

# POLICY BRIEF

By: Kunle Balogun and Adedeji Adeniran


June 2024

## Towards A Sustainable Regional Data Governance Model In Africa



### Preamble

Data governance has emerged as a central tenet for countries, not only to realise the benefits of digital revolution but also to mitigate the growing risks and threats that emanate from the digital space. Over the last decade, the number of African countries with at least a form of data protection/regulation policy has increased from 12 in 2012 to 36 in 2024. However, the national approach to data governance has its limits, particularly in African countries with low digital development and a high dominance of global digital platform firms.



A regional approach to data governance can address the power imbalances between individual countries and highly resourced digital firms. The regional approach additionally ensures resource pooling and knowledge sharing, creating an institutional framework to support compliance data policies.

In 2022, Africa introduced a regional data governance model with the approval of the AU Data Policy. The policy puts in place a coordinating framework for data protection, cross-border sharing of critical data, and other elements to facilitate the digital revolution on the continent.

With the regional approach in place, the question becomes how to effectively mainstream the framework at a national level in order to avoid friction and to promote synergy rather than undermining the existing national data governance efforts. According to [CIPESA \(2023\)](#), the proposed regional framework is likely to face inherent integration problems within the continent as a result of inward-looking and sovereignty concerns that have previously delayed other AU initiatives.

Given the enormous benefits of a regional approach, this brief recommends some proactive measures that could be introduced to integrate the regional data governance model with national data policy priorities. The concept is that the regional strategy is not superior to the national approach or vice versa, but that national data policies provide value and are more effective when they complement the regional approaches.

## Why National Data Policy Varies

While African countries have similar data governance issues such as data protection and privacy, data sovereignty and security, cross-border data flow, and data localisation procedure; the majority have interestingly diverse national data governance approaches to data localisation. While Rwanda, Zambia, and Zimbabwe use cyber security and cybercrimes legislation to place restrictions on cross-border data transfer, others use financial services (Nigeria and Ethiopia), telecom (Cameroon) and data protection (Kenya, South Africa, Tunisia and Uganda). On the other hand, countries like Mauritius restrict the exporting of specified data without strict authorisation. For example, Kenya prohibits the export of all public data without authorisation; Zimbabwe, Malawi, and Tunisia require personal information; Nigeria mentions all government, subscribers, and consumers data and Sierra Leone restricts the exportation of subscriber registration information.



National data policy varies for different reasons , including the following:

● **Governance system:** Non-democratic and authoritarian regimes are more restrictive on data flows, as national security weighs more in decision-making. This reflects the reality at the global level and is evident in the models adopted by the China, US, and EU governance systems.

● **Global influence:** Key players in the digital space (sovereign and business entities) have a marked influence on national policies in terms of exemptions and coverage. Many African countries have modelled their data governance policies around the EU's General Data Protection Regulation. Such influences can shape the data governance approach at the individual level. Other external influences can come from the existing bilateral trade and data-sharing agreements among countries, which also affect local data governance frameworks.

## The need for a complementary but not uniform approach

The purpose of a regional approach is not to impose a uniform approach to data governance across all countries, but rather to foster mutually beneficial synergy. Rules or laws established by different Member States for data governance issues, such as data protection and privacy, data localisation, and data transfer must not be geared towards a single utopia goal but should inspire some level of complementarity. This implies that, if a member State like Nigeria has a data protection law that sanctions access to personal data without the data subject's consent, another Member State like Ghana should have the autonomy to impose a different punitive measure for the same infraction.

## Recommendation for effective coordination of a sustainable regional data governance policy

The responsibility to ensure coordination begins with the framing of the regional policy . In theory and practice, a sustainable regional data governance should take cognizance of the existing data governance policies, roles, and frameworks to how they align with the continent's goals and values, as designed by the regional authorities. This is beneficial because it allows regional authorities in Africa to identify the existing commonalities and differences among the various Member States and prioritise the areas that need improvement or harmonisation. Member States also play a critical role in integrating national and regional policies.

The following recommendations will be beneficial to national and regional stakeholders who are looking into the issue of integration:

### A. National data governance policies

#### ● ***They must be Afro-centric***

The principles of the national data governance policies should be guided and shaped by the African socio-cultural, political, and economic realities, not those of the Europe or the United States. This implies that these policies must reflect Africa's contextual peculiarities. Despite the significant advances that both the European and the American data governance models have made in their respective approaches to data economy, each has flaws, which is why Africa, especially at the continental level, needs to look beyond modelling its data governance approach after either of the former continents. When countries view data governance issues through the same lens, it can support coordination with regional efforts.

#### ● ***The data policy environment should be transparent***

National data governance policies should be guided by transparency for all actors (local and external stakeholders). Transparency is one of the qualities that a well-governed data economy, at any level, must possess. Data governance decisions, controls, and processes must be clearly communicated to all actors in the data governance ecosystem in a way that leaves no one in doubt. For instance, any information on the laws that regulate data processing of data must be communicated to the data subject in a concise, transparent, intelligible, unambiguous, and easily accessible manner. Transparency supports coordination as stakeholders in each country are made aware of the laws and regulations in jurisdictions beyond their place of domicile. This eases the discovery of gaps and thus improves support for harmonisation.



- ***They must be rules-based***

All data governance principles at the national level should outline the core values and rules that will govern data-related decisions and actions, such as data ownership, accountability, and ethics. A rules-based data governance policy establishes clear rules that help create a consistent, transparent, and fair environment for all actors in the data governance ecosystem to do business and make adjustments where necessary.

## **B. Regional data governance policy**

- ***Provision of support system for capacity development to Member States***

The provision of a support system for capacity development can serve as a guiding role for regional authorities in ensuring that Member States' policy initiatives are implemented effectively. There are some Member States where capacity gaps in skill sets requisite in the areas of data protection, cyber security, and institutional data governance do not exist. Hence, capacity development is required to help them drive a robust digital economy where such skill sets are lacking.

- ***Creation of a platform for data policy auditing***

The regional authorities can conduct a data inventory and audit to identify the data sources, systems, and processes that exist in each Member State, how they are connected, and any flaws or gaps that exist. They should also review the existing data governance policies, regulations, and frameworks in all Member States to evaluate if they align with the region's overall goals and values. The findings could be presented to Member States to design an appropriate intervention and harmonisation process.

- ***Tracking of data governance performance and reporting of same to Member States***

Lastly, the regional authorities should define and track the key data governance performance indicators (KPIs) and metrics that can help evaluate the effectiveness of the region's data governance policies, standards, roles, and processes. Feedback and insights from data teams and users must be collected and analysed to identify the strengths and weaknesses of the region's data governance practices and to discover the opportunities and challenges for improvement. Such reports on the regional and national data governance performance results and recommendations could shape the coordination strategies.