayu and Beijing Baidu Netcom Technology Co., Ltd., , GLOBAL FREEDOM OF EXPRESSION - COLUMB. U. , https://globalfreedomofexpression.columbia.edu/cases/ren-jiayu-vbaidu/.
[54] Jack Karsten and Darrell M. West, "China's social credit system spreads to more daily transactions," Brookings, June 18, 2018.

lack of control an individual may have, as well as the exposure of what some consider private data, is a source of contention among observers both inside and outside of China.

Some countries, such as Vietnam, are following China's lead in developing cybersecurity policies that restrict data flows and necessitate local data storage and possible access by government officials.[55] Some US enterprises and other multinational corporations are considering abandoning the Vietnamese market rather than complying, while some analysts believe Vietnam's law may not be in accordance with current trade commitments.[56] India has also cited security as a justification for its draft Personal Data Protection Bill, which would impose broad data localization requirements and ban cross-border data transfers.[57] These countries, unlike the EU, do not identify protocols for allowing cross-border data flows. Officials in the United States have expressed worry about both Vietnam's and India's localization requirements.[58]

[55] Yee Chung Seck and Thanh Son Dang, "Vietnam National Assembly Passes the Law on Cybersecurity," Global Compliance News, July 2, 2018.
[56] Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review*, August 15, 2018.
[57] INDUSLaw, "India: The Debate – Data Localization And Its Efficacy," September 17, 2018.
[58] U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018.

3.0. ANALYSIS OF CROSS BORDER DATA RESTRICTIONS IN THE EAC AND ECOWAS RECS.

3.1. Introduction.

In the ECOWAS region and EAC Regional Economic Communities, the approaches to the flow of data has been a mixed bag. Due to the differences in political stability and economic development in the respective regions, there are stark contrasts in the presence, nature and sophistication of cross-border data flow regulations. For a small minority of politically unstable and least economically developed countries, policies relating to data governance and regulation have yet to be explored.[59] Ahead of the curve, however, are countries guided by different motivations within this emerging digital ecosphere. For these states, cross border data flow regulations are adopted for a myriad of reasons that include data sovereignty and economic development as well as cybersecurity and privacy concerns. These restrictions have played a key role in the nature and the type of data cross-border regulations within these countries.

Thus, this part shall first analyse the different cross-border regulations adopted in the continental level as well as the EAC and ECOWAS regional blocs and appraise their attempts to harmonize the approaches to cross border data flows. Secondly, it shall elaborate the themes underlying the regulations and procedures of specific countries in Africa and whether and to what extent they permit or enable data localization.

3.2. AU Malabo Convention and the ECOWAS Supplementary Act

The AU Malabo Convention which represents the attempt by the African Union to harmonize regulation of the cyber space in the African Content barely contains provisions touching on data localization.[60] That notwithstanding, it is clear from reading through the convention that the general approach adopted in the convention is that of protection of privacy and personal data.

Particularly regarding data localization, this stance is evidenced in **Article 14(6)** that requires the data controller to satisfy themselves of a third state's 'adequate level of protection' of the data to be transferred.[61] The convention, however, leaves out a definition or standards by which states can measure 'adequate level of protection' of personal data. It leaves it to individual states to determine

[59] The list of countries without any laws relating to data governance include Liberia, Sierra Leone, South Sudan and Burundi. Tanzania is in the process of drafting a law relating to data governance however, information related to it and its contents are scarce.

[60] Yet to enter into force subject to ratification by 15 states (Article 36). So far only 10 ratifications have been deposited with the chairperson of the African Union.

[61] A third state in the Convention is defined as a non-member state of the African Union.

the same according to their unique data needs and values, for example in Nigeria where the Office of Attorney General has to conduct an assessment of the receiving state's laws before onward transfer is made.[62] The standard therefore, in light of the Convention, is rather vague as it does not provide guidelines for establishing a safeguard mechanism or even a criteria to determine adequacy.[63]

The ECOWAS Supplementary Act mirrors the Malabo Convention in as far as the objectives and prerequisites of data localization are concerned. **Article 36(1)** requires that before data is transferred to a third state, it must have 'adequate level of protection' of the personal data within its territory. [64] It also leaves the determination of an 'adequate level of protection' standard to the member states but the overall idea is that cross border data flows is only permitted if the personal data in question can be guaranteed some level of protection in the third state.

On the other side of the continent, the EAC lacks a regional data protection instrument and there has been little to no effort on that end. Data localization is therefore regulated nationally by each partner state as shall be reviewed later in this discussion.

3.3. Privacy and Protection of Personal Data

In most of the states within the ECOWAS and EAC region, there has been a general emphasis on the protection of personal data and privacy. In fact, most cross-border regulations in these jurisdictions have been pursued solely in the context of personal data protection policies and laws. In this regard, there has been widespread adoption of the adequacy standard which only permits the transfer of personal data to another country if the receiving country is governed by an adequate standard of protection. This standard, inspired by the EU approach in the 1995 Directive and subsequently the EU-GDPR, is also reflected in the ECOWAS Supplementary Act on the Protection of Personal Data and the AU Convention on Cybersecurity. [65]

Apart from the transposition of the EU-inspired adequacy standard amongst these countries, these national regulations have inculcated additional and unique regulations including derogations,

[62] Clause 2.11 Nigeria Regulation Bill 2019
[63] African Union adopts framework on cyber security and data protection- Access Now- https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/ accessed 28th July 2022.
[64] a third state being any state that is not a member of the ECOWAS regional bloc.
[65] ECOWAS - Supplementary Act A1SA.1f01f10 on Personal Data Protection within ECOWAS, Article 36 (1); AU Convention on Cybersecurity, Article 14 (6)

exceptions and authorizations. The danger here is that the discordance in conceptualization of the adequacy standard in these countries compounded by some these additional and often convoluted requirements invariably contributes to de facto data localization because it renders cross-border transfers infeasible, impractical or expensive.

Thus, a country might not intend to actually localize data but its regulations significantly impede the process of cross-border transfer in a way that disincentivizes the process altogether, for example Nigeria's regulation of the Attorney General's supervision and analysis of a third country's data protection laws before cross border transfer is effected.[66] Nevertheless, this regulation mirrors Article 45 (2) (a) of the GDPR which provides that the Commission in coming up with an adequacy decision has to review the data protection law of the receiving state including its general and sectoral legislations and their compliance and implementation.[67] Consequently, this mirrors the requirement of Security Impact Assessment test done by data controllers to effect transnational transfers in accordance with the Chinese framework.[68] Materials required by the national cyber security and information departments as enunciated by the CyberSpace Administration of China's, Security Assessment of Cross- Border Transfer of Personal Information & Important Data of China include a Declaration Form, Contract entered into between the operator and the recipient and also an Analysis Report on the Security Risk Associated with the transfer.

This policy brief underscores the need for harmonization of data localisation policies as envisioned in the Malabo Convention and the ECOWAS Supplementary Act explored hereabove. In this part, we will outline the characteristics of these national regulations and how they affect data localization.

3.3.1. The definition of a third state.

The definition of a third state or a *pays-tiers/état-tiers* in the data protection laws of these countries is particularly important to the question of data localization. In the ECOWAS region, the ECOWAS Supplementary Act defines a third state as any non-state member of ECOWAS.[69] This

[66] Clause 2.11 Nigeria Regulation Bill
[67] Microsoft Word - Masteroppgave nesten ferdig.docx - https://bora.uib.no/bora-xmlui/bitstram/handle/1956/21714/96-JUS399-H19.pdf?sequence=1&isAllowed=y accessed 28th July 2022.
[68] A.37 The Cybersecurity Law of China and A. 8.7 The Information Security Technology- Personal Information Security Specification of China
[69] *ibid*, Article 2, 38

position is reflected in the data protection laws of Côte d'Ivoire,[70] Benin,[71]Guinea,[72] and Niger.[73] Secondly, in the laws of Senegal,[74] Mali,[75] and Togo,[76] a third state is defined to mean any other state while in Burkina Faso, that locution is avoided completely, preferring to refer instead to a foreign state or *pays étranger.*[77]

In the EAC region, the concept of a third state features less prominently. The region does not have a distinction of a third-state since there are no general rules relating to data protection. The specific countries within the EAC that have data protection laws do not define a third-party state. The general approach provided is the definition of a third party. Kenya, Uganda and Rwanda are in consensus with the definition of a third party being a person, including a natural person or a legal entity- juristic person excluding a person authorized to process or control data.[78]

This term *pays tiers* or third party is key in determining to which countries the requirements of cross-border transfer are applicable. For the first category of countries, it is permissible for a data processor to transfer personal data to another country within the ECOWAS regional economic community without the recipient state meeting an adequate level of personal data protection. For the second and third category of states in the ECOWAS bloc, their definition renders cross-border data flows more restrictive generally prohibiting cross-border transfer of data to any other country unless it is governed by an adequate degree of protection. This position is shared in the EAC region where the countries have enacted self-interested laws on data protection since there has been no drive for harmonisation at the regional level. The trend to discriminate between countries by exempting some countries while subjecting others to the standard, adequacy standard, is

[70] Loi sur la protection de données à caractère personnel (Law on the protection of personal data) No. 2013-450, Article 1
[71] Loi n° 2017-20 portant code du numérique en République du Bénin (2017 Digital code of the Republic of Benin), Article 1
[72] Loi No L/2016/037/AN relative à la cybersecurité et la protection de données à caractère personnel en Republique de Guinée (Law relative to cybersecurity and protection of personal data in the Republic of Guinea), Part II Article 28.
[73] Loi No 2017-28 du 03 mai 2017 relative à la protection des données à caractère personnel, Article 1
[74] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel (Law on the protection of personal data), Article 4
[75] Loi N°2013-015 du 21 mai 2013 portant Protection des Données à Caractère Personnel en République du Mali (Law on the protection of personal data in the Republic of Mali), Article 3
[76] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (Law on the protection of personal data), Article 4
[77] Loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Law on the protection of persons with regards to the processing of personal data), Article 42
[78] Data Protection Act of Kenya, Section 2; Data Protection and Privacy Act of Uganda, Section 2; Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 3 21°

antithetical to integration at the regional and the continental level. At a minimum, all countries within the same REC should be exempted from the standard with a view of progressively extending that preference to more countries within the ACFTA framework.

3.3.2. How the adequacy/sufficiency standard is evaluated

Cross-border transfer of data is only permissible where the recipient state assures an adequate or sufficient or equivalent level of protection of privacy and rights and fundamental freedoms of the data subject. This standard is difficult to reconcile when one considers that there are no harmonized criteria for adequacy between most countries in the ECOWAS region. Thus, a measure or policy in the receiving state can be considered adequate in one state but fall short in another. For some countries such as Côte d'Ivoire,[79] Togo,[80] Senegal,[81] Guinea, The Gambia and Niger,[82], there has been no attempt to further elucidate the criteria for this evaluation leaving unfettered discretion to the regulator to determine what this standard entails. The effect of this is that it implicitly enables data localization since a regulator is free to consider illegitimate factors to determine adequacy and creates uncertainty on the part of the processor.

Benin and Burkina Faso possess the most comprehensive breakdown of the evaluation of adequacy in the ECOWAS bloc. In Benin for instance, an adequate degree of protection is assessed taking into account: (1) the laws of the state both general and sectoral, the respect for rights and fundamental freedoms, the access of personal data by government authorities, the state's laws relating to transfer of data regarding onwards transfer, the administrative and juridical remedies available (2) the existence of independent regulatory authorities in the state in question charged to ensure the respect of rules relating to the processing of such data, assisting data subjects in the exercise of their rights and cooperating with the regulatory authorities of the member states of ECOWAS (3) the third states commitments under international law and binding obligations under conventions and other instruments in respect to the protection of personal data.[83]

In Burkina Faso, the criteria are almost similar. In this case, adequacy is determined taking into account: (1) existing general and sectoral laws and professional practices, (2) the treaties and

[79] Loi sur la protection de données à caractère personnel (Law on the protection of personal data) No. 2013-450, Article 26

[80] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (Law on the protection of personal data), Article 28

[81] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel (Law on the protection of personal data), Article 49

[82] Loi No 2017-28 du 03 mai 2017 relative à la protection des données à caractère personnel, Article 24

[83] Loi n° 2017-20 portant code du numérique en République du Bénin (2017 Digital code of the Republic of Benin), Article 391

conventions that the state is a party to, (3) or the guarantees *adhoc* or standardised agreed by the regulatory authority established by instruments that are legally binding and actionable to the persons involved in the transfer and further processing.[84] Mali's law on privacy also provides that adequacy shall be assessed by the regulator based on domestic legislation, international commitments and the extent to which the first two are effectively applied in the state.[85]

Cape Verde also considers nature of the data, the purpose and duration of the proposed processing, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in question, as well as the professional rules and security measures which are complied with in that country[86]

In Uganda, the test of adequacy is done by the data controller[87] or processor[88] who ensures that either: (1) the third state has "adequate measures" for the protection of personal data or (2) measures equivalent to the ones set by the Data Protection and Privacy Act of Uganda.[89] The use of the term "adequate measures" is vague since the specifics of what the data controller or processor is supposed to check -whether law or practice of the third state- is not provided. The provision of commensurate data protection laws to those of Uganda provides a clear platform on what adequacy actually entails.

3.3.3. Pre-approval procedures.

Some laws also require the approval of the regulator[90] for any effective transfer of data even where the recipient country assures an adequate degree of protection. Pre-approval procedures are particularly problematic because cross border data transfers are large scale and continuous exercises that are often automated. The idea of pre- approval procedures is generally political with countries claiming the need for data and information sovereignty. Thus, the requirement for seeking approval for each transfer is an inconvenience for any data processor seeking to delocalize

[84] Loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Law on the protection of persons with regards to the processing of personal data), Article 43

[85] Loi N°2013-015 du 21 mai 2013 portant Protection des Données à Caractère Personnel en République du Mali (Law on the protection of personal data in the Republic of Mali), Article 11

[86] Data Protection Act, The Republic of Cape Verde Law 133/V/2001, Article 19 (2)

[87] A person who determines the manner in which data is supposed to be processed; Data Protection and Privacy Act of Uganda, Section 2

[88] A person, who is not an employee of the data controller, who can process data on behalf of the data controller; Data Protection and Privacy Act of Uganda, Section 2

[89] Data Protection and Privacy Act of Uganda, Section 19(a)

[90] The regulator acts as an authority who oversees, checks and/or authorises the cross border transfer of data and works to ensure that the personal data of the data subject is not misused or violated in the country that seeks to protects the data subject's rights as well as the third country

processing of data. When compounded by the unfettered discretion of most regulators,[91] this leaves the otherwise well-intentioned data privacy laws creating cost and convenience obstacles for data processors which incentivize them to store personal data in local servers. The regulators are agents of the State hence it can easily be argued that they are driven by the interests of the State.

An analysis of the ECOWAS region shows that pre-approval of the regulator is required in the ECOWAS Supplementary Act,[92] as well as the national laws of Benin,[93] Niger,[94] Côte d'Ivoire,[95] Togo,[96] Guinea and Senegal.[97] The data protection law of Burkina Faso goes even a step further, requiring not only the prior approval of the regulator but also the signing with the contracting party a clause on confidentiality of data and another clause on the reversibility of data to facilitate the complete migration of data at the end of the contract as well as the implementation of technical and organisational security measures guaranteeing notably the encryption of data, the availability of data, the confidentiality, integrity, availability and the constant resilience of processing services and systems as well as an analysis and evaluation of taken measures.[98] Cross-border transfers in Mali do not require pre-approval of the regulator where the transfer is to a country governed by a sufficient degree of protection.[99]

In the EAC, pre-approval is deemed to be vital basing this on the laws of specific countries. It is seen as a means to protect the personal or even sensitive personal data of the data subject. The Ugandan law provides that an operator or a person authorised to process data on behalf of the data processor ought to seek authorisation from a data processor and the data obtained post-authorisation is deemed to be confidential.[100] In Rwanda, the cross-border transfer of personal data occurs after a supervisory authority accredits the data controller or processor to do so.[101]This

---

[91] Role of the Office of the Attorney General of the Federation of Nigeria in relation to data transfer.
[92] ECOWAS - Supplementary Act A1SA.1f01f10 on Personal Data Protection within ECOWAS, Article 36 (2)
[93] Loi n° 2017-20 portant code du numérique en République du Bénin (2017 Digital code of the Republic of Benin), Article 391
[94] Loi No 2017-28 du 03 mai 2017 relative à la protection des données à caractère personnel, Article 24
[95] Loi sur la protection de données à caractère personnel (Law on the protection of personal data) No. 2013-450, Article 26
[96] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (Law on the protection of personal data), Article 28
[97] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel (Law on the protection of personal data), Article 49
[98] Loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Law on the protection of persons with regards to the processing of personal data), Article 42
[99] Loi N°2013-015 du 21 mai 2013 portant Protection des Données à Caractère Personnel en République du Mali (Law on the protection of personal data in the Republic of Mali), Article 11
[100] Data Protection and Privacy Act of Uganda, Section 22(1)
[101] Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 48 1°

occurs as a means to protect the personal data of a data subject. The accreditation works as an approval or authorisation by the supervisory authority for the cross border transfer of personal data to occur. The authorisation also happens after the data controller or processor proves that there are safeguards to protect data in the third party state. The safeguards will be discussed.

3.3.4. Safeguards and guarantees.

Where the recipient country does not meet the standard of adequacy, some countries still permit cross-border transfers of data where the data processor makes sufficient guarantees of protection of the data and implements safeguards to ensure such protection. These guarantees may be in the form of contractual clauses or internal administrative rules of the controller in the third country providing for effective and actionable data subject rights. Ideally, safeguards and guarantees are derogations from the adequacy standard and loosen restrictions on the cross-border flows. However, they often come with stringent pre-approval procedures that make them counter-intuitive to their purposes.

An analysis of the data privacy laws in the ECOWAS region shows that in Burkina Faso,[102] Senegal,[103] Mali,[104] and Togo,[105] the regulator only authorizes such transfers after a duly justified request is submitted for the transfer by the data processor. In Benin, such transfers are authorized by decree of the Council of Ministers after the recommendation of the regulator.[106] In Côte d'Ivoire and Niger, there are no provisions for the transfer to countries not governed by an adequate degree of protection. Thus, it is presumed that such transfers are impermissible.

In the EAC, safeguards are mostly set up for the protection of sensitive personal data being data that relates to. In Rwanda, the data controller or processor is tasked with ensuring that there are measures, such as encryption and the strengthening of capacities of staff involved with the transfer, in place that will ensure that sensitive personal data.[107]It can also be interpreted that the safeguards

[102] Loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Law on the protection of persons with regards to the processing of personal data), Article 44
[103] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel (Law on the protection of personal data, Senegal), Article 51
[104] Loi N°2013-015 du 21 mai 2013 portant Protection des Données à Caractère Personnel en République du Mali (Law on the protection of personal data in the Republic of Mali), Article 11
[105] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (Law on the protection of personal data), Article 30
[106] Loi n° 2017-20 portant code du numérique en République du Bénin (2017 Digital code of the Republic of Benin), Article 392
[107] Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 11

ensure that the data controller does not lose, destroy or even damage data during transfer.[108]Further, a guarantee is provided through a written agreement if the data controller or processor authorises a person to transfer data outside Rwanda. Rwanda provides that the safeguards are ensured by the data controller or processor as registered under law hence can sue the data or processor involved for breaches.[109]

3.3.5. Necessity/ Derogations

This approach seeks for the need or reasons to offset data transfer, the necessity being the achievement of a certain specified objective. The bar set is quite high to the level of indispensable. Therefore, there has to be a connection between the necessary measure and the need to transfer the personal data of a data subject cross borderly while still respecting their fundamental rights and freedoms. This is borrowed from the EU GDPR (A. 23) which alternative requirements for data transfer include measures necessary for performance of a contract, compliance with a legal obligation, protection of vital interests, public or legitimate interests.[110]

The measures vary in different countries hence there is no general standard for necessary measures albeit some being similar in both the ECOWAS and EAC REC. It is important for countries to determine the importance of cross border transfer to the necessary measure set and also the contribution of the specific measure to the realisation of cross-border transfer of data. The general view provided then offers an objective element to necessity. However, a subjective sense can be derived since the character of countries, for instance what constitutes public interest and morality, is considered during the formulation of laws. This gives a lot of discretion to countries when it comes to determining what will constitute a measure necessary to allow cross-border transfer. The effect is that countries, especially in Africa, will install strict restrictions through local storage and processing requirements which infringe on the cross-border transfer of data.

In the ECOWAS REC, states can derogate from the adequacy approach where such data transfer is necessary in instances of public interest, performance or conclusion of a contract or any other

[108] Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 47
[109] Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 49
[110] Microsoft Word - Masteroppgave nesten ferdig.docx - https://bora.uib.no/bora-xmlui/bitstram/handle/1956/21714/96-JUS399-H19.pdf?sequence=1&isAllowed=y accessed 28th July 2022.

legitimate and explicit purpose.[111] These requirements are found in Gambia's Draft Policy Strategy,[112] and Cape Verde's Data Protection Act.[113]

Moreover, the adequacy requirement can be derogated from in situations where the data subject consents to the transfer. This is the case in the Gambia, Cape Verde, Ghana, Nigeria and Senegal. For Senegal specifically, consent requires that the data owners give clear permission, explicit consent which is a Chinese approach, for the use of their data through an affirmative action. Such consent can also be withdrawn. The data owner will also be allowed to revoke their consent to the processing of their data at any point. In addition, third-party subcontractors are also required to comply with the law.[114]

In Rwanda, the necessity of the cross-border transfer of personal data occurs in situations where there is need to fulfil contractual obligations between the data controller and subject, for the interest of the data subject, for fulfilling the contractual obligation between a data controller and data subject in the interest of the data subject, for public interest, for the sake of a legal claim, for the protection of data where the data subject is unable to give consent and for the performance of internationally ratified instruments in Rwanda.[115]

3.4.Strict Data Localisation Requirements.

Nigeria and Kenya employ a hybrid approach by making use of strict data localization requirements and the GDPR conditional transfer approach.

3.4.1.General Requirements

Nigeria and Kenya have data protection regulations similar to the EU GDPR on consent and adequacy with strict data localization rules for example the requirement for telecommunication companies and data communication firms to host all subscribed and consumer data as well as national data in Nigeria.[116] As at now, Nigeria is the only African country to adopt strict data

[111] https://africadpconclave.com/2020/10/05/personal-data-protection-and-cybersecurity-laws-in-jurisdictions-in-africa-encouraging-the-best/#:~:text=In%20spite%20of%20the%20adoption,to%20enact%20data%20protection%20laws. Accessed 8th April 2022

[112] section 9.1

[113] Article 20

[114] What to Consider Ahead of the AfCFTA Phase II Negotiation: Focus on Digital Trade Policy Issues in Four Sub-Saharan African Countries – https://www.bsg.ox.ac.uk/sites/default/files/2022-03/Digital trade policy AfCFTA_EN.pdf accessed 9th June 2022.

[115] Law Relating to the Protection of Personal Data and Privacy of Rwanda, Article 48 3°

[116] What to Consider Ahead of the AfCFTA Phase II Negotiation: Focus on Digital Trade Policy Issues in Four Sub-Saharan African Countries – https://www.bsg.ox.ac.uk/sites/default/files/2022-03/Digital trade policy AfCFTA_EN.pdf accessed 9th June 2022.

localization laws for economic purposes.[117] This was done to add domestic value i.e. local content to Nigeria's ICT products and redress the negative trade balance in the ICT industry.

Data Protection Regulation in Nigeria's Regulation Bill of 2019 is an indirect and de facto cross border restriction in that transfer of personal data to a foreign country or international organisation can only take place where that country, territory, international organisation or sector ensures an adequate level of protection, requirements of consent and processing of personal data for a legitimate and explicit purpose.[118]

Adequacy safeguards can be ensured when certain conditions are realised which include where the data subject has explicitly consented, transfer is necessary for the performance or conclusion of a contract, necessary for reasons of public interest, or establishment of a defence or legal claim inter alia provided the data subject is not answerable to a legal action in a 3rd country.[119]

The Kenya Data Protection Act (KDPA)[120] also has provisions where data can be transferred to another country only if the data controller or processor provides sufficient evidence that the foreign country has commensurate data protection laws (adequacy element) to those of Kenya in order to be able to show that the foreign country can protect the data at least to the level provided by the KDPA.[121]The requirement of consent is crucial during the cross-border transfer of sensitive personal data or information.[122]There is also an element of necessity which occurs;- for the performance of contractual obligations between the data controller and subject; for a matter of public interest; for a matter in a legal claim; for the protection of the interests of the data subject where the data subject is unable, not unwilling, to give consent; and for compelling the interests of the data controller so long as it does not go against the interests of the data subject.[123]

---

[117] The Impact of Data Localization Laws on Trade in Africa- 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 accessed 8th April 2022.
[118] https://africadpconclave.com/2020/10/05/personal-data-protection-and-cybersecurity-laws-in-jurisdictions-in-africa-encouraging-the-best/#:~:text=In%20spite%20of%20the%20adoption,to%20enact%20data%20protection%20laws. Accessed 8th April 2022
[119] Clause 2.12 Nigeria Regulation Bill 2019
[120] Act No 24 of 2019
[121] Data Protection Act of Kenya, Section 48 (a) and (b); Data Protection (General) Regulations of Kenya, Regulation 38 (1)(a) and (c)
[122] Data Protection Act of Kenya, Section 49; Data Protection (General) Regulations of Kenya, Regulation 38 (1)(b)
[123] Data Protection Act of Kenya, Section 48 (c)

3.4.2. Localization of Data Centres

In Kenya, a data processor or controller who processes data for public good is obliged to ensure that the process occurs through a data center located in Kenya and at least one serving copy of the personal data should be stored in Kenya.[124]Kenya has generally learnt the importance of having local servers storing information after the 2017 election where it was alleged that servers went missing as well as the servers which were located in France, were hacked. The localisation of data centers seeks to promote the data integrity, transparency, confidentiality and availability[125] as can be buttressed by the action of the Independent Electoral and Boundaries Commission where they brought the data centers containing election data in Kenya. Some safeguards provided include the fact that a civil registration entity can only transfer data outside Kenya upon approval by the National Security Council.[126]

In Kenya, the National ICT Policy of 2019[127] stipulates the need for the Kenya Government data to remain in Kenya. It also encouraged shared data centers for the government to aid in the storage of data. The Kenya Information and Communications Act[128] (KICA) requires that the Cabinet Secretary in charge of the Ministry of Information, Communications and Technology, Kenya, in coordination with the Communications Authority of Kenya (CAK) to create regulations to promote the privacy of telecommunications.[129] So far, the aim of the Kenyan Government seems to be pegged around the promotion of the right to privacy in Kenya through localisation.

KICA led to the establishment of the Kenya Information and Communications (Registration of Sim-Cards) Regulations of 2015. The regulation stipulates that telecommunication companies should provide the CAK access to their data in order for CAK to monitor the compliance of telecommunications to the KICA. This would only mean that the data centers of the telecommunication providers should be located in Kenya, Airtel has its data center in Nairobi while Safaricom has data centers in Kisumu and Thika. The telecommunication service providers are obliged to provide all communication data to the government and its agencies in case of emergencies.[130]

[124] Data Protection (General) Regulations of Kenya, Regulation 25
[125] Elections (Technology) Regulations, 2017, First Schedule Rule 14
[126] Data protection (Civil Registration) Regulations, Regulation 38
[127] Ministry of Information, Communications and Technology, Kenya November 2019
[128] No 2 of 1998
[129] Kenya Information and Communications Act, section 27(2)
[130] The Kenya Information and Communications (Consumer Protection) Regulations 2010, Regulation 19

In Nigeria, the National Information Technology Development Agency's (NITDA),[131] statutorily mandated by the NITDA Act 2007 to develop regulations for electronic exchange and interchange issued the mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (2019).[132] These Guidelines stipulate that both consumer and national data be hosted locally by telecommunication companies and data information management firms. Such data cannot be hosted outside the country without an express approval from NITDA and the Attorney General's supervision.[133] Such approval may be granted after much consideration including compliance with the Nigeria Regulation Bill as well as adequate and appropriate data security.[134] This was done with the aim to stimulate and increase indigenous innovation of information technology products and services for the development of the ICT industry.

Consequently, The Honorable Attorney General Federation (HAGF), which is the office of the Attorney General,[135] takes into account the legal system of that territory including matters rule of law, both general and sectoral legislations including public authorities access to personal data.[136] The HAGF also takes into account data protection rules of that foreign territory including rules of onward transfer of personal data, existence of an independent supervisory authority to implement data subject rights and the international commitments of that foreign territory when giving approval for transborder data transfers.[137]

When processing of personal data is done, such personal data is not to be transferred or disseminated to another.[138] In a nutshell, the Regulation requires personnel processing or controlling data to ensure data security by setting up firewalls, employing data encryption technologies, access being granted to specific authorised individuals, protection of emailing systems inter alia.[139]

---

[131] National Information Technology Development Agency which laid down the Nigeria Data Protection Regulation.
[132] How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them | ITIF accessed 8th April 2022
[133] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost accessed 8th April 2022
[134] Clause 2.6
[135] This is the Office of the Attorney General of the Federation who serves as a Chief Legal Officer of the Federation and also serves as a Minister of Justice concerned with policy questions. The role of the HAGF on matters international data flows reflects the fact that data agencies in Nigeria are not independent as is the case in other jurisdictions.
[136] Clause 2.11 Nigeria Regulation Bill 2019
[137] Clause 2.11 Nigeria Regulation Bill 2019
[138] Clause 2.1 Nigeria Regulation Bill 2019
[139] Clause 2.6 Nigeria Regulation Bill 2019

Sectorally, The Central Bank of Nigeria enacted local storage and processing requirements for entities engaging in point of sale (POS) card services. The Central Bank of Nigeria (CBN) introduced the Point of Sale (PoS) system in 2012 to further drive home its cashless policy aimed at enhancing Nigeria's payment system. Domestic transactions ***cannot be routed outside*** Nigeria for switching between Nigerian issuers and acquirers.[140] This is to ensure legislative adequacy in the destination country. NITDA also released the Nigerian Cloud Computing Policy which promotes cross-border data transfers, but also requires that, where cloud service providers are contracted by Nigerian national institutions, the condition is that data is stored in a jurisdiction with equivalent data protection given by Nigeria.

If these data localization rules are adhered to strictly, they can be protectionist and serve as non-tariff barriers to cross border trade especially trade agreements between Nigeria and for example the US which defends liberalization of data flows.[141] This is because Article 15 of the AfCFTA Protocol on Trade in Services allows for the enforcement of data localization rules only where they do not constitute arbitrary and unjustifiable discrimination to trade.[142]

3.5. Local Ownership of Business Requirements and Data Localisation

Data localization may happen through direct legal restriction or prescriptive requirements such as local business registration requirements.[143] An example of this is in Ghana where the Payment Systems and Bills Guidelines set out requirements to obtain a payment systems operator license where firms to be established must have at least 30% local ownership and the board of directors must include three Ghanaians one of them being the CEO.[144] This can be categorised as adoption of the Chinese approach of data localization prescriptive requirements.[145]

---

[140] The Central Bank of Nigeria's mandatory 2011 Guidelines on point of Sale (POS) Card Acceptance Services.
[141] The Impact of Data Localization Laws on Trade in Africa- 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 accessed 8th April 2022.
[142] Data Protection| eReader – https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-4-data-privacy-and-data-protection/data-protection/ accessed 8th June 2022.
[143] *ibid* 48
[144] Data Protection Laws of the World: Angola vs Ghana available at www.dlapiperdataprotection.com accessed 6th April 2022
[145] Data Protection Laws of the World: Angola vs Ghana available at www.dlapiperdataprotection.com accessed 6th April 2022

Data residency requirements affecting either storing or processing of data are put in place to make it infeasible i.e., more expensive, more time consuming and requiring government authorization, to transfer data.[146] These requirements do not necessarily inhibit transborder data because in Ghana, data transfer can take place in two scenarios;

i. where Business Process Outsourcing (BPO) operations, from 3rd countries, processing is done in Ghana, data protection laws from the third country are the ones to be complied with and therefore the Data Protection Act (DPA) cannot be used to transfer data in Ghana where such BPO business violates its own protection laws,[147] and

ii. where personal data protected by Ghana's DPA is outsourced to 3rd country BPO operations to process. The 3rd country BPO business must strictly comply with the DPA.[148]

Conclusion

This study has shed a lot of light on the importance and limitations of data restrictions. It can generally be assessed that it all depends on the point of view. The governments consider it as a mean to protect data integrity and sovereignty and in some cases, as a means for the realization of the right to privacy. Companies find it as restraining for their business as data is subject to scrutiny and technical procedures set by the government.

In the ECOWAS REC, the ECOWAS Supplementary Act 1 tries to unify the region's data protection approach. The unification, from the study, helps guide countries on how to make legislation. The EAC REC has no form of unification. Countries have domestic regulation while some even have no form of regulation in place.

Generally, the study has deduced that when countries make their own laws which involve strict data localization standards, the process of cross border data transfer is fettered by the technical procedures of the rigid law. It is also important to highlight that the person in charge of authorizing cross border data transfer in the ECOWAS and EAC countries has the capacity to deny the

[146] https://www.google.com/amp/s/incountry.com/blog/data-residency-laws-by-country-overview/amp/ accessed 16th June 2022.
[147] Africa Guide Local Ownership and Empowerment - https://www.bowmanslaw.com/cop-content/uploads/2021/01/Africa-Guide-Local-Ownership-and-Empowerment.pdf accessed 14th June 2022.
[148] Africa Guide Local Ownership and Empowerment (n 70) above

transfer process. This confined state will surely affect Africa's social, political and economic affairs down the line.

Annex

See the excel spreadsheet attached to this document tabulating the different regional laws.

State/Region	Requirements for cross-border data transfer	Types of data affected	Restrictions and Rationale
EAC	No regulation at the REC level	N/A	N/A
Kenya	**Personal data** The pre-approval by the data protection authority based on: a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor. - Subject to such derogations as the consent of the data subject, public interest or performance of a contract. -**For personal data of strategic interest**: local processing or storage of at least one serving copy in a local data center	-Personal data -Civil registration and legal identity -Election related data -public financial data -data emanating from a protected computer system -data relating to early childhood and basic education data -health data	- Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens. -Strict localization requirements for data of strategic interest as a matter of expediency in access to such data as well as law enforcement and regulatory reasons.
Uganda (GDPR inspired)	The data processor shall ensure: a) The recipient country assures a commensurate degree of protection; or b) the consent of the data subject	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.
Rwanda (GDPR inspired)	The pre-approval by the data protection authority based on: a) Assurance of appropriate safeguards to data protection by the processor - Subject to such derogations as the consent of the data subject, public interest or performance of a contract.	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.

ECOWAS	Except where the recipient state is a member of the ECOWAS The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state	Personal data	-Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens. -Possibly fostering e-commerce within the ECOWAS REC.
Nigeria	**ATM and POS Transaction data** Should be processed locally **Subscriber and consumer data** of ICT companies to be stored and processed locally ***Personal data (not yet in force)** The authorisation of data authority based on: a) commensurate degree of protection of the data in the recipient state b) Assurance of appropriate safeguards to data protection by the processor - Subject to such derogations as the consent of the data subject, public interest or performance of a contract.	-Data relating to POS and ATM transactions (Financial data) - Subscriber and consumer data - Government data - Personal data	- Localising subscriber and consumer data is to stimulate the digital domestic economy of Nigeria - For government data, cybersecurity -data protection bill is an implicit localisation requirement is to strengthen privacy rights of citizens.
Ghana	-No explicit provision that prevents the transfer of data to foreign states. Generally, data cannot be processed without the consent of the data subject. - However, in order for a firm to obtain a license as a payment systems operator (PSO), it is mandatory to have at least 30% ownership, and have at least 3 Ghanaians in the board of directors including one acting as CEO. *PSOs include examples such as GooglePay, ApplePay, AmazonPay. More locally, we have Safaricom MPesa.	Financial data	Implicit localisation. Only local PSOs and foreign PSOs abiding by Ghanaian local business ownership requirements can process financial data of Ghanaian citizens. Speculatory aim is data sovereignty
Benin	Except where the recipient state is a member of the ECOWAS: The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state; or	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data

	b) Assurance of appropriate safeguards to data protection by the processor. - Subject to such derogations as the consent of the data subject, public interest or performance of a contract.		privacy rights of citizens. -Possibly fostering e-commerce within the ECOWAS REC.
Burkina Faso (GDPR inspired)	The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor. c) Subject to such derogations as the consent of the data subject, public interest or performance of a contract.	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.
Cote d'Ivoire	Except where the recipient state is a member of the ECOWAS, the pre-approval by the data protection authority of every effective transfer based on a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor.	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens. -Possibly fostering e-commerce within the ECOWAS REC.
Mali	a) That the recipient state assures a commensurate degree of protection through national law or international obligations and that they are effectively applied; or b) The pre-approval of the data authority that the data processor assures appropriate safeguards on the protection of data through internal rules and contractual clauses	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.
Niger	Except where the recipient state is a member of the ECOWAS, the pre-approval by the data protection authority of every effective transfer based on: a) Commensurate degree of protection of data in the receiving state	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens. -Possibly fostering e-commerce within the ECOWAS REC.
Guinea	Except where the recipient state is a member of the ECOWAS, the pre-approval	Personal data	Qualitative restriction of

	by the data protection authority of every effective transfer based on: a) Commensurate degree of protection of data in the receiving state		personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens. -Possibly fostering e-commerce within the ECOWAS REC.
Senegal	The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor.	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.
Togo	The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor	Personal data	Qualitative restriction on the transfer of personal data through the requirement of pre-approval and the adequacy standard.
Cape Verde	The pre-approval by the data protection authority based on a) Commensurate degree of protection of data in the receiving state; or b) Assurance of appropriate safeguards to data protection by the processor. c) Subject to such derogations as the consent of the data subject, public interest or performance of a contract.	Personal data	Qualitative restriction of personal data based on adequacy standards. Aimed at protecting data privacy rights of citizens.

BIBLIOGRAPHY

Case laws

Europemballage Corporation and Continental Can Company Inc. v Commission EU:C:1973:22

United States v Microsoft Corporation [2018] 584

Statutes

AU Convention on Cybersecurity

Data protection (Civil Registration)

Data Protection (General) Regulations of Kenya

Data Protection Act of Kenya

Data Protection Act, The Republic of Cape Verde Law 133/V/2001

Data Protection and Privacy Act of Uganda

Elections (Technology) Regulations, 2017

General Data Protection Regulation, 2016

Kenya Information and Communications Act

Law Relating to the Protection of Personal Data and Privacy of Rwanda

Loi n° 2008-12 portant sur la protection des données à caractère personnel (Law on the protection of personal data),

Loi n° 2017-20 portant code du numérique en République du Bénin (2017 Digital code of the Republic of Benin)

Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (Law on the protection of personal data)

Loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel (Law on the protection of persons with regards to the processing of personal data)

Loi N°2013-015 du 21 mai 2013 portant Protection des Données à Caractère Personnel en République du Mali (Law on the protection of personal data in the Republic of Mali)

Loi No L/2016/037/AN relative à la cybersecurité et la protection de données à caractère personnel en Republique de Guinée (Law relative to cybersecurity and protection of personal data in the Republic of Guinea)

Loi sur la protection de données à caractère personnel (Law on the protection of personal data)

National Information Technology Development Agency which laid down the Nigeria Data Protection Regulation.

Nigeria Data Protection Regulation (2019)

Nigeria Regulation Bill 2019

Personal Data Protection within ECOWAS

The Central Bank of Nigeria's mandatory 2011 Guidelines on point of Sale (POS) Card Acceptance Services.

The Kenya Information and Communications (Consumer Protection) Regulations 2010, Regulation 19

The Privacy Act

Articles

Assan Jallow, '*Why the Internet has resulted in more International Business and What Factors are Responsible for the Increase in the Volume in International Trade*?' (13 October 2019)

Emma Fröderberg Shaiek, *Excessive Data Collection as an Abuse of Dominant Position; The Implications of the Digital Data Era on EU Competition Law and Policy*, Stockholm University, 2021

Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. The Multistakeholder Model, Paper, Belfer Center for Science and International Affairs*, Harvard Kennedy School (2019)

European Commission, Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence.

Francesca Casalini & Javier López González, *'Trade and Cross-Border Data Flows'* (2019) OECD Trade Policy Papers No.220 OECD Publishing, Paris

Global Investigations Review, 'Regulatory Compliance in the Context of a Cross-Border Data Breach' (8 June 2021)

INDUSLaw, "India: The Debate – Data Localization And Its Efficacy," September 17, 2018.

Jack Karsten and Darrell M. West, "*China's social credit system spreads to more daily transactions,"* Brookings, June 18, 2018.

Jinhe Liu, 'China's Data Localization' (August, 2019)

Jonathan M. Gaffney, *Watching the Watchers: A Comparison of Privacy Bills* in the 116th Congress.

Joshua Meltzer, '*The Internet, Cross-Border Data Flows and International Trade'* (February 2013) Issues in Technology Innovation Number 22

Kelsey Munro, "China's social credit system 'could interfere in other nations' sovereignty'," *The Guardian*, June 27, 2018.

Kuner C, *Regulation of transborder data flows under data protection and privacy law: past,*

LI Yanhua, *Regulation path and China's choice on global cross-border data*, Present day Law Science,17 (2019).

Liu Hongsong and Cheng Haiye. (2020) *Global governance of transborder data flow: progress, trends, and China's path* Global Review.

Martín Molinuevo and Simon Gaillard, '*Trade, Cross-Border Data, and the Next Regulatory Frontier: Law enforcement and data localization requirements'* (2018) World Bank Group Number 3

Martina F. Ferracane, '*Restrictions on Cross-Border data flows: a taxonomy'* (2017) European Centre for International Political Economy ECIPE Working Paper -No.1 of 2017

Martina F. Ferracane, *'Restrictions on Cross-Border data flows: a taxonomy'*

Nigel Cory and Luke Dascoli, '*How Barriers to Cross-Border Data Flows are spreading Globally, What they Cost, and How to Address them*' (July 19 2021), Information Technology and Innovation Foundation

Nigel Cory*, 'Cross-Border Data Flows: Where are the Barriers, and What do they Cost?'*

Nigel Cory, "*Vietnam's cybersecurity law threatens free trade*," *Nikkei Asian Review*, August 15, 2018.

present, and future, OECD Digital Economy Papers, 2010.

Ren Jiayu and Beijing Baidu Netcom Technology Co., Ltd. Beijing Haidian District First Interm People's Ct. Dec. 25, 2015.

Svetlana Yakovleva and Kristina Irion, "*Pitching trade against privacy: reconciling EU governance of personal data flows with external trade*" International Data Privacy Law, 2020, Vol. 10, No. 3

Svetlana Yakovleva and Kristina Irion, *"Pitching trade against privacy: reconciling EU governance of personal data flows with external trade"* (2020) International Data Privacy Law, Vol. 10

U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018.

United Nations Conference on Trade and Development, *'Global e-Commerce Jumps to $26.7 Trillion, Covid-19 boosts Online Sales*' (3 May 2021)

USTR, "2018 USTR Report to Congress on China's WTO Compliance," February 2019.

Yang Xi *Intergenerational development and experience of EU's personal data protection system —a model of internal regulation and external expansion*, International Business, (2019).

Yee Chung Seck and Thanh Son Dang, "*Vietnam National Assembly Passes the Law on Cybersecurity*," Global Compliance News, July 2, 2018.

Zhang Monan, *Cross-border data flow: global situation and the countermeasures for China*, China Opening Journal, (2020).