POLICY BRIEF

Data Protection Legal Regime and Data Governance in Africa: An Overview

Olumide Babalola

February 2022 / No.DG003

1. Context

Legal regime of data protection and data governance in Africa

There has been a spike in the processing of personal data across the world and this has led to the need to regulate dealings with information through the creation of legal frameworks. Sadly, Africa, unlike other regions, has been unable to engineer a formidable legal framework for the harmonization data protection enforcement. In other cases where it appears there are legal frameworks for data protection, it efficiency has not been maximized.

The problem

Data protection and data governance in Africa

While it is conceivable that African countries have made effort to enact legal framework for data protection and data governance due to the increased use of personal data, compared to the EU General Data Protection Regulation (GDPR), the African Union does not have a central legislation that generally regulates the concept of data protection its member states. The existing instrument (Malabo Convention) that appears pan-African is not yet enforceable due to non-ratification by the required number of member states.

This research analyses the provisions, efficiency, compliance and enforceability of data protection laws in Africa in relation to data governance. It concludes on the necessity of legal frameworks for data protection and some recommendations that could be adopted to develop new or strengthen existing data protection framework within the context of data governance.

The background

Africa does not have a single comprehensive data protection framework that is applicable to all its countries without ratification. Where there is a semblance of these laws, there is lack of institutional enforcement on one hand and adequacy of such frameworks on the other. Some of them are analysed below.

African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention)

The Malabo Convention is Africa's first international instrument on data protection which was passed in 2014. The Convention seeks to, among other objectives, harmonize the laws of member states on data protection and encourage member states to create frameworks to protect personal data within the continent.

Unfortunately, the adequacy of the Convention may be questioned as it left out the definition of important concepts such as pseudonymization; data protection authority; and cross-border processing, or the right to lodge complaint with regulator, right to data portability, restriction of further processes by the data subject. This omission may engender conceptual confusion especially in cross-border enforcement situations.

The convention does not provide a definition of what constitutes 'automated' or non-automated processing, and such omission is tricky given the constant rise in

profiling and automated decision making in Africa. Also, contrary to the provisions of the Convention, only 28 of the 30 countries with data protection laws in Africa have data protection authorities (DPAs). The convention contains only six re-phrased data protection principles with some difference from the universally recognized principles.

Supplementary Act on Personal Data Protection within the ECOWAS (ECOWAS ACT)

The Economic Community of West African States (ECOWAS) was established for the promotion of regional cooperation among member states especially for economic growth. The Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS (the Act) was passed in 2010 to regulate data protection within the member states.

The Act also omits important terminologies like processing; pseudonymization; personal data breach; cross border transfer etc, and rights to lodge complaint with regulator, right to data portability, etc. This omission may have far-reaching consequences when the Act is invoked to settle issues relating to transborder processing of data and questions of conflict of decisions on lead national DPAs.

The Act restricts transfer of personal data outside ECOWAS sub-region to only countries where there is an adequate level of protection for fundamental rights and freedoms but does not provide mechanisms for regulating such transfers.

Southern African Development Community (SADC) Model Law on data protection

The increasing need to create a harmonized set of policies for the information communication technology industry for the Sub-Saharan countries in the group of African, Caribbean, and Pacific states spurred the enactment of the Southern African Development Community (SADC) Model Law on Data Protection in 2013.

Like other African legislation on the subject, the law does not define important concepts like pseudonymization, data subject, access, and request, etc. Surprisingly, from the wording of the law, its scope is not limited to any region and this gives the picture of a Pan-African guide. However, the document is a soft law without a legally binding effect on member states but they only provide a guide on the approach to law-making on data protection.

Although the law makes it compulsory for data transfer to only take place between SADC members or non-members with adequate data mechanisms, it does not provide the parameters for determination of such level of adequacy.

East African Community (EAC) Legal Framework for Cyberlaws 2008

The East African Community (EAC) Legal Framework for Cyberlaws was recommended with the main objective of developing policies facilitating cooperation between member states.

However, it omitted important concepts such as data minimization, purpose limitation and accountability etc. While giving kudos to its progressive provisions on data protection, those are however non-binding on member States as they only offer guidance. It is however worthy of note that the framework remotely or otherwise influenced the data protection legislation in Kenya, Uganda and Rwanda which passed the legislation afterwards.

Research results

Data protection itself is directly linked with Data governance. Data governance relates to the collection and management of data which ensures effective and efficient use for the overall productivity of an entity. Data protection on the other hand, safeguards the collected personal data from misuse, and/or corruption within the confines of certain principles.

When the data governance is airtight, data protection would not be far behind. Earlier in this brief, we have demonstrated the inadequacies of data protection framework in Africa, hence, there is no gain saying that data governance on the continent needs some fine-tuning. This section of this research aims to identify legal principles for the effective protection of personal data and the gains of a formidable data governance ecosystem on the continent.

Accuracy

The principle of accuracy enforces the accuracy, completeness, and consistency of personal data. Under this principle, organizations (private and public) are duty bound to ensure the accuracy of information they keep and opinions that they express regarding data subjects especially when such decisions affect the latter.

Storage limitation

Storage of data is one of the main components of data governance. Sometimes, information are stored indefinitely in unregulated and unguarded databases without the consent of data subjects. Essentially, personal data must not be kept in a form that identifies data subjects for longer than is justifiable by law.

Accountability

The principle principally requires legal entities to acknowledge and assume liability for their operations on personal data in the course of the organizational activities. Data controllers have the bounden duty of demonstrating adequate technical and organizational measures to secure data in compliance with the relevant data protection legislation for the ultimate protection of data subjects rights.

Confidentiality and integrity

This principle simply mandates organizations processing personal data to employ appropriate measures to protect such personal information from misappropriation, corruption, theft and/or destruction. Confidentiality in this sense, speaks to the duty of the organization handling data to ensure that such information are not shared or exposed to unintended persons.

Privacy right guarantees

Privacy cannot be separated from data protection as the latter originated from the former. A formidable legal framework for data protection would guarantee data subjects' privacy and ensure considerable control over their personal information, deepening consumers' trust in processing activities.

Healthy democracy

A healthy democratic state is one in which its citizens can make informed and autonomous choices especially with respect to their personal data. Effective data protection laws ensures consent. Where there is no consent then processing of data is in line with the notion of data subjects' rights and the transparency, fairness and accountability obligations. Thus, it is safe to conclude that a world where data protection is respected is one in which the seeds of corporate or governmental totalitarianism cannot flourish.

Economic gains from free flow of data

The concept of free flow is not merely restricted to cross jurisdictional data transfers but also instances where there are legal barriers that do not impose data localization requirements. Data localization requirements have the direct effect of raising the costs for doing business across jurisdictions. Implementing an African data protection framework for the free flow of data may create an opportunity for African countries having an adequate level of data protection.

Implications for policy makers

African currently has only one binding regional instrument - ECOWAS Supplementary Act on Data Protection. Out of 55 African countries, only 30 have fully dedicated data protection laws, and less than 28 of them have established DPAs to enforce compliance with the laws. Hence it is clear that, data governance on the continent remains largely unsupported by legislative and enforcement framework.

For a properly regulated data governance, it is hoped that African countries would evenly ratify the Malabo Convention. The transborder cooperation of national DPAs envisaged by the regional treaties ought to be encouraged and strengthened to boost enforcement of regional and municipal data protection laws.

Mission

To strengthen local capacity for conducting independent, rigorous inquiry into the problems facing the management of economies in sub-Saharan Africa.

The mission rests on two basic premises: that development is more likely to occur where there is sustained sound management of the economy, and that such management is more likely to happen where there is an active, well-informed group of locally based professional economists to conduct policy-relevant research.

www.aercafrica.org

Learn More

www.facebook.com/aercafrica

www.instagram.com/aercafrica_official/

twitter.com/aercafrica

www.linkedin.com/school/aercafrica/

Contact Us
African Economic Research Consortium
Consortium pour la Recherche Economique en Afrique
Middle East Bank Towers,
3rd Floor, Jakaya Kikwete Road
Nairobi 00200, Kenya
Tel: +254 (0) 20 273 4150
communications@aercafrica.org