FMC

ADVOCATES

SAFEGUARDING TRADE IN THE DIGITAL AGE: EXPLORING DATA PRIVACY IN INTERNATIONAL COMMERCE WITHIN AFRICA

LETTER FROM THE EDITOR

Dear Readers,

Greetings and a warm welcome to this edition of our Legal Take Publication dubbed 'Safeguarding Trade in the Digital Age: Exploring Data Privacy in International Commerce within Africa", where we delve into the fascinating realm of data privacy and international trade.

In an increasingly interconnected world, the relationship between data privacy and global commerce has become a paramount concern for businesses, governments, and individuals alike. This issue aims to provide comprehensive insights into the challenges and opportunities arising from this intersection, with a specific focus on the African context.
Our journey begins with a critical examination of "Mitigating Data Risks in Trade" and reflections on the state of data privacy legislations within the African Regional Economic Blocs. Africa is a continent of immense diversity, encompassing various economic blocs with unique challenges concerning data privacy regulations. In this publication, we explore the progress made by regional organizations, such as the Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC), in developing robust data privacy frameworks that align with international standards. By understanding the regional landscape, we aim to foster a dialogue that encourages harmonization of data privacy laws and facilitates smooth cross-border trade in Africa.

Assessing the adequacy of cyber laws and the legal framework in the East African Community (EAC) in addressing data privacy challenges is the next topic we delve into. As technology continues to drive economic growth in the East African region, it is essential to evaluate the existing legal framework's effectiveness in safeguarding data privacy. Our experts analyze the strengths and weaknesses of current cyber laws and identify areas for improvement. By enhancing the legal framework, the EAC can create a conducive environment for digital trade and foreign investment while ensuring that individuals' privacy rights are adequately protected.

Cross-border risks are inherent in international trade, particularly when it comes to data transfer. In "Cross Border Risks: Exploring Data Transfer Frameworks within the EU and Africa," we investigate and compare the complexities surrounding data transfers within the European Union (EU) and Africa. The EU's General Data Protection Regulation (GDPR) and the AfCFTA present unique challenges for businesses engaged in transcontinental trade. This publication examines the legal frameworks and mechanisms in place to facilitate cross-border data transfers, while upholding data privacy and security.

The regulatory steps taken by the Office of the Data Protection Commissioner in securing information transferred out of Kenya are also under scrutiny in this issue. Kenya, as a key player in Africa's tech and trade landscape, has been proactive in adopting data protection measures. We explore the regulatory landscape and highlight the steps taken by the Data Protection Commissioner to ensure that data transfers involving Kenya comply with data protection regulations. Such initiatives play a crucial role in enhancing data privacy standards and bolstering international trade relationships.

"The Interplay of Free Cross Border Data Flow and Data Privacy in International Trade: A Kenyan Perspective" serves as a capstone article, weaving together the various themes explored in this publication. As data-driven global trade becomes increasingly prevalent, the balance between facilitating free cross-border data flow and safeguarding data privacy emerges as a critical concern. This article presents a Kenyan perspective, shedding light on the challenges faced by the nation in striking this balance and the steps taken to encourage responsible data practices and foster a thriving digital economy.
As we navigate the intricacies of data privacy and international trade, it is essential to recognize that these topics are not isolated realms. Instead, they intersect and shape each other in profound ways, influencing how businesses conduct global transactions and how governments frame regulatory policies. Collaboration among stakeholders - policymakers, legal experts, industry leaders, and citizens - is vital in establishing a cohesive and forward-looking approach to data privacy in the context of international trade.

I extend my heartfelt gratitude to all the esteemed team at FMC Advocates who contributed their expertise to this issue. Their valuable insights have enriched our understanding of the multifaceted relationship between data privacy and international trade in the African context.

In conclusion, as technology continues its rapid evolution, data privacy will remain a critical consideration in the realm of international trade. We hope that this publication sparks fruitful discussions and fosters an environment of continuous learning and growth in the tech law domain.

Thank you for your continued support, and we hope you find this edition both informative and enlightening.

Sincerely,

Lewis Ndonga
Editor,
August 2023

MITIGATING DATA RISKS IN TRADE

Reflections on the State of Data Privacy Legislations within the African Regional Economic Blocs

By Alfred Nyaga & Diana Wariara

The digital age has certainly been disruptive for African States and transitioned us into a global information economy in which vast amounts of information are transmitted, stored, and collected across the globe. This has been further enabled by massive improvements in computing and communication power. In Africa, online, social, economic, and financial activities have been facilitated through mobile phone uptake and greater internet connectivity. The transborder nature of the internet as well as the speed and sheer volume of communications often poses a dilemma for governments, that is, protection of data privacy vis-à-vis promotion of the digital economy.

It goes without saying, cross border trade thrives on transfer, exchange, and collection of data within the regional economic blocs in Africa. This is crucial in promoting trade between different jurisdictions. However, there have been concerns on the magnitude of data collected, exchanged, and transferred during cross-border trade between citizens of different states in Africa. Further to this, it is worth noting that some of the member states of different regional economic blocs have made enormous strides in addressing the issues of cross border transfers of data while others still have a long way to go.

In the interest of promoting seamless trade and economic development within the member states, the blocs have resolved to enact and adopt data protection frameworks to address the concerns of breach of data privacy during trade. This being a protectionist measure aimed at curbing data loss and misuse risks. Data privacy is not an alien concept with respect to cross-border trade in African regional economic blocs. However, it is still in its initial and formative stages of growth and appreciation by African states. To this end, data privacy frameworks have been adopted by various regional economic communities (RECS) in Africa to promote seamless trade within the member countries and to spur economic development within their member states. This Article shall examine the data protection framework within ECOWAS and SADC and highlight key challenges.

The Data Protection framework on the East African community shall be examined in this publication.

DATA PROTECTION LEGAL FRAMEWORK WITHIN THE ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS)

ECOWAS was developed to spur seamless economic growth within its fifteen (15) members states (that is Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal, and Togo). Due to digitization, there was a need to protect the privacy of traders engaged in cross-border trade and e-commerce transactions within the bloc. On 16th February 2010, the Heads of States and Government of the ECOWAS signed into law the "Supplementary Act on Personal Data Protection within the ECOWAS" which extensively borrows from the European Union General Data Protection Regulation (GDPR).

The ECOWAS framework stipulates the required content of data privacy laws and obligates member states to establish data protection enforcement authorities. The purpose of the legislation is to establish a harmonized legal framework for the processing of personal data. To preserve the independence of the data protection authority, its member states cannot be members of government, or business executives or own shares in businesses in the information or telecommunications sector. Further, the ECOWAS framework restricts cross-border transfer of data to only countries that have adequate protection of data privacy. This measure is aimed at ensuring the protection of personal data. However, this limitation has a far-reaching effect on trade because member states with inadequate regulations on data privacy are restrained from engaging in cross-border trade which heavily relies on exchange and transfer of data with traders in different member states.

The legislation does not address the harmonization of data protection legislation within the economic community. Harmonization of the laws entails members states enacting and/or amending their data protection laws to align with the ECOWAS framework thus achieving consistent and uniform laws including the application and implementation of the laws. Therefore, the lack of harmonization of the legislations adversely affects cross-border trade due to fear of traders engaging in trade with citizens of member states where their data is likely to be misused or face data risks such as tampering, fraud, phishing, espionage, malware attacks among other risks.

DATA PROTECTION LEGAL FRAMEWORK WITHIN THE SOUTHERN AFRICA DEVELOPMENT COMMUNITY

The Southern African Development Community Model Law on Data Protection came into force in 2013 to address the aspects of data protection in cross-border transactions within its sixteen (16) member states. This is because data privacy is a key factor for consideration in cross-border trade due to the large amounts of data collected, exchanged, and transferred within the economic bloc. The framework addresses data privacy of data subjects who are only natural persons involved in trade within the bloc.

The SADC Model Law on Data Protection defines various key terminologies in data protection such as: data subject, data controller, processor, consent, child personal data, processing, protection authority, recipient, sensitive data third party, and cross-border data flow. However, the legislation does not define important concepts such as anonymization, profiling, and personal data breach. As such, the limited scope of application of the framework makes it difficult to fully appreciate data privacy within the economic community and adequately address cross-border transfer and collection of data within the bloc.

Interestingly, from the wording of the framework, its scope is not limited to any particular region, thus portraying a picture of Pan-Africanism in the bloc. That said, it is worth noting that Pan-Africanism in cross-border trade is an ideology that that Africans have a sense common interests, collaboration and brotherhood which aims at promoting sustainable and economic development in the region. Indeed, the SADC Model Law on Data Protection is indigenous in nature as it homegrown to address matters of data protection with a key focus to the African region.

The framework forms soft law for Member states as it seeks to provide a guide on the approach to law-making on data protection just like the OECD Guidelines in Europe. Even though the legislation makes it compulsory for data transfer to only take place between SADC members or non-members with adequate data protection mechanisms, it does not provide the parameters for determination of such level of adequacy mechanisms. Therefore, the law is silent on what can be regarded as adequate data protection measures by member states which makes it ambiguous and subject to inconsistent interpretation by courts, enforcement agencies and traders.

CHALLENGES FACING DATA PRIVACY WITHIN THE AFRICAN REGIONAL ECONOMIC BLOCS

Data privacy within the African regional economic blocs has been marred by myriad of challenges which curtail the efficacious application of the data protection frameworks within the Region. Below are a few challenges:

1. Lack of harmonized data protection laws - The member states of the African regional economic blocs have different legislations which do not correlate with the framework enacted by the economic blocs. This discrepancy in the provisions of the law has led to uneven and inconsistent application of data protection legislation within the blocs. Notably, most of the member states do not have in place data protection laws which has led to further inconsistencies in the application of the data privacy frameworks within the regional blocs.

2. The perception of data protection being a threat to cross-border trade - The notion of data privacy has been viewed as a hindrance to cross border trade due to heavy requirements placed on states as well as states to ensure that the data collected and transferred across borders during trade is protected from any form of infringement. This perception of data privacy being a trade barrier has derailed recognition and appreciation of data privacy within the blocs.

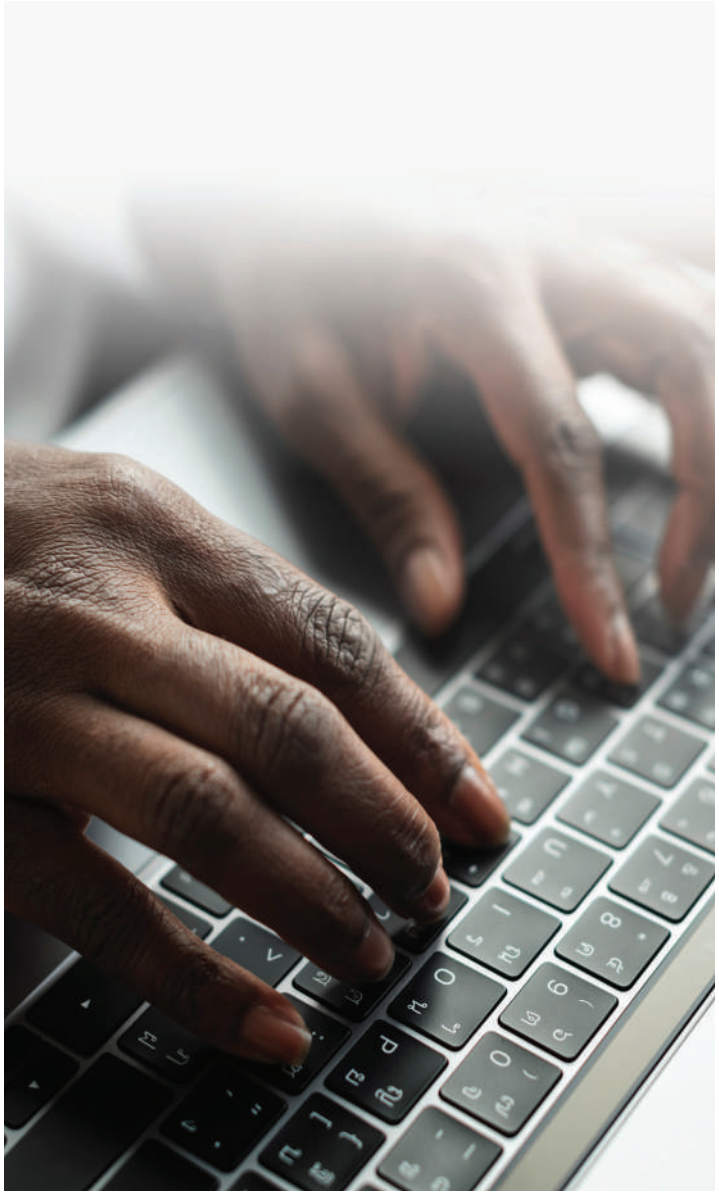
3. Inadequate tech infrastructure - Some of the member states of the African regional economic blocs lack high level tech infrastructure to safeguard data, whereas others are well endowed with tech infrastructure. Such variances may limit the exchange of data, as traders may not be willing to engage in trade with citizens from states where their data is susceptible to breach or infringement.

4. Lack of enforcement of data privacy - The Data privacy frameworks within the African regional economic blocs lack an enforcement agency to enforce their provisions. This has faced a lot of criticism toward the regional economic blocs because they lack enforcement agencies to enforce the provisions of the data privacy frameworks.

5. Lack of goodwill in implementation of the data privacy- of the digital economy which does not have to be perceived as a barrier to trade. By bridging these gaps, African states may be better positioned to take advantage of emerging technologies for instance artificial intelligence which has the potential to bolster trade within the region without compromising on pertinent issues in respect to data privacy and protection.

Conclusion

The digital economy in Africa offers immense potential for economic growth and innovation. However, effective data protection measures are vital to ensure trust, privacy, and the responsible use of personal data. By addressing the challenges, we shall be better positioned to capitalize on the opportunities available for African Staes in the digital economy. African states can foster a robust data protection framework that supports the growth and sustainability



Author Profiles

Alfred Nyaga is a highly skilled and detail-oriented Paralegal based in Kenya, specializing in data protection, privacy, and cyber security. With a keen interest in safeguarding sensitive information in today's digital world, Alfred's expertise lies in providing comprehensive support to legal teams and clients on matters related to data protection and cyber security. His meticulous approach to research and analysis, coupled with his strong knowledge of data protection regulations, ensures that clients receive efficient and effective guidance in navigating the complexities of data privacy laws. Alfred's commitment to staying up to date with the latest developments in cyber security makes him an asset to the firm.

Diana Wariara is a talented Senior Associate based in Kenya. She has a keen interest in cross-border transactions, where she adeptly navigates the complexities of international business law. Diana's proficiency in data protection and privacy adds value to her practice, as she recognizes the significance of safeguarding personal information in an increasingly interconnected world. Her sharp analytical skills and a deep understanding of the evolving regulatory landscape makes her a trusted advisor to her clients.

ASSESSING THE ADEQUACY OF CYBER LAWS AND THE LEGAL FRAMEWORK IN THE EAST AFRICAN COMMUNITY IN ADDRESSING DATA PRIVACY CHALLENGES

By: Vanessa Mugo and Anne Mumbi

Data has become one of the world's most valuable assets with the advancement of technology. Governments, corporations, and other institutions are increasingly analyzing data to improve service delivery and allocation efficiency. It therefore follows that cyber-security concerns are not just the concern of one country but a global problem with many intricate layers, and improving cybersecurity and protection is now a global issue that warrants regional and international involvement. Since cybercriminals frequently operate from nations with lax legislation, restricting efforts to tackling such challenges simply at the national level will not be helpful. This underscores the necessity of addressing and eventually harmonizing the East African Community's (the EAC) legal initiatives addressing cyber-issues, particularly in cybercrimes and cyber-security in light of data privacy concerns.

The position of EAC member states

The EAC, at present is comprises of 7-member states that is: Kenya, Uganda, Tanzania, Rwanda, Burundi, South Sudan and more recently the Democratic Republic of Congo (DRC). The efforts made by these states in addressing data privacy and protection and cyber laws in general varies greatly with the most progressive legislation measures being those in Kenya.
Generally, African countries have had a slow progression in addressing data protection and cybersecurity matters. This could be attributed to several factors, key being the divergent approaches on the concept of the right to privacy in relation to data collection, processing, and usage. The attempt by the African Union (the AU) in addressing this concern was the drafting of AU Convention on Cyber Security and Personal Data Protection (the Malabo Convention), Africa's first international instrument on data protection passed in 2014. However, this failed almost at inception owing to reluctance in ratification. Presently, by May 2023 only 15 states have submitted their ratification to the convention including Rwanda- the only EAC member state to have signed it.

Rationale for harmonization of cyber laws to address data privacy

With the different legal regimes of all member states, it is evident that a harmonized system would be crucial in addressing data privacy challenges in the EAC. The rationale behind the harmonization approach was mainly the increased use of the internet without border restrictions, the cyberspace is virtual and lacks the physicality from which to depict the aspect of territoriality such that no State may claim sovereignty over cyberspace per se.

To this end, there was need for combined efforts in investigating and criminalizing cybercrimes including data privacy violations that could supersede state boundaries and territoriality in the EAC which led to the eventual drafting of the framework for cyberlaws.

EAC Legal Framework for Cyberlaws

The Experience of the East African Community (the Framework) is the guiding framework that was developed in conjunction with the United Nations Conference on Trade and Development (UNCTAD) to address cyber and data collection challenges in the region and to respond to the lacuna in law at the time. The Framework contains several recommendations made to the governments of the member states regarding changing national laws to:

1. Support electronic commerce;
2. Support the use of data security mechanisms;
3. Discourage conduct intended to jeopardize the confidentiality, integrity, and availability of information and communication technologies;
4. Safeguard consumers in an online environment; and
5. safeguard personal privacy.

The recommendations represent both international best practices and were intended to harmonize the legislative reform process among the EAC Partner States.

Implementation of the guiding principles of the Framework

Ultimately, the Framework, though not binding on EAC Member States, has had great influence in the domestic data privacy and protection legislation of the member states. Kenya, Uganda, Tanzania and Rwanda are perhaps the most progressive EAC member states in data protection law with not only data protection legislations but also well set up data protection authorities. Burundi, South Sudan and DRC are yet to adopt data protection legislation. All these States have provisions for the right to privacy in their respective Constitutions that have since been used to bridge this gap. For instance, in DRC, Article 31 of the Constitution protects the right to privacy and the secrecy of correspondence, telecommunications, and any other form of communication and this has in turn been used to protect data subjects though not as effectively as an express legislation for the same would have.

The Framework does not interfere with the use of domestic cybercrime laws but serves as a guide for the member states in coming up with domestic cybercrime legislations. Essentially, this would mean that EAC member states are free to enact legislation to the degree that it falls within the parameters established by the Framework, whether it is to address state-specific cybercrime problems or other issues including data protection and privacy.

Adequacy of the cyberlaw legal framework in addressing data privacy challenges

The point of convergence with regards to data privacy and implementing the Framework is that all Member States in their laws - whether explicitly or under the ambit of the respective constitutions - share consensus that private data should be protected. The legal regimes also, as a matter of public policy, take into consideration social aspects such as children etc.

However, there are challenges, key being the fact that the legal systems of the various States have different laws governing cybercrime. While some states have a dedicated law addressing cybercrime, others rely on provisions from other laws. However, if all Member States were governed by the same law implementation and enforcement would be seamless since most cybercrime acts are cross border in nature.

Further, the member states of the EAC employ two distinct legal systems that is Burundi and Rwanda both adhere to the civil law system, whereas Kenya, Tanzania, and Uganda follow the common law system. Consequently, the region's efforts to harmonize its legal systems have been slowed down in part by the different legal systems.

Also, Member States have been discussing cyber-security and drafted the East African Community Electronic Transactions Bill of 2014 that has not been assented to by the Heads of States of the Partner States. This poses a grave challenge to the cooperation between States to prevent cybercrimes and makes harmonization of laws on cybercrimes difficult.

EAC Framework's Purpose

The EAC Legal Framework for Cyberlaws was developed in collaboration with UNCTAD to address cyber and data collection challenges in the region, with recommendations aimed at supporting electronic commerce, data security, and safeguarding privacy.

Recommendations for Member States

The Framework contains recommendations for EAC member states to adapt their national laws to support electronic commerce, data security, discourage harmful online conduct, safeguard consumers, and protect personal privacy.

Influence on Member States

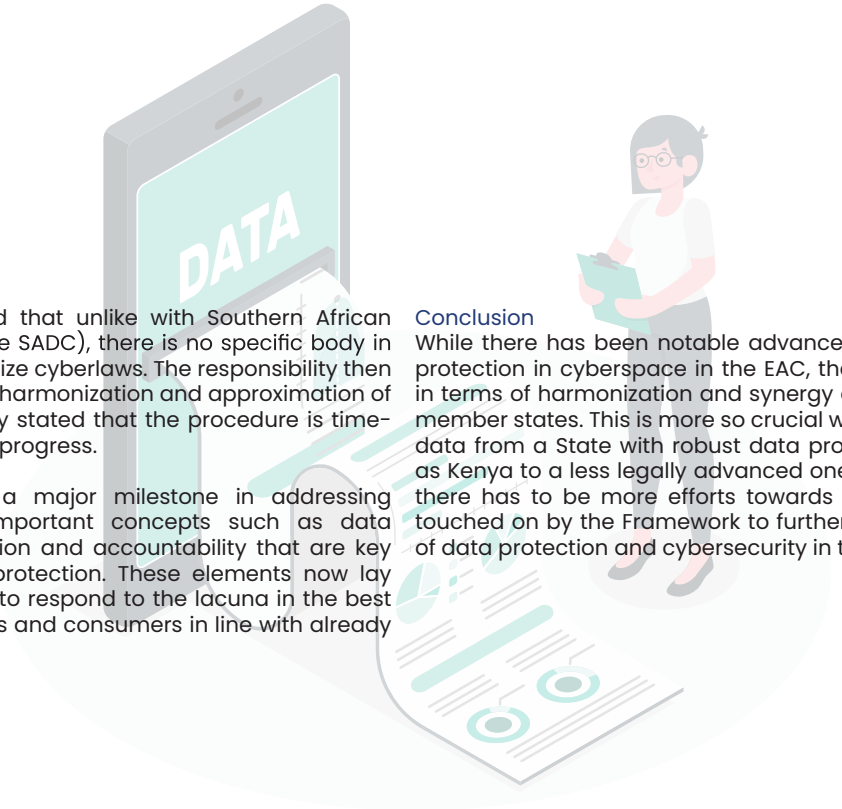
Although not legally binding, the Framework has had a significant impact on domestic data privacy and protection legislation in EAC member states, with Kenya, Uganda, Tanzania, and Rwanda being at the forefront in enacting data protection laws.

Harmonization Challenges

Member states' different legal systems, varying approaches to cybercrime laws, and the absence of a specific body for harmonizing cyberlaws within EAC have posed challenges to achieving uniformity and cooperation in addressing cybercrimes.

Incomplete Framework

While the Framework was a significant step in addressing cyberlaws, it lacks certain crucial elements, such as data minimization, purpose limitation, and accountability, which are fundamental in data privacy and protection. These areas are left to individual states to address within their existing cyberlaws.



It should also be considered that unlike with Southern African Development Community (the SADC), there is no specific body in the EAC mandated to harmonize cyberlaws. The responsibility then falls on the subcommittee on harmonization and approximation of laws, which has unequivocally stated that the procedure is time-consuming thus derailing the progress.

While the Framework was a major milestone in addressing of Cyberlaws, it left out important concepts such as data minimization, purpose limitation and accountability that are key areas in data privacy and protection. These elements now lay squarely on individual states to respond to the lacuna in the best interests of their data subjects and consumers in line with already set cyberlaws.

Conclusion

While there has been notable advancement in data privacy and protection in cyberspace in the EAC, there is still a lot to be done in terms of harmonization and synergy of the legal regimes of the member states. This is more so crucial when it comes to transfer of data from a State with robust data protection mechanisms such as Kenya to a less legally advanced one like South Sudan. Further, there has to be more efforts towards addressing the areas not touched on by the Framework to further advance the progression of data protection and cybersecurity in the future.

Author Profiles

Anne Mumbi is an Associate at the Firm specializing in areas of practice such as corporate, commercial, real estate, intellectual property and private client matters. She has experience in advising local and international clients on corporate and commercial aspect through preparation of commercial benefit agreement, loan agreements and deed of indemnity. Anne also has an interest in drafting articles about current legal affairs in Kenya and advising client on estate planning.

Vanessa Mugo is a Paralegal at FMC and a law school graduate from Africa Nazarene University. She has interests in employment and labor law, commercial transactions, data protection law, and dispute resolution including both ADR and litigation. She has actively assisted clients in coming up with pinpoint data protection and employment policies in conformity to relevant laws in their different lines of service. She is also involved in research work in responding to different clients' needs as they arise especially in relatively novel areas of law including technology and the need for cybersecurity and intellectual property matters.

CROSS BORDER RISKS: EXPLORING DATA TRANSFER FRAMEWORKS WITHIN THE EU AND AFRICA

By Fidel Mwaki & Lewis Ndonga

Data privacy regulation is now a key aspect of international trade and regions. Regions such as the European Union (EU) through its General Data Protection Regulations (the GDPR) have set the benchmark for existing and emerging regional trade association to consider adopting regional data protection frameworks that govern cross border trade within and outside the regional economic zone.

In Africa, data privacy issues are an emerging area. Across the continent, African nations are at various stages of adoption of data privacy laws, with over half the countries having some form of legislation or regulation in place. Notably, in the past five years, a majority of African nations have signed up to an agreement creating an African Continental Free Trade Area (the AfCFTA), which is now recognized as the largest regional single trading bloc in the world (larger than the EU) and spanning over 1.3 billion people, whose objectives include creating a single, liberalized market while reducing barriers to trade and investment in Africa.

As regional trading blocs in the EU and Africa reinforce or accelerate their growth with the rise of digital markets, it is important to consider the impact that data transfer rules within these jurisdictions have when it comes to enabling cross border transactions while protecting individual rights to data privacy and protection.

Africa and the AfCFTA General Exception

AfCFTA is Africa's most significant attempt at a continental trade association, though its implementation has been slow to take off due to a variety of reasons, not least being the uneven rate of economic development among its Member States.

The preamble to the AfCFTA Agreement recognizes the "different levels of development among the Member States and the need to provide flexibility, special and differential treatment and technical assistance to Member States with special needs", thus ensuring that Member States who are still in earlier stages development are not discriminated by any onerous requirements under the AfCFTA Agreement for which they are not ready to comply with.
As digital markets gain traction in intra-African trade, it is important to consider the position of the AfCFTA Agreement in balancing data privacy rights of its citizens with the promotion of free trade amongst Member States.

Firstly, it should be pointed out that the AfCFTA Agreement has no substantive provision on data privacy or protection of individual personal data. Under its Protocol on Trade in Goods, there is hardly a mention of any data privacy obligation, while in contrast the Protocol on Trade in Services briefly sets what is called a "General Exception" under Article 15, providing that:

"...nothing in this Protocol shall be construed to prevent the adoption or enforcement by any State Party of measures: (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Protocol including those relating to: ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

This General Exception grants Member States flexibility to adopt unique internal data privacy laws provided that such laws are consistent with the provisions of the Protocol on Trade in Services under the AfCFTA Agreement, while in addition to the General Exception, Member States that are underdeveloped can rely on the text of the preamble to benefit from the principle of non-discrimination under the AfCFTA.

Secondly, as the 21st century progresses, cross border trade in services is now primarily conducted through digital markets; this a consequence of rapid advancements in technology and supporting infrastructure that has allowed such services to be traded instantly over international digital networks. Africa has not been left behind with many cross-border transactions happening digitally on a daily basis between parties operating in different jurisdictions. While trade in services within the context of AfCFTA remains untapped, it is clear that the current agreement can shape how trade between Member States will occur despite the increasing data privacy risks that are emerging as a result of inconsistent adoption or implementation of enabling legislation across Africa. Ultimately, cross-border transactions may require personal data to be transferred across national borders for legitimate purposes. When you consider Kenyan law as an example, a key aspect of data privacy legislation is the provision on transfer of data outside Kenya.

Under the Data Protection Act (the Kenya DPA), a data controller or processor may only transfer personal data to another country in cases where:

a. *the data controller or processor has given proof to the regulator on the appropriate safeguards with respect to the security and protection of the personal data;*

b. *the data controller or processor has given proof to the regulator of the appropriate safeguards including jurisdictions with commensurate data protection laws; and*

c) the transfer is necessary:

I. for the performance of a contract between the data subject and the data controller;

II. for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another person;

III. for any matter of public interest;

IV. for the establishment, exercise, or defense of a legal claim;

V. in order to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or

VI. for compelling legitimate interests pursued by the data controller or processor not overridden by the interests, rights, and freedoms of the data subjects.

It is therefore clear that for entities operating in Kenya and looking to trade their services across the continent within the framework of AfCFTA, the provisions of the Kenyan DPA create mandatory obligations for them as data controllers and processors to ensure that any personal information shared with parties in other jurisdictions is backed by appropriate safeguards.

In addition, Kenyan entities should ensure that their contractual arrangements consider whether the data protection legislation (if any) in place in the jurisdiction where a counterparty resides is adequate, and if not, then practical or contractual measures may be adopted to ensure protection of personal data transferred to the other Member State, such as:

a. putting in place data protection agreements to govern processing or transfer of personal data between the two entities in different jurisdictions;

b. adopting robust data access and protection clauses as part of the main contractual terms;

c. obtaining legal assurances from the counterparty that they shall manage all personal data in accordance with legal requirements under the Kenyan entity's data privacy laws; and

d. incorporating Kenyan law as the governing law for the contract or ensuring that the Kenyan DPA governs handling of personal data throughout the transaction.

Nonetheless, it is notable that the AfCFTA Agreement does not provide for a harmonized provision on transfer of data, considering the importance of data flows in trade in services in the context of digital markets – a consequence of the nascent nature of AfCFTA as compared to well established regional blocks such as the EU.

The EU GDPR and International Data Transfer Rules

The GDPR has for several years now led the globe in terms of developing standards for managing cross border transfer risks.

At its basic level, the GDPR acknowledges data transfer as necessary for international trade and co-operation. As such, any transfer of data outside the EU must be done in accordance with the GDPR and provide for similar protections as the GDPR. Such transfer also includes any subsequent transfer of data to a third country.

The GDPR provides that transfer of data can only be done under the following circumstances:

1. Adequacy decisions

The EU Commission can make decisions on which jurisdictions have implemented data privacy provisions similar to those provided under the GDPR. Such decisions are known as adequacy decisions. In making adequacy decisions, the Commission must consider the following:

a. the rule of law and effective and enforceable data subject rights;

b. the existence and effective functioning of independent supervisory authorities in the other country with responsibility for enforcing the data protection rules, including adequate enforcement powers; and

c. the other country's international commitments or other obligations arising from legally binding conventions or instruments in relation to the protection of personal data.

As of the date of this piece, the EU Commission has listed the following countries as having adequate protections similar to those provided under the GDPR, namely: Andorra, Argentina; Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the Law Enforcement Directive (LED); and Uruguay. Not a very long list!

2. Appropriate Safeguards

In the event that a country is not considered as having adequate data protection provisions, data transfers can still be done as long as the transferor of data (in this case a data controller or processor) has provided appropriate safeguards to secure any data transferred out of the EU, and on condition that enforceable data subject rights and effective legal remedies are available for data subjects. Such safeguards include:

a. legally binding and enforceable instruments between public authorities or bodies;

b. binding corporate rules – these are data protection policies implemented within a group of entities, one of which located in the EU, that provides for transfer of personal data, including the security of such data. These are particularly important, especially for large conglomerates with their headquarters within the EU and subsidiaries across the world. Having such binding corporate rules is essential in international trade, especially considering the different legal positions across the world on matters data privacy;

c. standard contractual clauses (SCCs) adopted and approved by the Commission – these are pre-approved model data protection clauses that can be adopted by data controllers/processors and provide binding obligations on the data controllers/processors in the other countries with respect to the protection of personal data. Such SCCs make it easier for controllers/processors in countries without robust data protection provisions like those of the EU to transfer data from the EU. In 2021, the EU Commission released the latest version of SCCs relating to the transfer of data.

3. General Exceptions

The GDPR recognizes that not all transfers can be done under the systems stated above. In such a case, data may be transferred outside the EU under the following circumstance:

a. the data subject has explicitly consented to the transfer, having been informed of the possible risks of such transfers;

b. the transfer is necessary for the performance of a contract between the data subject and the controller;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. the transfer is necessary for public interest;

e. the transfer is necessary for the establishment, exercise or defense of legal claims;

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

Conclusion

The European Union is a step ahead in terms of a regional data protection regulation and African nations can benchmark such progress by enacting overarching substantive data privacy regulations for the continent under AfCFTA that can work alongside national legislation to ensure safe transfer of data across borders as intra-African trade takes flight. With trade set to liberalize across Africa in the next decade, it is incumbent upon Member States to fast track the enactment or implementation of data privacy laws across the continent.

Implementation of both regional data privacy frameworks and national laws will ensure that parties can benefit from secure frameworks to allow for smooth and efficient trade within digital markets across the two regional trading blocs.

01 ADEQUACY DECISONS

02 APPROPRIATE SAFEGUARDS

03 GENERAL EXCEPTIONS

Author Profiles

Fidel Mwaki is an Advocate of the High Court of Kenya and member of the Tech Group at FMC Advocates. Frequently, he advises local and foreign clients on the increasing impact of law and technology in their professional and business affairs. Currently, he is focused on supporting clients in understanding the legal and commercial aspects of technology infrastructure, data privacy, cybercrime, communications and media, technological innovations, and intellectual property to ensure that their investments are well structured and add value their long-term business goals.

Lewis Ndonga is an Advocate at FMC, with particular interest in tech and data protection law. He has advised clients on several matters within this space, including data privacy compliance, tech contracts such as IT services consultancy contracts and non-disclosure, cross-border transfer of data, including the transfer of sensitive personal data and data privacy obligations of international entities based in Kenya. He firmly believes in the use of the law to support technological innovation and lends his talents to advising clients on the same. He has a keen interest in cutting-edge innovations, data privacy, and emerging digital trends which drives him to stay at the forefront of legal developments. His diverse experience enables him to offer comprehensive counsel to tech companies, startups, and individuals alike, ensuring their interests are protected in an ever-evolving technological landscape.

INTERESTING DEVELOPMENTS IN EU-US DATA TRANSFER REGULATION

By Lewis Ndonga

The EU and the US are two of the strongest economic powerhouses in the world.

The 27 EU countries account for about 14% of the world's trade in goods. On the other hand, the US boasts of around 7 trillion USD in exports and imports of goods and services in 2022. Nonetheless, the two giants have opposing views regarding the flow of data and data privacy. The EU favours a strict data privacy approach, where personal data belonging to persons in the EU is secured under frameworks such as the GDPR, where the obligations of bodies (including public bodies) with respect to individual's data are specified. The US favours a free flow of information, particularly for the justification of national security and public interest.

This makes international trade between the two a tight rope to walk on.

Nonetheless, the two have recognized the importance of co-operation and have entered into various frameworks to support the transfer of data.

Developments in Data Transfer Regulation

1. The EU-US Data Privacy Shield

The EU-US Privacy Shield was set up by the US. Department of Commerce to allow for the transfer of data from the EU to the US. This was particularly important considering the presence of US-based social media giants within the EU such as Meta (previously Facebook).

The principles of the Privacy Shield were developed to facilitate trade and commerce between the US and the EU.

The Privacy Shield is a voluntary endeavor, with organizations having to join and declare their commitment to comply with the principles of the Privacy Shield. The US Federal Trade Commission is the regulatory authority tasked with ensuring compliance with the principles of the Privacy Shield. These principles include:

a. **Notice** – organizations under the Privacy Shield are obliged to notify individuals of their involvement in the Privacy Shield, the kind of personal data collected, the organization's commitment to comply with the Principles with respect to data received from the EU, the purposes for which the organization collects and uses personal data, contact information and complaint mechanisms, the type or identity of third parties to which the organization discloses personal information, and the purposes for which it does so, the right of individuals to access their personal data, the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual among others.

b. **Choice** - organizations under the Privacy Shield must allow individuals to opt out where their personal information is to be disclosed to a third party or to be used for a materially different purpose. Such choice must be clear, conspicuous, and readily available For instances of sensitive information such as personal information specifying medical or health conditions, racial or ethnic origin, etc., organizations must obtain affirmative express consent from individuals if such information is to be disclosed to a third party or to be used for a different purpose.

c. **Security** – organizations must ensure that reasonable and appropriate measures are taken to protect personal data from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

d. **Purpose limitation** – the processing of personal information must be limited to the information that is relevant for the purposes of processing. Organizations are not allowed to derogate from the original authorized purpose.

On 12th July 2016, the EU Commission validated the Privacy Shield through its adequacy decision. Until 2020, the Privacy Shield was the go-to framework to support transfer of data outside of the EU.

2. The Schrems II Decision

EU activist Max Schrems called for the invalidation of the Privacy Shield by the Irish Data Protection Commissioner and asked for the transfer of information from the EU to the US by the social media company Facebook (now Meta) to be stopped. In 2020, The Court of Justice of the European Union (**the CJEU**) was called upon to determine the matter. In a decision now known as the Schrems II, the CJEU invalidated the Privacy Shield, with the court stating that the US government still maintained a high level of surveillance under US laws. Such laws do not adequately protect EU data subjects whose information is being transferred to the US from national security agencies.

The CJEU found that the US laws do not satisfy the adequacy requirements that protections in other countries should be essentially equivalent to the protections under the GDPR. Furthermore, the CJEU highlighted that there were no sufficient remedies before a properly established judicial body within US law to which any guarantees with respect to data safety would be enforced.

3. The Trans-Atlantic Data Privacy Framework.

It has been recently announced that the US and the EU are currently developing the Trans-Atlantic Data Privacy Framework, which would essentially allow for cross-border data transfer between the two. While the framework has not been published, the factsheet for the same gives us the following key takeaways:

- The Trans-Atlantic Data Privacy Framework intends on limiting the access by US intelligence agencies by limiting the same to what is necessary and legitimate;
- Strong obligations on companies collecting data from the EU, continuing the practice of self-certification with the US. Department of Commerce; and
- Very importantly, establishing a two-tier dispute resolution mechanism for enforcing data subject rights, including the establishment of the Data Protection Review Court in the US.

The Trans-Atlantic Data Privacy Framework seems to take heed to the Schrems II decision, and the EU-US trade systems continue to remain in limbo as the framework is being prepared. Multinational companies find themselves in a sticky situation where their business is inherently intertwined with data transfer out of the EU. Currently, majority of the organizations are left to take advantage of the other safeguard mechanisms such as SCCs and binding corporate rules.

ENHANCING CROSS-BORDER DATA SECURITY: THE OFFICE OF DATA PROTECTION COMMISSIONER'S REGULATORY MEASURES IN KENYA

By: Lyne Achieno

We are now living in an era where data is the new gold and everybody wants their data protected and not made available to every Tom, Dick and Harry. The Constitution of Kenya, 2010 guarantees the right to privacy as a fundamental right for every Kenyan, the Data Protection Act 2019 (the Act) has since been enacted and various regulations have since been published to operationalize the provisions of the Act. Towards implementation of the Act, the Office of the Data Protection Commissioner (the ODPC) was set up and appointment of Data Protection Commissioner.

The steps taken by the ODPC in safeguarding the transfer of data outside Kenya

Data protection involves safeguarding personal information, in accordance with a set of principles laid down by law. One of the principles of data protection set out by the Act is that every data controller or data processor shall ensure that personal data is not transferred outside Kenya, unless there is proof of adequate data protection safeguards or the consent from the data subject.
The ODPC, in carrying out its mandate in ensuring protection of information transferred out of Kenya provides for the following bases for the transfer of personal data outside Kenya;

1. Transfer based on consent

Consent is an essential element of data protection legislation and principles. Data controllers and data processors are required to obtain prior consent for the collection, use and disclosure of personal data. The ODPC Guidance Note on Consent defines consent as any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to data subject. Consent must meet the minimum criteria as defined.
Consequently, the Data Protection (General) Regulations, 2021 (the Regulations) requires the data subject's consent to the transfer of their personal data to a recipient outside Kenya. However, prior to the data subject issuing their consent, the data subject must be duly informed of the safeguards and risks involved in cross-border transfer of their personal data. Therefore, the data subject should be well informed by the transferring entity prior to consenting to the transfer. Where the consent is obtained by providing false or misleading information or any using other deceptive or misleading practices in relation to the transfer, the transferring entity commits an offence and shall be liable to a fine not exceeding K.Shs.3,000,000/= or an imprisonment term not exceeding 10 years or both.
Crucially, a data subject has a right to withdraw consent from the processing of their data and the transfer of the data subject's data should cease once they withdraw their consent.

2. Appropriate Data Protection Safeguards

The transfer limitation principle provides that personal data should not be transferred outside Kenya unless there is sufficient proof of adequate protection safeguards or consent from the data subject. The Act, gives effect to the limitation principle, and states that a data controller or data processor may transfer personal data to another country where;

a. the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data; and

b. the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data and the appropriate safeguards including jurisdictions with commensurate data protection law.

Any country or a territory is taken to have such safeguards if that country or territory has-

a. ratified the African Union Convention on Cyber Security and Personal Data Protection.

b. reciprocal data protection law with Kenya.

c. an adequate data protection law as shall be determined by the Data Commissioner.

3. Transfer based on Necessity

Transfer is necessary if:

a. it could be for a performance and conclusion of contract;

b. for any matter of public interest;

c. establishment, exercise or defence of a legal claim;

d. to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consents; or

e. the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

4. Transfer based on Adequacy Decision

The Data Commissioner in making decisions in regards to transfer requires that the data controller or data processor shows the effectiveness of the security safeguards and makes informed decision based on the proof provided. Determination on adequacy is based on confirmation that the recipient country or organization has in place adequate level of protection and the ODPC may publish a list of approved countries and organizations.
The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

Means of enforcement by the ODPC

The Act clearly provides for the protection of data transferred out of Kenya, it further provides for how the right of a data subject can be enforced, where a person can lodge either orally or in written form a complaint under the Act. Therefore, for instance if a data subject's consent was not given prior to the transfer of information, the person may lodge a complaint against the transferring entity. The Data Commissioner will conduct an investigation and if satisfied that an entity has failed or is failing to comply with the provisions of the Act, issue an enforcement notice.
Failure to comply with the provisions of the Act and the Regulations attracts the issuance of enforcement notice from the ODPC; the notice is served upon a non-compliant entity requiring the entity to take steps or measures to remedy the situation within a specified period of time of not less than twenty-one days.
Failure to comply with an enforcement notice without a reasonable excuse will attract a penalty notice, through which a penalty will be imposed. The penalties under the Act and the Regulations includes both fines and prison terms.
The Data Protection (Complaints Handling and Enforcement) Regulations, 2021 promotes Alternative Dispute Resolution (ADR) through negotiation, mediation or conciliation. Where a dispute is determined through ADR, the parties must sign a binding agreement in a prescribed form which will be deemed to be a determination of the Data Commissioner.

Conclusion

There are well established regulations governing transfer of personal data outside Kenya and the enforcement mechanisms put in place however there is still a gap when it comes to enforcement, what happens to information that is transferred out that breaches the principles of privacy of a data subject, when the non-compliant entity does take any measures or steps to remedy the situation and as a result it is fined, still the data subject will be affected. Also, when the non-complaint entity is fined by the ODPC who should receive the fine, is it the aggrieved data subject or ODPC? The ODPC needs to have international regulatory and supervisory authorities to deal with enforcing the transfer of data outside Kenya and have better streamlined policies that protect Kenyans.

THE INTERPLAY OF FREE CROSS BORDER DATA FLOW AND DATA PRIVACY IN INTERNATIONAL TRADE: A KENYAN PERSPECTIVE

By: Paula Kilusi

In our increasingly interconnected digital world, the exchange of data across borders has become a cornerstone of global trade and economic growth. Kenya, as a vibrant emerging economy and a hub for technological innovation in Africa, actively participates in international trade, relying on the free flow of data. However, alongside the benefits of data exchange, concerns about data privacy have gained prominence.

This article examines the relationship between free cross-border data flow and data privacy in Kenya, exploring the challenges and opportunities faced by businesses, policymakers, and individuals. By analyzing the impact of data privacy regulations on international trade, we aim to propose strategies to strike a balance between these interests, offering insights to navigate Kenya's evolving digital landscape.

Importance of Free Cross Border Data Flow

Free cross-border data flow refers to the unrestricted movement of data across national borders without unnecessary barriers or restrictions. This open exchange of data brings several benefits:

1. **Economic growth and innovation**: Free data flows foster economic growth and drive innovation by enabling businesses to access global markets, collaborate with international partners, and leverage data-driven technologies. It allows companies to expand their customer base, enter new markets, and create new products and services.
2. **Enhanced productivity and efficiency**: Cross-border data flow enables seamless communication, collaboration, and information sharing among businesses, leading to increased productivity and operational efficiency. It allows companies to access global talent pools, leverage cloud computing services, and utilize data analytics to improve decision-making and optimize processes.
3. **Market expansion and diversification**: Free data flows remove geographic barriers and enable businesses to reach customers beyond their domestic markets. This opens up opportunities for small and medium-sized enterprises (SMEs) to compete globally, expand their customer base, and diversify their revenue streams.
4. **Access to information and knowledge**: Free cross-border data flow facilitates the exchange of information, ideas, and knowledge across borders. It enables individuals, businesses, and governments to access a vast pool of resources, educational materials, research, and best practices from around the world.

This unrestricted access to information promotes learning, innovation, and continuous improvement.

Free cross-border data flow plays a vital role in facilitating international trade by enabling seamless digital transactions, reducing trade barriers, and fostering global connectivity. Here are some key aspects of how it facilitates international trade:

a. **E-commerce and digital trade**: Cross-border data flows are crucial for e-commerce and digital trade, allowing businesses to engage in online sales, marketing, and distribution across borders. It enables consumers to access a wide range of products and services from different countries, contributing to increased trade volumes and market opportunities.

b. **Supply chain integration**: Cross-border data flows help integrate global supply chains by enabling real-time tracking and sharing of information related to production, inventory, logistics, and customer demand. This improves supply chain visibility, efficiency, and responsiveness, ultimately benefiting international trade.

c. **Trade in services**: Many services, such as telecommunications, financial services, software development, consulting, and creative industries, heavily rely on cross-border data flows. Access to global markets and the ability to provide services remotely are facilitated by free data flows, promoting trade in services and creating new business opportunities.

d. **Market research and analysis**: Cross-border data flows enable businesses to gather market intelligence, analyze consumer preferences, and tailor their products and services to specific markets. This helps companies make informed decisions and develop effective market entry strategies, thereby supporting international trade.

The Significance of Data Privacy

The significance of data privacy is recognized and protected through various laws and regulations. The country has established a robust legal framework to safeguard the privacy and protection of personal data, ensuring individuals have control over their personal information.

At the international level, Kenya has ratified the International Covenant on Civil and Political Rights (ICCPR), which acknowledges the right to privacy under Article 17. This commitment highlights the importance of protecting individuals' privacy rights and ensuring they are not subject to arbitrary interference.

On the national front, Kenya enacted the Data Protection Act of 2019 alongside the Data Protection Regulations 2022 which provide a comprehensive framework for the protection of personal data and privacy. This legislation establishes the Office of the Data Protection Commissioner as an independent regulatory authority responsible for overseeing compliance with data protection regulations and addressing data breaches. The Data Protection Act regulates the collection, processing, storage, and transfer of personal data, emphasizing the importance of obtaining consent and implementing appropriate security measures.

Additionally, Kenya has actively participated in regional initiatives and agreements to promote data protection and privacy. As a member of the African Union (AU), Kenya has adopted the Malabo Convention on Cyber Security and Personal Data Protection. This convention establishes substantive provisions for data protection that member states, including Kenya, must adhere to, further reinforcing data privacy standards.

Impacts on International Trade

Data privacy regulations can create trade-offs and challenges for international trade in Kenya. While protecting individuals' privacy and personal data is essential, it can sometimes clash with the free flow of data across borders, impacting trade and economic activities. Here are some key considerations:

1. **Impediments to Cross-Border Data Flows**:
- Stricter data privacy regulations may impose restrictions on cross-border data transfers, requiring companies to comply with additional requirements or obtain specific authorizations, which can increase costs and administrative burdens.
- Data localization requirements, mandating that data be stored within national borders, can limit the efficiency of cross-border data flows and hinder the operations of multinational companies.

2. **Impact on Digital Trade and Services**:
- Data-driven digital trade, including e-commerce, cloud computing, and online services, relies heavily on the seamless flow of data across borders. Data privacy regulations that restrict cross-border data transfers can impede the growth and development of these sectors.
- Small and medium-sized enterprises (SMEs) that engage in digital trade may face significant compliance costs and challenges in adhering to multiple data privacy regimes when expanding their operations internationally.

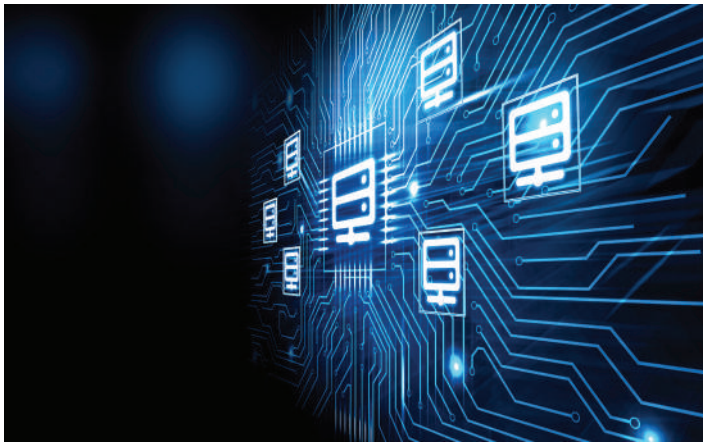
3. **Potential Barriers to Global Supply Chains**:
- Data privacy regulations that require specific safeguards for data transfers can disrupt global supply chains, especially in sectors relying on real-time data exchange or sharing sensitive information across borders.
- Compliance with varying privacy standards in different jurisdictions can create complexities for businesses involved in international trade, leading to delays, higher costs, and potential conflicts between regulatory requirements.

4. **Balancing Privacy and Economic Growth**:
- Striking the right balance between protecting privacy and fostering economic growth is crucial. While robust data privacy regulations are necessary to safeguard individuals' rights, overly restrictive measures can hinder innovation, digital transformation, and international competitiveness.
- It is essential for policymakers to carefully design data privacy frameworks that not only protect personal data but also support trade and economic development by promoting trust, security, and responsible data practices.

Finding the right equilibrium between data privacy and international trade requires a comprehensive approach that considers both the protection of personal data and the facilitation of cross-border data flows. Policymakers, businesses, and other stakeholders should engage in ongoing discussions and collaboration to develop solutions that address privacy concerns while promoting an enabling environment for international trade.

Balancing Free Cross Border Data Flow and Data Privacy in Kenya

There can be potential conflicts between the principles of free cross-border data flow and data privacy. The desire to promote the seamless flow of data across borders for economic growth and innovation must be balanced with the need to protect individuals' privacy and ensure the responsible handling of personal data.
One conflict arises from the risk of data breaches and unauthorized access to personal information when data is transferred across borders. Free data flow can increase the exposure of personal data to foreign jurisdictions with different data protection standards, potentially compromising individuals' privacy and data security.



Additionally, the free flow of data may pose challenges in enforcing local data protection laws. When personal data is transferred outside Kenya, it may become subject to different legal frameworks, making it difficult for Kenyan authorities to ensure compliance and protect individuals' privacy rights.
Balancing free cross-border data flow and data privacy requires careful consideration of various factors. Some challenges and considerations include:

1. Harmonization of data protection laws: Aligning Kenyan data protection laws with international standards facilitates cross-border data transfers while ensuring privacy. For example, the General Data Protection Regulation (GDPR) in the European Union serves as a benchmark for many countries globally.
2. International cooperation: Collaborating with other countries and organizations addresses challenges in cross-border data transfers. Examples include bilateral data transfer agreements, such as the EU-Japan Adequacy Decision, which allows data to flow freely between the European Union and Japan.
3. Technological advancements: Keeping pace with evolving technologies is crucial. Kenya must update policies to address new privacy risks posed by artificial intelligence, big data analytics, and the Internet of Things. For instance, the Singapore Personal Data Protection Commission issues guidelines on the responsible use of artificial intelligence.
4. Public awareness and education: Enhancing awareness about data privacy rights and responsible data handling is vital. For example, campaigns like "Stay Smart Online" in Australia educate individuals and businesses about online privacy and security.

By addressing these challenges and considerations, Kenya can strike a balance between facilitating free cross-border data flow for economic growth and safeguarding individuals' privacy rights, creating an environment that fosters innovation while protecting personal data.

Potential Solutions and Recommendations

In order to strike a balance between free cross-border data flow and data privacy in Kenya, several strategies and recommendations can be pursued.

Firstly, harmonizing data protection laws with international frameworks such as the General Data Protection Regulation (GDPR) and regional agreements like the East African Community Data Protection Bill can facilitate the smooth transfer of data across borders while ensuring consistent privacy standards.

Additionally, seeking adequacy decisions with other countries or regions can demonstrate that Kenya's data protection standards are equivalent to international counterparts, allowing for the free flow of personal data while upholding privacy safeguards. It is essential to develop robust data protection mechanisms through comprehensive legislation, enforcement mechanisms, and regulatory oversight to enhance privacy rights without impeding international trade. This includes establishing clear guidelines on lawful data processing, data breach notifications, and individual rights to maintain a balance between privacy and trade.

The EAC Legal Framework for Cyberlaws was developed in collaboration with UNCTAD to address cyber and data collection challenges in the region, with recommendations aimed at supporting electronic commerce, data security, and safeguarding privacy.

The EAC Legal Framework for Cyberlaws was developed in collaboration with UNCTAD to address cyber and data collection challenges in the region, with recommendations aimed at supporting electronic commerce, data security, and safeguarding privacy.

The EAC Legal Framework for Cyberlaws was developed in collaboration with UNCTAD to address cyber and data collection challenges in the region, with recommendations aimed at supporting electronic commerce, data security, and safeguarding privacy.

Examining international frameworks and agreements can guide Kenya's approach towards reconciling these two objectives. The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data offer valuable principles and recommendations that can inform Kenya's data protection strategies.
Exploring cross-border data transfer mechanisms like standard contractual clauses and binding corporate rules, which are recognized globally, can facilitate secure and lawful cross-border data transfers while upholding privacy standards.

Furthermore, leveraging regional integration efforts, such as the African Union's Malabo Convention and the African Continental Free Trade Area (AfCFTA), can help harmonize data protection regulations across African countries, promoting a unified approach to data privacy and facilitating trade across borders.

To effectively implement these strategies, recommendations for policymakers, businesses, and other stakeholders are crucial.

- Policymakers should ensure the development and implementation of robust data protection laws and regulations that strike a balance between privacy and trade. They should also foster dialogue with international counterparts to establish mutual recognition of data protection standards and promote cross-border data flows.
- Businesses must invest in data protection measures and compliance frameworks to adhere to privacy regulations while maintaining their international trade operations. They should adopt privacy-by-design principles, embedding privacy considerations into products, services, and data management practices.
- Stakeholder collaboration, including public-private partnerships, can facilitate knowledge sharing, best practices, and capacity building on data protection and international trade. Collaboration between government, industry associations, and civil society is essential to develop industry-specific guidelines that address both privacy and trade requirements. Public awareness and education campaigns should be conducted to educate individuals about their privacy rights, the importance of data protection, and the benefits of international trade. Promoting privacy-conscious behavior among individuals, businesses, and organizations is crucial to ensure responsible data practices.

By implementing these strategies and recommendations, Kenya can create an environment that upholds data privacy rights while facilitating free cross-border data flow, thereby supporting both data-driven international trade and the protection of personal data.

Conclusion

To reconcile free cross-border data flow and data privacy in Kenya, a multi-faceted approach is essential. This includes adopting technological solutions, engaging in international frameworks, and establishing robust data protection policies. By finding a harmonious balance, Kenya can protect individuals' rights, promote trade, and fuel innovation in the digital age.

By adopting technological solutions such as data anonymization and encryption, Kenya can protect personal information while facilitating the flow of data across borders. This ensures privacy while enabling seamless data exchange. Active engagement in international frameworks and agreements, such as the East African Community (EAC) and adherence to global standards like the General Data Protection Regulation (GDPR), ensures consistency with international data practices. This fosters trust and compatibility in cross-border data transfers.

Establishing robust data protection policies requires collaboration among policymakers, businesses, and stakeholders. Clear guidelines on data handling, transparency, and mechanisms for individuals to exercise their data rights are essential. Prioritizing data protection creates an environment that upholds privacy rights and supports international trade.

By striking a harmonious balance between free cross-border data flow and data privacy, Kenya safeguards personal information, promotes trade, and drives economic growth. This approach fosters innovation and positions Kenya as a trusted participant in the global digital economy.

Author Profile

Paula Kilusi is a dynamic and passionate law student at the University of Nairobi, with a keen interest in tech law, employment law, and corporate law. As an active member of the Young Arbiters Society and student member of the Women in ADR committee, Paula is committed to promoting alternative dispute resolution methods. She is also an Associate Editor at the University of Nairobi Law Journal, where she has honed her legal writing skills. With a strong desire to learn and grow, Paula is enthusiastic about exploring new legal areas and expanding her expertise. She can be reached at kilusipaula@gmail.com for any inquiries.

ADVOCATES

SCAN ME

GET IN TOUCH

FMC ADVOCATES
Kalson Towers
2nd Floor, Left Wing
The Crescent ,Off Parklands Road Westlands
Nairobi-Kenya
0725 762 784
consult@fmcadvocates.com
www.fmcadvocates.com