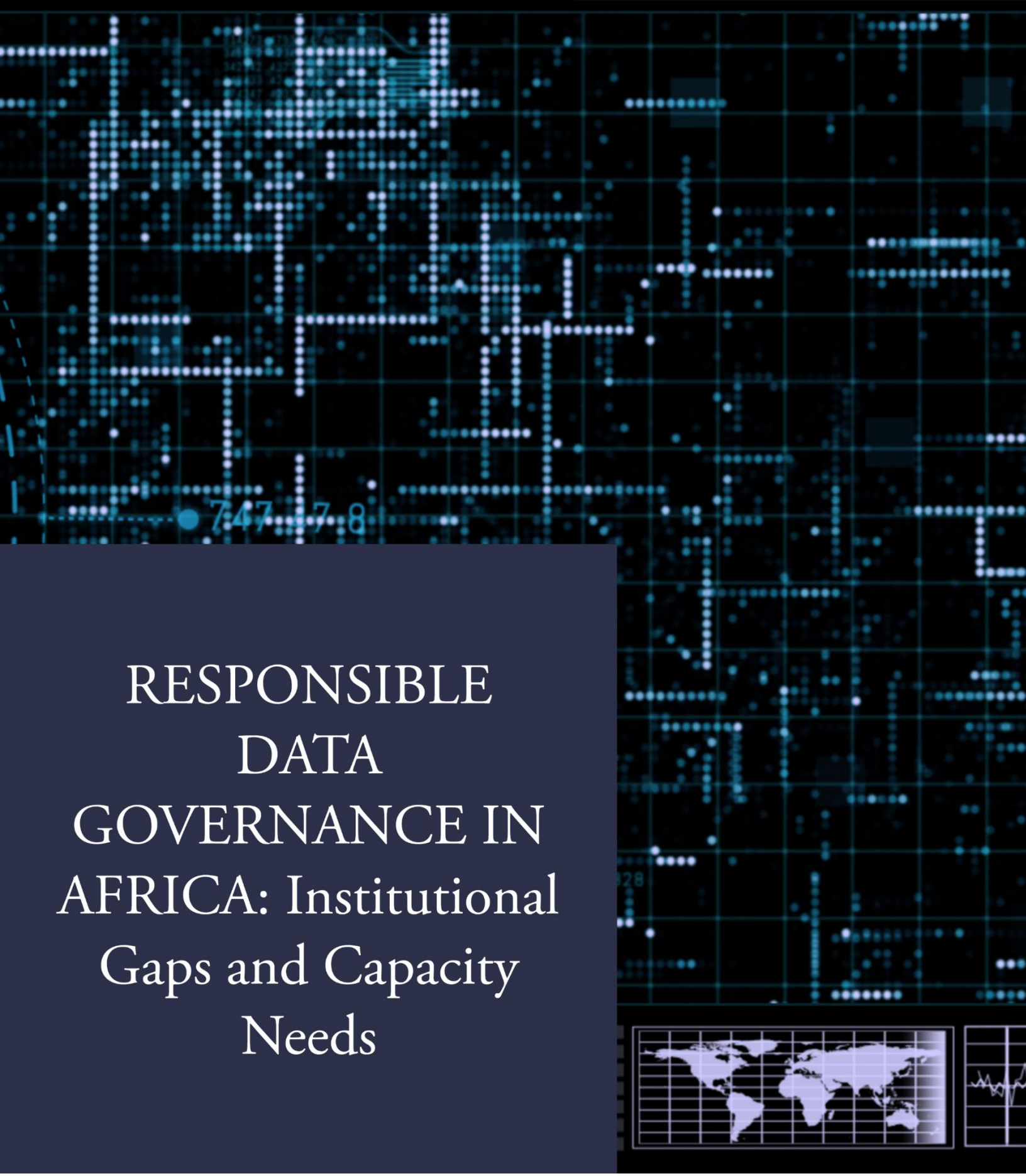

RESPONSIBLE DATA GOVERNANCE IN AFRICA: Institutional Gaps and Capacity Needs

CSEA
Centre for the Study of the Economies of Africa

TABLE OF CONTENTS

Authorship

Lead Author: Damian Okaibedi Eke PhD

Contributors: Paschal Ochang, Tolu Ogundele, Ayodeji Adimula, Favour Borokini, Simisola Akintoye, Ridwan Oloyede, Lebura Sorborikor, Mercy Adeyeye, Bamidele Wale-Oshinowo

Funding Acknowledgement

This report is part of CSEA's knowledge series on strengthening data governance in Africa, funded by The William and Flora Hewlett Foundation.

Citation

Eke, D., P. Ochang, A. Adimula, F. Borokini, S. Akintoye, R. Oloyede, L. Sorborikor, M. Adeyeye, B. Wale-Oshinowo, T. Ogundele. 2022. Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs. Centre for the Study of African Economies (CSEA)

Published: September 2022

EXECUTIVE SUMMARY

Africa is quickly becoming the new data frontier in the face of continued increase in the deployment of digital technologies. A proportionate data governance ecosystem is, however, still lacking. The available governance ecosystem is characterised by a lack of relevant institutions or in most cases non-functional institutions for effective data governance implementation. As part of the bid to understand how to create a functional and responsible data governance ecosystem that can play a vital role in Africa's competitiveness in the global data economy, this report explored the questions; what are the institutional gaps impeding responsible and sustainable data governance in Africa and what are the peculiar institutional capacity needs of existing institutions? To answer these questions, we used a multidimensional research approach to study five African countries namely Nigeria, Morocco, Kenya, Mauritius and South Africa. In this study, we identified clear institutional gaps and capacity needs that require significant attention.

The findings show that institutions that make or create data and monitor governance laws beyond data protection, that can generate evidence-based research for data governance and that can facilitate Findable, Accessible, Interoperable, Reusable (FAIR) data are lacking in Africa. They also demonstrated that whereas data protection regulations are gaining traction in Africa, most established institutions created to monitor compliance and enforcement are yet to operate independently of government control. This lack of independence grossly affects effectiveness at different levels. Furthermore, our findings show that both private and public data-driven entities that should apply data governance principles to their processing workflows are yet to establish data governance roles within their organisations.

To understand institutional capacity needs, we studied established institutions for monitoring the compliance and enforcement of data protection regulations which are often called Data Protection Authorities (DPAs) in these countries. We identified that compliance and enforcement of data protection regulations remain low, and this is informed by a number of factors including; a lack of robust organisational culture built around the right people, non-functional systems and processes that support efficient data related policies for the right stakeholders, and a lack of enabling infrastructure to adequately respond to the views and needs of data stakeholders. The findings of this research show that for DPAs in Africa, lack of the right mix of relevant expertise, skills and knowledge (particularly technical and ethical skills), non-integration of contextual African values, lack of resources (including funding and technologies), lack of clear policy methodology, monitoring and enforcement plans and risk assessment approaches contribute to the existing inefficiency of data governance mechanism.

1. BACKGROUND

Like many parts of the world, data ecosystems are significantly increasing in size, complexity and power in Africa owing to advancements in digital technologies. From business management processes, smart cities, socio-political decisions, and educational activities to academic/industrial research and innovations, big data has become a critical asset that underpins successful and efficient operations worldwide. The realisation of these potentials, however, requires access to data in various formats and volumes across disciplinary and national boundaries. Such international, interdisciplinary, and intercultural data use can raise a number of challenges relating to privacy, data protection, appropriateness of data use outside of their original purpose, distribution of costs and benefits, the possibility of data abuse and misuse, and intellectual property. To find appropriate responses to the above concerns, data ecosystems need to be based on sound, ethically acceptable, socially desirable, and legally compliant data governance principles.

Responsible data governance structures are the bedrock of optimal maximisation of the values of data. Through the implementation of responsible principles, processes, standards, policies and technologies, data governance ensures the availability, usability, integrity, quality, security, and compliance of data collected, processed, shared and applied in businesses, innovation and research. Evidence shows that reliable institutions and resources to support a well-functioning data governance environment are lacking in most African countries (Osakwe and Adeniran, 2021). Whereas data governance continues to gain traction in Africa, sustainable and relevant institutions of data governance are still missing. This means that the data ecosystem in the continent remains fragmented and the value and utility of data are yet to be optimally maximised.

As part of the bid to understand how to create a functional data governance ecosystem that can play a vital role in Africa's competitiveness in the global data economy, this study explored institutional gaps and capacity needs for data governance in Africa, and sought to answer these questions; ***what are the institutional gaps for responsible and sustainable data governance in Africa and what are the peculiar institutional capacity needs for available institutions?*** The mapping of the institutions, resources and capacities for data governance is essential in developing a rigorous and practical data governance environment in Africa. The overall aim is to gain insights into how to define interventions to address the data governance challenges by building relevant institutions and capacities, taking into account the interconnectedness of the institutions, challenges and capacity issues. Data is a crucial component of the overall competitive business strategy in Africa. The outcomes of the project will directly contribute to the African Union's (AU) goal of promoting the region as a globally attractive place for digital organisations and help to create a digitally led sustainable economy. The advocacy project makes a key contribution to the African ambition to gain a place in the global data economy.

This project used a multidimensional research approach with a variety of research strategies that are currently utilised across the social sciences. These include Desk Research, Focus Groups and Doctrinal Analysis. The structure of this report starts with a conceptual clarification of what we mean by data governance and continues to the identification of institutional gaps as regards the establishment of a robust and responsible data governance ecosystem in Africa. Subsequently, discussions will focus on the institutional capacity needs of available institutions, particularly data protection authorities in five selected countries (Nigeria, Morocco, Kenya, Mauritius, and South Africa). The results demonstrate significant institutional gaps and capacity needs that form barriers to a functional African data governance ecosystem. This report concludes with viable recommendations to address these gaps and needs.

2. DATA GOVERNANCE: MEANING AND CRITICAL ELEMENTS

The origin of data governance is associated with Information Technology (IT) governance and stakeholder efforts to prevent the misuse and abuse of data within organisations (Merkus, Helms and Kusters, 2019). Comparing data to a valuable asset, Chen, (2010) discusses three distinct evolutionary eras of data governance which are the *application,*

enterprise repository and *policy* eras. In the application era (1960 - 1999), activities around data were more about processing technology rather than governance, thus organisations were more inclined to build systems that made transactions easier and less labour intensive. In the enterprise repository era (1990 - 2010), Chen (2010) asserts that organisations began to analyse data for the purpose of decision making. As a result, it became imperative to build large scale repositories like data warehouses and systems that support data governance and management. In the policy era (2010 - date), data and its use became more complex, due to many organisations' multiple operations and systems. Hence, to accurately combine, store and present information, organisations established institutions and systems that catered for data quality, security and lifecycle management. Thus, current definitions focus more on policy elements. In the context of biomedical research, Eke et al., (2021) defined the concept of data governance as the principles, procedures, frameworks, and policies that ensure acceptable and responsible processing of data at each stage of the data life cycle, from collection, storage, processing, curation, sharing, and use to deletion. Similarly, Ndemo and Thegeya (2022) posit that data governance involves establishing principles to enable an environment for the sharing of data, with the ultimate goal of improving living standards, while at the same time recognizing and protecting the rights of data originators and users.

There are three critical elements of effective data governance; *people, processes* and *technologies*. The *people* element ensures that the relevant stakeholders are properly identified (the data subjects, data generators, processors, users, custodians etc). The element of *processes* means the establishment of the right processes, policies, and procedures (including the identification of the relevant regulations, ethical principles, and guidelines) for data processing. Finally, the *technology* element means the deployment of the appropriate technologies for best and responsible outcomes (including technologies for privacy, security, compatibility, and interoperability). All three elements are situated within organisational and institutional dynamics. Data governance is thus defined in this paper as the framework or approach (of people, procedures or processes, and technology) set up by organisations and institutions to ensure that data processing activities in each stage of the data lifecycle are responsibly done in a way that maximises benefits for relevant stakeholders while complying with relevant ethical and legal requirements. Stakeholders to the data can be different in different contexts such as public policy, business, innovation, and research.

Data governance is a concept that is foundationally shaped by ethics and law. Although it has a descriptive meaning, it also has a regulatory and ethical scope which involves laws, regulations, ethics and standards, as well as allocation of responsibilities and liabilities (Micheli et al., 2020; Eke et al., 2021). At the foundations of data governance are laws and ethical principles (established by institutions or socio-cultural entities) that shape how data should be treated. Data here does not only refer to personal data but to all forms of data (including personal data, non-personal human data, animal data and technical data). That means that data governance is not just data protection, which is simply focused on the protection of personal data. It includes the governance of all forms of data used for operations of entities.

An effective data governance framework not only helps institutions to ensure data availability, integrity, usability, security and compliance, but also ensures that all stakeholders benefit from the data ecosystem. Compliance with laws, regulations and ethical principles is particularly important because data that meets organisational goals and objectives increasingly come from diverse sources, in different formats and from different jurisdictions. This raises complications regarding knowing which legal framework to apply and how to apportion responsibilities and liabilities. These include human data, animal data and technical data. Contrary to some beliefs, data governance goes beyond the provisions of data protection regulations to include mechanisms of making data available and usable in a way that benefits the organisations as well as data subjects. Each stage of the data lifecycle raises critical questions with data governance implications.

It is also important to note that data governance is interpreted differently in different disciplines. Interpretations given to data governance in business organisations are not the same in research and innovation activities or in public service

institutions. While the fundamental dynamics of data governance are the same in all cases, the central focus of data governance in each discipline or field is different.

3. DATA GOVERNANCE INSTITUTIONS

BOX 1

Institutions Relevant for Sustainable and Responsible Data Governance include institutions that;

Create/make relevant data governance laws, standards, regulations, and policies. (e.g International, regional, or national bodies e.g WTO, OECD, the African Union, National Legislatures, DPAs or Commissions).

Monitor compliance and enforcement (e.g DPAs, security agencies, Civil society groups)

Generate evidence-based research to inform and maintain data governance (e.g Academia including research centres, funders, and international collaborative projects)

Apply DG frameworks to their data processing activities based on available laws, regulations and policies (e.g public institutions, private entities – businesses)

Facilitate FAIR (FAIR- Findable, Accessible, Interoperable and Reusable) data principles. These institutions - e.g High Performance Computing centre (HPCs), data centres, data repositories)

Data governance frameworks and structures are institutionally driven. These are structures established, implemented, monitored, and maintained by institutions that are diverse in nature but often interconnected in operations *(see Box 1)*. Data governance requires institutions at both the micro and macro levels (Ndemo and Thegeya, 2022). At the micro-level, data governance includes management of the availability, usability, integrity, and security of data, while at the macro level, the development of such a framework requires the establishment of an appropriate economic, legal and institutional ecosystem, as well as the development of proper standards for the exchange and protection of data. Data governance involves inter and intra-power relationships in institutions and all the actors affected by, or that affect the way data is accessed, controlled, shared, and used. Fundamentally, data governance is about identifying these actors (their roles and responsibilities), employing the right principles, procedures, and frameworks with appropriate technologies to ensure that the value of data is fully maximised, risks are mitigated, legal and ethical principles are complied with. Data governance institutions include institutions that create or make data governance laws, standards, and regulations, monitor compliance and enforcement, generate evidence-based research that informs and maintains data governance, apply data governance frameworks for data processing activities, and facilitate FAIR (Findable, Accessible, Interoperable and Reusable) data.

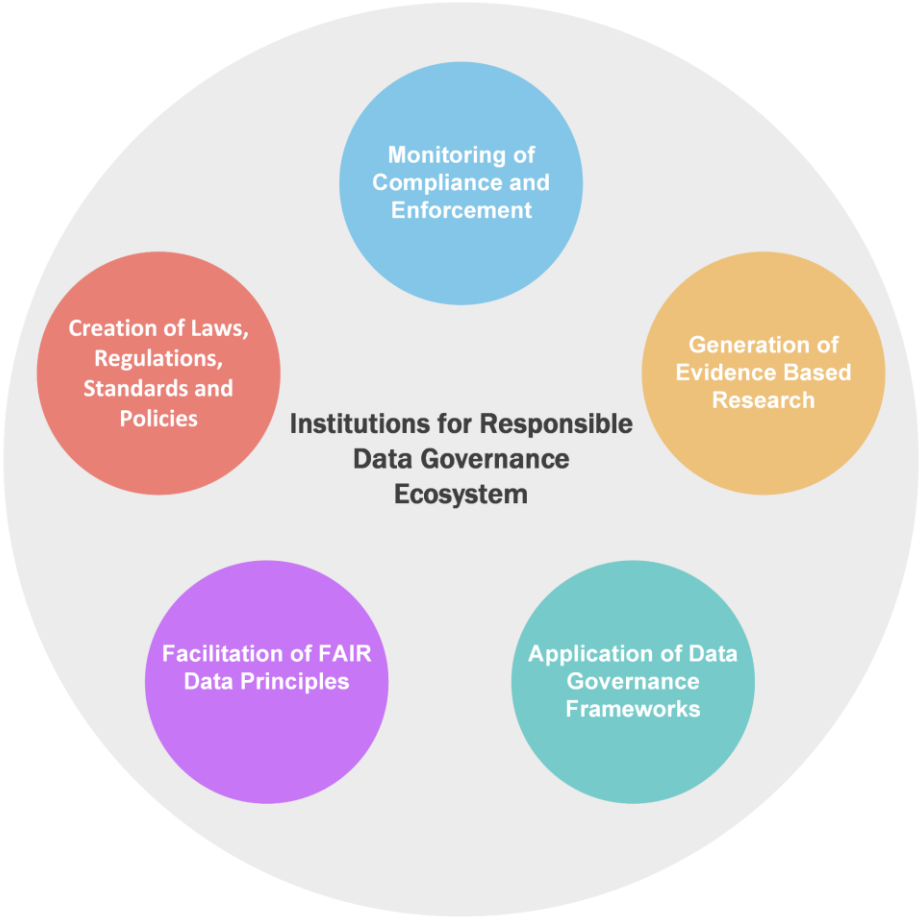

Figure 1: Overview of institutions for Responsible Data Governance Institutions

Regarding laws, there are international, regional and national regulations and laws that data-driven entities in Africa should be aware of. At the international level, a number of laws, treatises and policies cover aspects of data governance. Some of the international institutions with relevant data-related policies include United Nations (UN), World Trade Organisation (WTO) and Organisation for Economic Co-operation and Development (OECD). The UN's Universal Declaration of Human Rights (UDHR) is critical to data policy-making processes. Data governance is a rights-based approach that should align well with the rights provided in the UDHR including rights to privacy. The WTO recognises the importance of data and data sharing in international trade as well as the tension between the need to share data and the imperative for data protection. Thus, they hosted a guest panel on *Data governance and International trade* on 8 June, 2021 to discuss how national and transnational approaches to governing data and data-driven sectors can build trust and facilitate growth and innovation. The OECD on the other hand has been playing an important role in promoting data governance and the principle of respect for privacy as a necessary condition for open data sharing across borders for a number of years. Important to this is the publication of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[1] These transnational organisations and the policies they create are particularly important because data processing for most data-driven entities in Africa interacts with multiple jurisdictions.

[1] https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

At the continental level (Africa), relevant policies, regulations or declarations include; the African Continental Free Trade Area (AfCFTA) Agreement[2], African Union Convention on Cyber Security and Personal Data Protection, 2014[3], Declaration on Internet Governance and Development of Africa's Digital Economy 2018[4] and the African Union Digital Transformation Strategy (2020-2030)[5]. In addition to these continental efforts to promote data governance, a number of regional efforts have also been put in place. In West Africa, there is the Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection (2010). East African Community Cyberlaw Framework, 2010[6] prepared by the East African Community (EAC) Task Force on Cyberlaws has been providing guidance in East Africa. In Southern Africa, the Southern African Development Community (SADC) Model Law (2013)[7] provides guidance.

A typical example of regional data governance laws and regulations are the European General Data Protection Regulation (GDPR)[8] and the European Data Governance Act (DGA)[9] created by the European Parliament and Council of the European Union. In addition to the European Data Protection Board and the European Data Innovation Board that facilitate best practices that align with these laws, there are national public authorities in member states that monitor compliance and enforcement. These are functional institutions that contribute to the creation and maintenance/sustenance of the data governance ecosystems in Europe. Another crucial institution involved in monitoring the compliance and enforcement of data governance laws and regulations are civil society groups. According to the European data protection supervisor (EDPS), civil society groups are natural allies when it comes to putting data governance principles to practice, empowering individuals to assert their rights and holding data processing institutions accountable for their actions. Some of the landmark data protection and privacy cases (for example, *Digital Rights Ireland* (CJEU), *Zakharov v. Russia* (ECtHR), *10 Human Right Organisations v. the United Kingdom* (ECtHR)), have been brought to the attention of the regulatory and judicial authorities by civil society groups. This helps in developing both the law and rights awareness among a broader public.

Data governance requires robust evidence-based research to inform its underlying principles and best practice approaches. The data governance landscape is an ever-changing ecosystem that continually needs to align with societal expectations, regulatory provisions, technical requirements and organisational objectives. The establishment of this alignment requires evidence-based research and critical institutions that contribute to this include academic and research institutions as well as funding bodies. Some of the areas of data governance where research is critical include;

1. **Data Collection**: What type of data? How is the data collected? Who is collecting the data? What technologies are used?

2. **Data Processing (cleaning, curation, storage, archiving)**: What data and metadata formats and standards are applied? How is the data processed? Where is the data stored? What technologies are used to ensure security and privacy? What other mechanisms ensure quality?

3. **Data Application**: How are risks mitigated e.g data misuse, abuse, bias and discrimination? How do you ensure that all relevant stakeholders benefit?

---

[2] https://afcfta.au.int/en

[3] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[4] https://www.afigf.africa/sites/default/files/DeclarationonInternetGovernance_adoptedAUSummit2018.pdf

[5] https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

[6] https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

[7] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[8] https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

4. **Data Sharing**: Who has access to the data? How do users get access? How do you decide who owns or controls the data e.g data licensing, intellectual property concerns?

5. **Data Retention**: Who added what and when? Who changed what and when? How long should the data be retained? Where is data stored and how?

6. **Data Deletion**: how do you avoid inappropriate retention, loss of data and unintended deletion?

The crucial role of researchers in data governance was evident during the COVID-19 pandemic when many researchers played a major part in shaping the responsible development of contact tracing apps in a way to preserve confidentiality and privacy. On 19 April 2020, more than 400 scientists and researchers signed a Joint Statement on Contact Tracing, explaining why centralised data processing apps raise greater concerns than decentralised systems (Larus, 2020). These scientists provided scientific evidence why implemented apps should preserve the privacy of their users, thus safeguarding against many other issues and noted that such Apps can otherwise be repurposed to enable unwarranted discrimination and surveillance. Subsequently, the centralised Pan European Privacy-Preserving Proximity Tracing (PEPPPT) was replaced by the decentralised privacy-preserving proximity tracing (DP-3T) protocol.

In addition to the institutions that create laws, monitor compliance and generate evidence-based research, the majority of data governance institutions are entities that apply these external instruments to their internal data processing activities. These are the public and private entities that create both the people and technical infrastructure for data processing pipelines. They include; public entities (e.g public health institutions, public education institutions), private enterprises (e.g business organisations) and research entities (e.g research centres processing biomedical data). The organisations that process data (human, animal and technical data) are all expected to develop data governance frameworks or structures that can facilitate usability, accessibility, quality and integrity of the data in a way that can ensure that organisational goals are met.

The final critical institutions for an efficient data governance ecosystem are the institutions that facilitate FAIR data principles (Wilkinson et al., 2016). These institutions make data Findable, Accessible, Interoperable and Reusable with minimal constraints. The overall aim of these institutions is to optimise the reuse of data. To achieve this, harmonised metadata standards, as well as secure technologies, are required. The FAIR guiding principles for scientific data management and stewardship are critical enablers to digital transformation as well as successful organisational operation. These institutions range from High-Performance Computing centres, data centres, to biobanks and other data repositories or infrastructures. A data repository or infrastructure helps in the curation and storage of datasets from various sources in a way that makes it easier to find, access, use/apply and mine for different purposes. Gaia-X[10] and some infrastructures under the European Strategy Forum on Research Infrastructures (ESFRI)[11] are good examples here. The value of data is optimised when entities that need them can find them, access, interoperate and reuse them. This report explores which of the above institutions of data governance are available in Africa and what institutional capacities do available institutions have? Following the above understanding of the core institutions for a responsible data governance ecosystem, we studied five African countries; Nigeria, Morocco, Kenya, Mauritius and South Africa.

3.1 OVERVIEW OF DATA GOVERNANCE INSTITUTIONS IN AFRICA

At the continental and regional levels, there are identifiable institutions that create or make data governance related laws, regulations or policies in Africa. The first among them is the African Union (AU). From the Convention on Cyber Security and Personal Protection, African Union Digital Transformation Strategy (2020-2030), Declaration on Internet Governance and Development of Africa's Digital Economy 2018 to Personal Data Protection Guidelines for Africa the AU has demonstrated the intention to shape governance of data processing activities in Africa. The Economic Community of West African State (ECOWAS) and the Southern African Development Community (SADC) as regional economic communities have also adopted the Supplementary Act on Personal Data Protection within ECOWAS, 2010 and the

[10] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

[11] https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/our-digital-future/european-research-infrastructures/esfri_en

SADC Model Law on Data Protection (2013) respectively. While these are the right steps in the right direction, their focus remains on data protection which is only a part of data governance.

To provide a robust overview of data governance institutions in Africa, we provide the findings from the selected five countries; Nigeria, Morocco, Kenya, Mauritius and South Africa.

3.1.1 NIGERIA

Making of laws, regulations, and policies

Institutions in Nigeria identified as creating or making data governance laws, regulations, policies and standards include; National Assembly: The Nigeria National Assembly (made up of the House of Representatives and the Senate) is responsible for making critical laws and creating agencies that apply to data processing in Nigeria. Some of these laws and agencies include; the Nigerian Constitution, the Cybercrime Act 2015, Credit Reporting Act 2017, Freedom of Information Act, 2015, the National Identity Management Commission Act (NIMC) 2007, the Nigerian Commissions Act (NCA) 2003, the child's Rights Act 2003, among others. In addition, there are also agencies established by the National Assembly that make data governance policies and regulations. These include;

- National Information Technology Development Agency (NITDA) (that developed the Nigerian Data Protection Regulation)
- National Identity Management Commission (NIMC) given the functions and powers, to establish the National Identity Database and the National Identification Number (NIN) (that created policies and regulations such as Regulations on NIMC Licencing of Front-end Services[12], Regulations on Access to Register Information in the National Identity Database[13], Regulations on Registration of Persons and Contents of the National Identity Database,[14] Guidelines on Biometric Standards, Privacy Policy For The National Identity Management System (NIMS), National Policy & Institutional Framework for an Identity Management System for Nigeria, National Policy for the Promotion of Indigenous Content in the Nigerian Telecommunications Sector).
- Nigerian Communications Commission (NCC) (that created regulations such as; Lawful Interception of Communications Regulations,[15] Mobile Number Portability- Business rules & Port Order Processes 2020[16] and Consumer Code of Practice Regulations[17]

This shows that in Nigeria there are quite a number of institutions that are designed to enact/design data governance laws and regulations in Nigeria. It must be noted that there is still no substantive law on data protection, only subsidiary and sectoral regulations (Babalola, 2022). Whereas the sectoral efforts as regards regulations, particularly NDPR, are commendable, it is palpably evident that Nigeria does need an effective data protection legislation (Ibid). There have been several legislative attempts to regulate Data Protection at the National Assembly, but none has succeeded. This leaves the data protection ecosystem fragmented without a harmonised approach for all sectors. Albeit, data protection is only an element of data governance and not the whole of it. The EU is currently leading the way in recognising the importance of robust data governance laws and building institutions to maintain the data governance ecosystem.

[12] https://nimc.gov.ng/docs/NIMClicencing_frontend_services.pdf

[13] https://nimc.gov.ng/docs/NIMCaccess_register.pdf

[14] https://nimc.gov.ng/docs/NIMCregistration_person_contents.pdf

[15] https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/839-lawful-interception-of-comunications-regulations-1/file

[16] https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/972-regulations-on-mobile-number-portability-business-rules/file

[17] https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/102-consumer-code-of-practice-regulations-1/file

Currently, there is no specific law that focuses on the nature and dynamics of data governance in Nigeria (to enable positive outcomes for individuals, businesses, and the society) and no institution is responsible for data governance.

Monitoring Compliance and Enforcement

In Nigeria, the National Human Rights Commission (NHRC)[18] is a central enforcement agency for data governance cases. This is mainly because core parts of human data processing directly relate to the rights of privacy and data protection. The Consumer Protection Council (CPC) is another institution that monitors compliance and enforcement as well as established agencies that create sector-specific policies such as NITDA, NIMC and NCC. For a number of years, NITDA was the major institution that created, monitored and enforced the data protection regulation in Nigeria. In February 2022, the establishment of a new agency, the Nigerian Data Protection Bureau (NDPB), was approved. The NDPB is expected to take over enforcement of compliance with the provisions of the Nigeria Data Protection Regulations 2019 (NDPR) from NITDA (Eke et al., 2022).

Considering that NITDA was under the supervision of the Federal Ministry of Communications and Digital Economy, it did not enjoy the independence required to monitor and maintain compliance with Data Protection regulation. Many people have also raised concerns that the new NDPB will be under the residual control and supervision of the Ministry since it was not established pursuant to any statute but through executive fiat (Alao, 2022). This means that Nigeria still lacks an independent agency that monitors compliance and enforcement of data protection regulations.

There are also civil society coalitions and non-governmental organisations that hold data processing institutions accountable. Examples include recently initiated cases related to data breaches such as *Incorporated Trustees of Laws and Rights Awareness Initiative v. Zoom Video Communications Inc (FHC/AB/CS/53/2020) and Digital Rights Lawyers Initiative v. National Youth Service Corps (NYSC) (FHC/IB/98/2020)*. The former contested the non-compliance of Zoom's privacy policy with the Nigeria Data Protection Regulation (NDPR) while the latter was instituted against the National Youth Service Corps (NYSC) contesting that the NYSC published and sold a yearbook containing corps members' personal data without consent. The overall assessment here is that Nigeria still lacks effective institutions for monitoring compliance and enforcement in a way that protects the citizens and advances innovation and business operations.

Generation of Evidence-based Research

There are just a few institutions in Nigeria that are engaged in generating evidence-based research on the nature and direction of data governance in Nigeria. Most of these organisations are research think tanks and advocacy organisations. Educational institutions are yet to make data ethics, data management and data governance curriculum or research priorities. This is evident in the dearth of literature on these concepts and the total lack of data governance or data ethics in the University curriculum in Nigeria.

Application of DG Frameworks

Many institutions in both the private and public sectors are required to apply or should apply data governance frameworks and structures to their data processing activities. Some of the public institutions that should be applying DG frameworks in Nigeria include the Independent National Electoral Commission (INEC), the Nigerian Immigration Service, the Directorate of Road Traffic Services, the Federal Road Safety Corps (FRSC), the National Population Commission, the Federal Inland Revenue Service (FIRS), Joint Tax Board (JTB), Corporate Affairs Commission (CAC), Health Establishments Health Management Organisations (HMOs) and National Health Insurance Scheme (NHIS). Educational institutions, as well as small, medium, and large-scale businesses (from telecommunications, banking, fintech, social media, logistics, manufacturing, to security), are also part of this category of institutions. Many of these abound in Nigeria. Data governance regulations and laws become practical in these institutions where procedures and processes are developed for data processing workflows. Whereas there are many institutions that should apply DG frameworks to their workflows/pipelines, only a small number of these institutions understand the importance of internal data governance mechanisms. Some entities that understand its importance do not have such mechanisms or frameworks

[18] https://www.nigeriarights.gov.ng/

owing to a number of factors. Public institutions, especially, have been found not to apply elements of data governance resulting in fragmented and unstructured data ecosystems. In the private sector, only large corporations are found to apply some technical elements of data governance and data management. Small scale entities are yet to consider data governance mechanisms due to a number of factors (e.g funding).

Facilitation of FAIR

There are also a number of institutions in Nigeria designed to facilitate FAIR data principles (findability, Accessibility, Interoperability and Reusability). In Nigeria, there are several data centres dedicated to storing and sharing applications as well as centralising IT operations and equipment of businesses. These centres are yet to demonstrate that they can facilitate FAIR data principles. In the biomedical field, there is the **National Data Repository (NDR)** which is Nigeria's central repository of patient-level data for diseases. Data are ingested from implementing partners (IPs) and electronic medical record (EMR) systems. **54Gene** is another health technology platform building a repository of diverse genetic datasets to be made FAIR to unlock scientific discoveries as well as improve diagnostic and treatment outcomes within Africa and the global community.

In recent times, the Nigerian National Agency for Science and Engineering Infrastructure (NASENI) implemented HPC that assists both internal scientists and external engineers in carrying out their research which for now only involves simulations and modelling. It does not yet provide a database facility for FAIR. Nigeria still lacks functional data hubs or infrastructures for centralised or decentralised data operations for businesses, research, and innovation.

3.1.2 MOROCCO

Making of laws, regulations, and policies

In Morocco, underlying data governance is the personal data protection law called Law n° 09-08 of 18 February 2009 (in French). This law relates to the protection of individuals with respect to the processing of personal data. Associated with this is its implementation of Decree n° 2-09-165 of 21 May 2009. Institutions responsible for making these laws are the Moroccan Monarchy with most of the executive powers and the Parliament divided into two chambers (Representative and Advisors). This is one of the earliest data protection laws established in Africa. There is no law or regulation to address other aspects of data governance in Morocco. The lack of a data governance law means that there is no legislative provision that shapes the optimal maximisation of data for society, businesses, and the environment. This is an institutional gap that needs consideration.

Monitoring Compliance and Enforcement

The Commission Nationale de Contrôle de la Protection des données à caractère Personnel[19] (CNDP) is responsible for ensuring that the processing of personal data of citizens/residents is done within the ambit of the law, and that their privacy, freedoms and human rights are not violated. The independence of the CNDP, however, has remained debatable. The CNDP establishes a list of countries that satisfy the requirements of the Data Protection law and defines relevant exceptions. The Commission also manages complaints and data breaches and offers expert opinions in front of the courts. The CNDP also has a role in informing the public about their rights and obligations. The Commission also has investigative powers and is endowed with law enforcement powers as well. It can require direct access to facilities in which data is being processed.

In addition to this commission, there are agency-specific bodies that also monitor the compliance and enforcement of how data is processed with digital technologies. These include; the National Council of Information Technology and the Digital Economy (Conseil National des Technologies de l'Information et de l'Economie Numérique), established by Royal Decree 2-08-444.[20] It monitors the implementation of a national strategy to promote the use of information technology by both the public and private sectors. There is also the National Telecommunications Regulatory Agency (ANRT) which is the public body responsible for the control and regulation of the telecommunications sector. ANRT was created in

[19] National Control Commission for the Protection of Personal Data in English

[20] http://www.egov.ma/sites/default/files/decret_cnti_bo5744_fr.pdf

February 1998 under Law no 24-96 on postal and telecommunications services which dictated the general outlines of the sector's reorganisation. This means that there is still an institutional gap as regards monitoring other aspects of data governance beyond data protection in Morocco because there is no law that covers these aspects.

Generation of Evidence-based Research

There are no institutions identified in Morocco that focus on the generation of research and scientific evidence to support the development and maintenance of data governance both as a theoretical and practical concept. From academic institutions to private research centres, data governance remains poorly studied in Morocco. This does not necessarily mean that there is a total lack of an institution or entity studying data governance but may mean that such an institution is not visible online.

Application of DG frameworks

There are a number of public and private institutions in Morocco that should apply data governance frameworks. In the public sector, there is the Moroccan Consular service that collects personal information for all immigration services. Others include the directorate of statistics, ministry of health, ministry of justice and other ministries where personal data are collected. There is also the National Police mandated to issue the national biometric ID card under the scheme called *Carte nationale d'identité électronique (CNIE)*. In addition to these, there are local and foreign businesses processing personal data of Moroccan citizens that are expected to apply responsible data governance frameworks. However, it is important to note that while these institutions focus on complying with available data protection regulation, there is no indication that they have robust data governance structures sensitive to the interests, needs, values and benefits of the society.

Facilitation of FAIR

In 2021, the Mohammed VI Polytechnic University in Rabat (UM6P), formally opened its new data centre The African Supercomputing Centre (ASCC)[21] which houses what it claims to be the most powerful supercomputer in Africa called *Toubkal*. This infrastructure is intended to help the University coordinate research across Africa in a range of areas, including artificial intelligence and Internet of Things (IoT) technology, Food Security, genomics and analytics. Also, the 'Cyber Security Centre of Excellence for Africa' which is expected to open in 2024 in Marrakech aims to serve as a regional data hub, playing a strategic role in the fight against cybercrime with the support of law enforcement bodies, effective criminal justice systems, and active international collaboration. There is also the Morocco open data portal[22] that makes government data open and easy to access to the public. These centres make it possible to store and use big data in a way that is FAIR. Institutions for FAIR are therefore emerging in Morocco.

3.1.3 KENYA

Making of laws regulations and policies

The Parliament of Kenya which is a bicameral legislature is the major institution responsible for making laws and regulations that shape data governance in the country. Under Article 31(c) and (d) of the Constitution of Kenya, the right to privacy is guaranteed as a fundamental right. It was the Parliament that established the Data Protection Act no. 24 of 2019 (the DPA) in Kenya to ensure the protection of this constitutional right. The Act also established the Office of the Data Protection Commissioner (ODPC). Subsequently, in 2021 the ODPC in collaboration with the Taskforce for the Development of the Data Protection General Regulations, created and published regulations[23] such as; the Data Protection (General) Regulations, 2021 ('General Regulations'); the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 ('Complaints Handling and Enforcement Procedures Regulations'); and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021('Data Controllers and

[21] https://ascc.um6p.ma/

[22] https://morocco.opendataforafrica.org/

[23] https://www.dataguidance.com/sites/default/files/the_data_protection_regulations_2021fin._1.pdf

Data Processors Regulations'). Prior to these, data protection in Kenya was shaped by laws such as the Kenya Information and Communications Act, 1998, the Kenya Information and Communications (Consumer Protection) Regulations of 2010 and the Kenya Information and Communications Act (Registration of SIM Cards) Regulations 2015. In the biomedical sphere, the Public Health Act 2012 and the Health Act, 2017. For financial activities, data processing is regulated under the National Payment System Act, 2011, and the National Payment System Regulations, 2014[24] under the National Payment System Act. There is also the Consumer Protection Act, of 2012. These Acts and regulations indicate that there is a thriving ecosystem of data protection regulations but nothing on data governance as a whole.

Monitoring compliance and enforcement

In Kenya, the Office of the Data Protection Commissioner (ODPC) is responsible for monitoring compliance, implementation, and enforcement of data protection regulations in Kenya. The ODPC derives its power from the Data Protection Act of 2019. ODPC harmonises the previously fragmented data protection landscape and ensures that the rights and interests of data subjects are protected. For data governance in general, there is no compliance or enforcement agency. In the civil society space, the Data Policy Centre (DPC)[25] is also working towards ensuring that the rights of citizens are upheld and legislations are complied with and innovation is not stifled through advocacy.

Generation of Evidence-based Research

Research institutions such as the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and DPC, contribute to the body of evidence available to policymakers in the areas of data protection, data bias and open data at the national and sectoral levels. Teaching and research in data governance and related fields is yet to gain traction in major educational institutions. Robust evidence generation institutions are still lacking in Kenya.

Application of DG frameworks

From local authorities to national agencies, commissions or services, there are a number of public institutions processing data that need to apply data governance frameworks and structures. Entities under institutions such as the Judicial service commission, Kenya National examinations council, National Bureau of Statistics, Central Bank of Kenya and Kenya Defence Forces etc. In addition to these, local and foreign businesses and entities processing data and that requires data governance abound. However, there is no evidence to suggest that these institutions apply data governance mechanisms beyond compliance to data protection regulations. This lack of application of other elements of data governance is an evident institutional gap.

Facilitation of FAIR

There are a number of platforms and repositories designed to facilitate FAIR. These include Kenya Open Data Initiative (KODI)[26] which makes key government datasets freely available to the public through a single online portal. The KODI provides visualisations tools, data downloads, and easy access for software developers. There is also the Kenya Health and Research Observatory (KHRO)[27] which is designed to enhance the availability and use of data and evidence on health. These are critical infrastructure that facilitates FAIR in Kenya but there is a dearth of these platforms or portals that can sustain the amount of data being generated and that requires it to be made available.

[24] https://platform.dataguidance.com/legal-research/national-payment-system-regulations-2014

[25] https://dpccipit.org/about/

[26] https://kenya.opendataforafrica.org/

[27] https://khro.health.go.ke/

3.1.4 MAURITIUS

Making of laws regulations and policies

The National Assembly of Mauritius is the major institution that makes laws for data protection. It was the National Assembly that made the Data Protection Act 2017 which replaced the Data Protection Act 2004 ('the 2004 Act'). The Data Protection Office[28] subsequently establishes policies and guidelines for organisations processing personal data. Some of these guidelines include; the introductory Guide to the Data Protection Act 2017[29], Guide on Data Protection for Health Data and Artificial Intelligence Solutions in the Context of the COVID-19 Pandemic.[30] The Data Protection Act of 2017 was designed to heavily align with international standards namely the General Data Protection Regulation (GDPR) and the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'). Whereas the modelling of acts and laws to conform to international standards are commendable, there are possibilities of alienating the contextually unique socio-cultural contexts which are peculiar to the country and Africa.

With reference to data governance in general, the Ministry of ICT in Mauritius has also created a National Open Data Policy[31] in 2016. This policy sets out processes and procedures for managing government data in an open, transparent, and responsible way. This is a policy that addresses the availability, usability, quality, and accessibility of government data and shapes the country's Open Data Initiative. The government of Mauritius has also developed the Data Sharing Policy and Data Architecture.[32] This policy is focused on achieving interoperability of the Mauritius ICT ecosystem.

Monitoring compliance and enforcement

In Mauritius the Data Protection Office (DPO) is under the administrative control of the Data Protection Commissioner ('DPC')[33] and is considered the primary institution that ensures compliance and enforcement of the Data Protection Act. It is also a public office under the aegis of the Ministry of Technology, Communication, and Innovation. The Office was established under Section 4 of the now-defunct 2004 Data Protection Act. The DPO receives and addresses complaints related to data breaches or unlawful disclosure of, and access to, personal data. The DPC and the DPO provide a harmonised national approach for compliance and enforcement. The Ministry of ICT monitors the compliance and enforcement of the Open Data Policy.

Generation of Evidence-based Research

Our research revealed that there is no entity in Mauritius focused on generating scientific evidence in data governance and neither is it the priority for academic institutions. This does not necessarily mean that there is a total lack of such an institution or entity but may mean that such an institution is not visible online. However, such an institutional gap will mean that there is no robust approach to advancing the knowledge and practice of data governance in Mauritius.

Application of DG frameworks

Like in many other countries, there are data-driven public and private institutions that apply or should apply data governance frameworks. Some of these public institutions in Mauritius include the Ports Authority, the Statistics Mauritius, Economic Crime Office and other national agencies, offices and boards in finance, agriculture, health, transport, justice

[28] https://dataprotection.govmu.org/SitePages/Index.aspx

[29] https://dataprotection.govmu.org/Pages/Downloads/Publications%20and%20Guidelines/Guidelines.pdf

[30] https://dataprotection.govmu.org/Communique/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf

[31] https://ict.io/en/the-national-open-data-policy-set-up-by-the-mauritian-government/

[32] https://ega.ee/project/data-sharing-policy-and-data-architecture-for-mauritius/

[33] https://dataprotection.govmu.org/SitePages/Index.aspx

and security and small, medium, and large-scale businesses that depend on data for their operational functioning that require data governance structures and principles.

Facilitation of FAIR

In Mauritius the Government Online Centre (GOC) is a centralised data centre run by the government of Mauritius to support e-Government services. Set up in 2005, it is managed by the National Computer Board (NCB) and hosts the Government Web Portal (GWP), which provides secured online Government services round-the-clock. The GOC also hosts physical servers as well as cloud environments (g-Cloud infrastructure) for virtual servers providing back-office applications, such as Registry, Central Personnel Systems, Labour Market Information System, Environment Information System, Central Population Database amongst numerous others.

In 2019, the Ministry of Health and Wellness launched a Laboratory Information Management System (LIMS) using an open-source program, known as OpenELIS. This LIMS was deployed to allow for better surveillance and management of the COVID-19 pandemic. Its expansion to a national data warehouse means that the capabilities of the system can be spread to various lab facilities all over the country allowing Ministry of Health and Wellness staff and public health officials to track national COVID-19 cases numbers and trace ongoing and potential outbreaks of COVID-19 and other infectious diseases.

OpenData Mauritius which is the National Open Data Portal is also an Initiative to facilitate FAIR government data and was launched by the Ministry of Information Technology, Communication, and Innovation, in line with the e-Government Strategy and the Mauritian National Open Data Policy. This initiative makes data open and accessible to citizens and businesses for carrying out data-driven initiatives such as the development of mobile apps, data analysis, creation of innovative products and research among others. Also, to promote open data the government has launched the Mauritian Open National Spatial Data Infrastructure (OSNDI) which will act as a common platform for the collection and sharing of geospatial datasets and maps with the aim of facilitating access to geospatial information free of charge while providing tools for analysis. Furthermore, to promote the adoption of open source the NCB has set up a repository for all open-source applications for the benefit of SMEs. These institutions provide infrastructures for FAIR data but particularly government data.

3.1.5 SOUTH AFRICA

Making of laws regulations and policies

The Parliament of South Africa has enacted data-related laws aside from the Constitution. These include; the Electronic Communications and Transactions Act, 2002, Protection of Personal Information (POPIA) Act, 2013 (Act 4 of 2013). There is also the Promotion of Access to Information Act (PAIA) 2000. This is a law that ensures the citizens' constitutional right of access to information held by the government, or any person or entity is ensured. In addition to these, the right to privacy is protected in common law and in section 14 of the Constitution of the Republic of South Africa. Another institution that creates regulations related to data is the Information Regulator[34] which is an independent body established by section 39 of the POPIA. This is an entity which provides guidelines, and creates processes, procedures and policies that help organisations to abide by the provisions of the POPIA. The IR regulates the processing of personal information and the promotion of access to information in accordance with the Constitution and the law to protect the rights of South African citizens.

Monitoring compliance and enforcement

In South Africa, the Information Regulator is charged with monitoring and enforcing compliance by public and private entities with the provisions of PAIA and POPIA. Through different means including creating information officers, codes of conduct, exemptions, guidance notes and guidelines the Information Regulator protects information or promotes

[34] https://inforegulator.org.za/

access to information. They are empowered to handle complaints, litigations and enforcement notices relating to data protection.

Generation of Evidence-based Research

In South Africa several research centres involved in the contribution of knowledge to the field of data governance exist. One of such institutions is the Centre for Human Rights situated in the University of Pretoria which is a research and capacity development centre and plays host to research units for groups or individuals interested in research. The centre comprises internationally acclaimed professors, researchers, and industry experts in various sectors and aims to advance research on issues revolving around human rights, international development, expression, information and digital rights, and democracy and civic engagement among others. Specifically, they have created an online course on digital rights and data protection in the African context.

Another research centre is the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) which is a centre for leading research and advocacy in information and communication technology-related policy issues in East and South Africa. CIPESA aims to improve the effective representation of African interests in policy-making processes and ensure that international policy decisions translate positively impact Africa. The organisation's thematic areas include online freedom, open data and e-governance, internet governance and ICT for democracy. They regularly research and release publications within their thematic areas, including African data governance. The organisation's board consists of academics, researchers, and advocacy experts. Their work often contextualises the African perspectives in relation to global issues, and they collaborate with similar-minded organisations to achieve their goals.

The Centre for Competition, Regulation and Economic Development (CCRED), University of Johannesburg (CCRED) is also a research and capacity development centre focused on the generation of evidence-based research around data governance. The centre's research focuses on three strategic areas; competition and barriers to entry, regional value chains, local industrial development and inclusive growth. In their work around local industrial development, they have researched data governance issues and complications in South Africa.

Application of DG frameworks

In South Africa public and private entities are compelled by the information regulator to apply the POPIA in order to comply with the lawful processing of personal information. One of such scenarios is the use of an Information Officer as defined in terms of POPIA section 55 (2). According to the POPIA, the accounting officer of a public body and a head of a private body by virtue of their positions are by default the Information Officer (IO) unless they are exclusively defined. In terms of POPIA, the IO encourages compliance with the 8 conditions for lawful processing of personal information, and in terms of the Promotion of Access to Information Act (PAIA) the IO ensures voluntary disclosure of information and accessibility to information held by the public or private body. This shows that almost all data-driven entities in South Africa are expected to apply DG frameworks to the processing of data as provisioned in the POPIA.

Facilitation of FAIR

South Africa is considered as the home to the majority of data centres in Africa. With around 55 data centres currently mostly located in or near the urban centres of Cape Town and Johannesburg, South Africa alone accounts for 54 percent of the raised floor space for the entire African continent. Therefore, it is not surprising to find out that a lot of public and private open data initiatives exist in South Africa. Some of the notable open data initiatives include the South African Environmental Observation Network (SAEON)[35], Stats SA,[36] Datafirst,[37] the E-government Portal,[38] The

[35] https://ulwazi.saeon.ac.za/about/

[36] https://www.statssa.gov.za/

[37] https://www.datafirst.uct.ac.za/about-us

[38] https://www.eservices.gov.za/tonkana/home.jsf

South African Cities Open Data Almanac,[39] and Open Data South Africa[40] which is encouraging wider use of government data in communities around South Africa for social impact.

This section has shown the overview of available data governance institutions in these countries but also the significant institutional gaps that exist. Whereas there are institutions responsible for making data protection laws, which is only a part of data governance, there is no national or regional institution focusing on data governance as a whole. This means that other data types (non-personal data, animal data and technical data) and other aspects of data governance such as data quality, integrity and usability are left ungoverned. There are also evident gaps as regards institutions that monitor compliance and enforcement. These institutions are created to monitor compliance with data protection regulations and mostly lack independence from government control. There are no regulations or laws on data governance as a whole, therefore there are no agencies for compliance monitoring. The paucity of institutions focused on generating evidence-based research to inform and shape data governance theoretically and practically is identified. In addition to data governance, related disciplines such as data ethics, computer ethics and Technology ethics have also not received adequate attention in academic curricula and research. Furthermore, there is no shortage of data-driven institutions that should be applying data governance frameworks but only a handful of these institutions in Africa are applying DG principles in their data processing pipelines. Finally, institutions that can facilitate FAIR are critically lacking in Africa. There is an emergence of open data spaces for public data but other data spaces such as Health data, industrial data, mobility data, financial data, energy data and agriculture data lack crucial infrastructure to ensure the findability, accessibility, interoperability, and reusability.

4. DATA GOVERNANCE INSTITUTIONS IN AFRICA: DPA OPERATIONAL AND CAPACITY NEEDS

To understand the institutional capabilities and capacities for data governance, Data Protection authorities (as institutions designed for monitoring compliance and enforcement) in the selected countries. The reason behind the choice of DPAs is that data protection has emerged as a major aspect of the data governance ecosystem in Africa. DPAs provide a structured framework for addressing the legal challenges around personal data processing. DPAs are commissioned to create, enforce, or monitor the regulations and policies related to data protection. Three high-level parameters revolving around enabling infrastructure for data governance, systems, and processes to support efficient data governance structure and around organisational culture adequate for data governance were used to identify the needs of DPAs. These questions revolve around the three critical elements of data governance; people, processes and technology and are as follows:

Organisational culture, built around people with the right skills and experience, which meets the needs of stakeholders (e.g data subjects, data generators and data users)

- Having the right mix of expertise, skill set and knowledge in the workforce to support the evolving regulatory landscape of the data economy (e.g capacity development trainings, stakeholder engagement)
- Reflecting contextual African values as well as promoting equality, diversity, and inclusion in a way to drive sense of shared ownership of data

Systems and processes that support efficient data related policies for the right stakeholders

- Having a clear policy methodology - supporting the development of iterative regulations and policies in a modern, open and collaborative manner which reduce burdens on business, provide increased regulatory certainty and reduce risk for those who are regulated.

[39] https://scoda.co.za/scoda/#/home

[40] https://opendataza.gitbook.io/toolkit/

- Monitoring and enforcement plans/mechanisms, and
- Risk assessment approaches for decisions and actions in line with the need to protect data rights, promote innovation, growth, and competitiveness.

Enabling infrastructure/technologies for adequately responding to the views and needs of data stakeholders

- Available technologies and technical knowledge to support effective and efficient delivery of services to stakeholders.
- Available funding and resources that can be deployed to meet demands; sustainable funding model

4.1 ORGANISATIONAL CULTURE, BUILT AROUND PEOPLE WITH THE RIGHT SKILLS AND EXPERIENCE, WHICH MEETS THE NEEDS OF STAKEHOLDERS (E.G DATA SUBJECTS, DATA GENERATORS AND DATA USERS).

Data governance requires the right people with the right expertise, skills and experience. These include legal experts, forensic investigators, data ethics experts, public policy specialists, ICT experts, and data analysts, among others. It also requires an organisational culture independent of government influences since it is supposed to govern data processing activities in both public and private sectors.

Nigeria: National Information Technology Development Agency (NITDA) is an agency created to implement the Nigerian Information Technology Policy and coordinate general IT development in the country that ended up as the Data Protection Authority. Its primary mandate was not to implement Data Protection principles. The implication of this is that there was a pool of ICT expertise to harness together but insufficient expertise in law and ethics. We however note that beginning from 2022, the responsibility for administering and enforcing data protection in Nigeria now rests on the Nigeria Data Protection Bureau (NDPB). As a regulatory agency NITDA was reported to have lacked the resources to employ sufficient people with the right skills to cover the whole country and to respond to the unique contexts and concerns of data stakeholders in Nigeria. In addition, the organisational culture of NITDA and possibly NDPB is judged to be mired in conflict of interest owing to their lack of independence (Alao, 2022). NITDA was run under the general supervision of a government ministry, the Federal Ministry of Communications and Digital Economy and NDPB's independent status is not yet assured. The independence of a regulatory body such as that is relevant because the government collects more personal data than most large corporations in Nigeria.

Kenya: The Act provides that the Data Commissioner shall be required to consult with the Cabinet Secretary in establishing the directories. The compulsory involvement of the Cabinet Secretary and the Ministry of ICT means that the ODPC is dependent on government institutions. Although the ODPC is no longer dependent on the Ministry of ICT to provide funding because the National Assembly allocates an annual budget to the commission, the Commissioner (Immaculate Kassait) has been vocal on the need for increased funding to enable the Commission to fulfil its mandate.[41] To ensure that the Commission has the right people for effective compliance, OPDC developed strategies for capacity development. This includes training of staff and other stakeholders on conducting inspections on data controllers and data processors as well as on emerging technologies, and existing guidelines through the development and implementation of a data protection online training curriculum.

Mauritius: The Data Protection Office under the administrative control of the Data protection commissioner is an independent agency that was provided for by law and has so far made 70 decisions at the time of writing this report.[42] According to information from the DPO's annual report,[43] this agency has reported insufficient funds to secure a

[41] http://vellum.co.ke/data-protection-commissioner-announces-opportunities-for-the-odpc-and-stakeholders-to-collaborate-during-dual-data-protection-report-launch/

[42] (https://dataprotection.govmu.org/Pages/Decisions/Decisions-on-Complaints.aspx).

[43] https://dataprotection.govmu.org/AnnualReports/Annual%20Report%202021.pdf

secondment of police officers for prosecution. They also mentioned that they didn't have enough money to hire staff and therefore are understaffed. Finally, qualification deficits amongst legal practitioners

Morocco: The CNDP organises frequent training in 2013 and 2014 but the frequency of the training has reduced progressively since 2013. The DPA is however yet to organise any since the 2019 Data Protection Day.

South Africa: The Information Regulator was established by the provisions of section 39 of the POPIA and is only subject to the law and the constitution. This makes it an independent agent. In terms of staff expertise, the IR appears to have the same makeup as the other studied DPAs in the sense that it is made of staff with a lot of legal expertise. In its 2019/2020 annual report, the IR pointed out that inadequate funding was preventing the full implementation of its mandate.

On the issues of reflecting African values and promotion of inclusion and empowerment of stakeholders, we found that none of the regulations nor the DPAs acknowledged African values but made references to principles of autonomy, justice, transparency, and accountability. While these are critical principles that should underline data protection, African contextual principles of solidarity and interconnectedness are conspicuously missing. However, in relation to inclusion and empowerment of stakeholders, we found the following:

Nigeria: The Nigerian DPA (NITDA) has carried out the following activities with respect to stakeholder inclusions and partnerships: (a) NITDA published the NDPR Performance report for the year 2019-2020 to give all stakeholders the opportunity to understand how the Agency has fared in the implementation of the NDPR. This understanding would generate further research and provide guidance to other regulators, partners, data controllers, data processors and all other stakeholders. (b) NITDA also issued an implementation framework to guide stakeholders on how the GDPR should be implemented. (c) As one of its capacity-building and awareness events, NITDA also organised a Stakeholders' workshop on the NDPR Implementation Framework in Lagos and Abuja. (d) NITDA has developed a draft DPCO Code of Practice (Code) to entrench professionalism and regulate the activities of the DPCOs and will be released upon consummation of the stakeholders' engagement process.

Morocco: The **National Control Commission for the Protection of Personal Data** (CNDP) has initiated a DATA-TIKA programme and entered into strategic partnerships with both public and private institutions including the Casablanca Stock exchange, Morocco Numeric cluster, UMR5, Moroccan Federation for the Outsourcing of Services, MDJS (Moroccan Games and Sports), Moroccan Agency for Energy Efficiency (AMEE), Caisse de Dépôt et de Gestion (CDG), the ministry of health and OCP and Mohammed VI Polytechnic University (UM6P) among others. The DPA has also entered into partnerships outside of the Data-TIKA programme with government bodies, private sector players and multinationals for the protection of personal data in Morocco.

Kenya: With respect to stakeholder inclusion, we note that the ODPC has included empowering data controllers and processors through training programmes to enhance compliance with the provisions of the Act as one of its strategies for awareness creation. Since its establishment in 2020, the ODPC has organised Sixteen (16) virtual and physical awareness creation and consultation forums with various stakeholders drawn from the public, private sector, and development partners. In addition, it has developed a training curriculum, developed a draft data protection curriculum which is awaiting stakeholders' validation and approval by Kenya School of Government (KSG) council and commissioned a training needs assessment.

Mauritius: As part of its stakeholder engagement, the Data Protection Office in Mauritius delivers regular presentations; some are made at the request of controllers to provide training to their staff, others at the request of associations or organisations. Through the in-house training initiative introduced in 2018, this office provided training on provisions of the DPA to Data Protection Officers of the public and private sectors to help them implement the DPA in their respective organisations. The DPA is also a major stakeholder in Government projects which involve the processing of personal

data of individuals. In 2020, the office provided its recommendations on many projects such as the Laboratory Information Management System for Covid 19, Airport Health Laboratory, SIM Card Regulations, Mobile Application for Gender-Based Domestic Violence, Advance Passenger Information and Passenger Name Record (API/PNR) System, amongst others.

South Africa: The Information Regulator has embarked on various stakeholder engagements to increase its visibility, raise its profile and create awareness of POPIA amongst data subjects and responsible parties. These stakeholder engagements were held in various formats and at various fora such as public lectures, face-to-face consultations, and training on POPIA as well as presentations at a number of workshops and conferences. The Regulator lists amongst its activities, stakeholder engagements with both the private and the public sectors which include, but are not limited to institutions of higher learning, law enforcement agencies, the telecommunications sector, and the financial services sector.

4.2 SYSTEMS AND PROCESSES THAT SUPPORT EFFICIENT DATA RELATED POLICIES FOR THE RIGHT STAKEHOLDERS

We also explored available **policy methodologies** of these DPAs. The critical question was whether they have the right policies, enforcement plans and mechanisms and assessment approaches that can support diverse stakeholders. Only in two countries did we find stakeholder participation in policy development.

Nigeria: We found that NITDA issues draft versions of its policies and regulations to the public to receive comments from individuals and relevant stakeholders. An example is the NDPR implementation Framework which had 3 publicly available draft versions before the final version was issued. This is a policy methodology that helps to consider stakeholder concerns.

South Africa: The South African DPA has a sub-programme for research and policy. This sub-programme is responsible for the development of policy and the conducting of research. The methodology adopted by the sub-programme for the development of policies is centred on robust research and stakeholder involvement.

On **monitoring and implementation plans**, we found the following;

Kenya: The DPA's implementation plan is to ensure enforcement of the Data Protection Act; establish and maintain a register of data controllers and processors; promote self-regulation among data controllers and data processors; conduct assessments; receive and investigate any complaint by any person on infringements of the rights under the Data Protection Act, 2019; carrying out of inspections of public and private entities with a view to evaluating the processing of personal data; promoting international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements.

Mauritius: The DPA engages in sensitization, training, and investigation of breaches and has a register of controller and processor which enables it to monitor data protection compliance. It also has a privacy compliance assessment portal in its website.

Nigeria: The Nigerian DPA (NITDA) inaugurated a Data Breach Investigation Team to monitor and investigate compliance. NITDA was also working with the Nigerian Police to enforce the NDPR[44]. The DPA website is also enabled to receive reports and complaints for any breaches of the data protection law. The DPA issued an Implementation Framework for better understanding of data protection compliance and inaugurated a Data Breach Investigation Team to facilitate compliance. However, the focus was mainly on data protection and less attention was paid on promotion of innovation.

South Africa: According to the Annual Report for 2020/2021, The IR monitors compliance with POPIA and PAIA and is developing guidance notes relating to online safety and appropriate, reasonable, technical, and organisational measures to prevent loss of, or damage to, or unauthorised destruction, and unlawful access to personal information.

[44] https://nitda.gov.ng/nitda-to-collaborate-with-nigeria-police-on-npdr-enforcement/

The Regulator is also developing a breach notification form to ensure that the reporting of data breaches follows the provisions of POPIA. The IR also has a compliance and monitoring Sub-programme of the Protection of Personal information division of the Information regulator. This sub-programme is responsible for the monitoring and enforcement of compliance by public and private bodies in accordance with the provisions of POPIA. Under the sub-programme compliance and monitoring, the following was achieved as per the Annual Performance Plan for 2021: (a) Approved Guidelines for Codes of Conduct were published and implemented; (b) Readiness Plan for POPIA was developed, approved, and implemented; (c) Guidelines for registration of Information Officers were approved and published; and (d) Drafting of the Guide for POPIA and PAIA. The Information regulator publishes annual performance plans for each financial year that contains Quarterly Targets for the years in question and a Performance Matrix with Outcomes, Outputs, Indicators and Targets for the financial year. The IR has a risk management policy in place as part of its governance mechanism.

One of the most critical elements of an efficient regulatory ecosystem is the ability to evaluate the established systems and processes to understand what is working and what does not work. This provides an opportunity to improve the processes. These evaluation mechanisms can include risk assessment and general policy assessments. None of the DPAs studied have information on evaluation mechanisms apart from Nigeria. While there is no document setting out the evaluation mechanisms put in place by NITDA, we note that NITDA conducts public surveys and also requests stakeholders' comments and feedback on its policies, guidelines and implementation framework before issuing final versions. In a survey conducted in July 2020, 74% of the respondents opined that the NDPR met the need of the Nigerian environment; 76% said the unique introduction of Data Protection Compliance Organisations (DPCOs) helped in their compliance with the NDPR. 72% noted that NITDA has provided requisite support for industry adoption of the NDPR. The rate of public awareness was put at 54%. 85.3% of the respondents stated that compliance with the NDPR enhances good perception about their business. However, the effectiveness of the implementation and enforcement plans are limited by the lack of independence of many of the DPAs.

4.3 ENABLING INFRASTRUCTURE/TECHNOLOGY FOR ADEQUATELY RESPONDING TO THE VIEWS AND NEEDS OF DATA STAKEHOLDERS

The infrastructure for effectively responding to data stakeholder needs include technologies, technical knowledge, and experience, as well as funding resources. In its technology strategies DPAs should be able to identify priority areas that include cybersecurity, Artificial Intelligence, big data, machine learning and web and cross device tracking. These are technologies considered critical to the implementation of the data protection in our tech-driven data processing activities. The adoption of technologies to ensure effective education and awareness for staff. DPAs should be able to provide effective guidance to organisations about how to address data protection risks arising from technology, to ensure that the public are aware of data protection risks arising from technology, to recruit and retain staff with technology expertise to establish new partnerships to support knowledge exchange with external experts, to engage with relevant stakeholders on technology issues related to data protection and to engage with organisations in a safe and controlled environment to understand and explore innovative technology. These are objectives that are not clear from studying these five DPAs in Africa- in their current activities and in their available strategies. It is not clear if this lack of prioritisation of technology is informed by these DPAs being underfunded.

During the FG, representatives from the DPAs were reluctant to provide any information related to available funding mechanisms for their operations. The unified perspective of the participants was that DPAs generally are underfunded and that a greater efficiency of the operations of the DPAs requires more appropriate funding. There was also no publicly available information on funding for these DPAs other than the following information; In its 2020-2022 report, the **Mauritian** DPA reported that it got Rs5.5 million funding. The Nigerian[45] and South African[46] DPAs didn't provide exact funding numbers but alluded to a situation where their activities were hampered by lack of funds. We however experienced difficulties obtaining funding information on the DPA from Morocco due to language barriers and translation difficulties.

[45] https://ndpb.gov.ng/Files/NDPR%20(Lite)%20Performance%20Report%20%202019-2020.pdf

[46] https://www.justice.gov.za/inforeg/docs5-pp.html

To **summarise** findings from the DPAs, the lack of DPAs' independence from government control stands out. Not being able to independently hold the government accountable for data processing activities that occur in public institutions puts data subjects and other data stakeholders at risk. It is also obvious that these institutions lack the technical tools, skills, and systems to support the effective and efficient monitoring of compliance and enforcement in ways that consider the unique contexts and circumstances of Africa. This includes knowledge management systems and Enterprise resource planning (ERP), systems for efficient internal operations that includes risk management and compliance. This is mostly because these agencies are significantly underfunded and lack the financial capacity to acquire or deploy physical, technical and people resources to meet the demands of the data subjects and data generators. Engagement of relevant stakeholders is also very low and there is clear evidence that policy methodologies are not robust (transparent and collaborative) enough. There is no consistent approach to risk management as regards decisions and actions that prioritise privacy rights and well as promote innovation. We have also identified that DPAs are yet to be built around organisational culture, sensitive to African values, interests, and expectations, with the right people with the right skills, expertise and experience that meets the needs of all relevant stakeholders.

5. IMPLICATIONS FOR THE AFRICAN DATA ECONOMY

Institutional Gaps

From the findings, it is obvious that an efficient data governance ecosystem in Africa involves institutions that can ensure the availability, usability, integrity, security and quality of data shaped by functional regulations, contextual ethical principles and technical infrastructure. It should be about sustainable institutions that can ensure that data is made available for the benefit of businesses, public administrations, the environment, and the citizens. To ensure that Africa harnesses the benefits of data, it is clear that data protection regulations are insufficient. The data spaces in Africa require data governance laws. Without such laws, critical elements of data governance will be ignored, and crucial issues left unaddressed. Personal data is not the only form of data that requires governance structures. Optimal maximisation of all forms of data (including environmental data, animal data, mobility data, agriculture data and transport data) depends largely on efficient governance mechanisms. As data-driven innovations become central to business operations and public service delivery, it is important for these businesses to find, access, interoperate and reuse datasets. Without such possibilities through established institutions, businesses will lack the capability to efficiently detect business opportunities, minimise time-to-market and be able to have a competitive advantage. Most importantly, without institutions that generate evidence-based research, the operationalisation of data governance in Africa will be 'stuck in the mud' and not be able to keep up with the constantly changing socio-cultural and technological landscape.

Institutional Capacity Needs

In considering the capacity needs of the compliance and enforcement monitoring institutions, it was evident that identified gaps and needs can have impact on existing and potential data economy. Effective monitoring of compliance and enforcement of data protection provisions imbues trust. It is important for data subjects to see data-driven organisations as trustworthy institutions. A strong data protection implementation and enforcement help foster citizens' trust and increased use of digital tools, which in turn can lead to more investment, competition, and innovation in the digital economy. Therefore, it is important to address the identified capacity needs of the DPAs including making them independent of any government control.

6. RECOMMENDATIONS

In building a functional data economy in Africa, there is a need to develop an ecosystem of functional institutions with identifiable stakeholders (policymakers, industry, academia, and citizens). This will lead to a greater free flow of data

that can open more business opportunities and increase the availability of knowledge base and possible capital as well as facilitating critical research and innovation for human flourishing in Africa. As data generation, application and sharing continues to expand in Africa, we propose the following recommendations for key stakeholders in Africa.

Policy Makers

Establish data governance laws

Data as "any digital representation of acts, facts or information …"[47] has tremendous value and benefits for businesses and society at large. A data governance law or regulation that goes beyond the consideration of just data protection is designed to maximise this value; to increase the amount of data available for re-use and foster advanced application for operations, research, and innovation. There is a need for national or regional data governance laws but preferably an Africa-wide regulation that can allow wider access to data without jurisdictional constraints. If possible, at the continental level. Policymakers in Africa need to jettison the increasing need to create protectionist data governance systems. Such a siloed system hurts rather than protects people and businesses. Creating an ecosystem characterised by solidarity, openness, transparency, responsibility, and justice is needed for improved stimulation of research and innovation as well as efficient delivery of products and services. Particularly a functional digital technology ecosystem in Africa will be dependent on a harmonised data governance ecosystem. Therefore, there is a need to initiate multi-stakeholder partnerships and collaborations to develop the mechanisms for a socially acceptable and legally compliant data governance framework for Africa.

Assure the Independence of Compliance and Enforcement Monitoring agencies

The independence of DPAs and other established institutions for monitoring compliance is critical to the effectiveness of implementation of established laws and regulations. Responsible mitigation of risks to citizens apparently depends on this.

Create Funding mechanisms for Data governance

Given the required scale of impact, an efficient data governance ecosystem for a competitive data economy needs sufficient funding; not only for the existing DPAs but also for new data governance agencies to shape and maintain potential data governance laws. This is a fact that policy makers should appreciate. From the findings, it is obvious that a responsible data governance landscape in Africa will have tremendous impacts on businesses, public service delivery and crucial research and innovations. Variety of funding mechanisms including international collaborations and public-private partnerships should be explored to fund data governance initiatives.

Be committed to community building and Public Engagement

Strategic cooperation via a public-private partnership (PPP) is critical to the development of a functional data economy in Africa. The African Union and other regional bodies should be able to initiate PPP programmes that can encourage exchange of best practices as an important element of the African data governance ecosystem. PPPs can address the challenges of resources and develop incentives to share data between partners, facilitate knowledge and technology transfers and promote digital entrepreneurship. Community building also involves creating effective pathways of conducting public engagement exercises that can educate the public on their rights and the responsibilities of those who process their data. The public debates that ensued over the use of health data in the wake of the COVID-19 pandemic (Sleigh and Vayena, 2021) is a lesson on the need for public engagement in data governance.

Integrate African socio-cultural Values into Data governance processes

African peculiar socio-cultural values are currently overlooked in the available institutional data governance processes and frameworks. Data does not only underline business and public operations and services, but it also shapes value-

[47] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

laden innovations such as AI. If African values are missing from this ecosystem, an important question becomes; whose values and interests are these built on? It is important for policy makers to consider the integration of relevant ethical principles and values specific to African socio-cultural contexts into data governance frameworks. Lack of African values in data governance structures could potentially lead to transposition of culturally noncompliant data governance models in Africa. It is therefore critical for Africa's data governance ecosystem to be founded on African norms and values, whilst taking into consideration the diversity of African culture, individual peculiarities, jurisdictional needs, and sensitivities.

Industry

Build solid data infrastructures for FAIR

Open data repositories, portals, platforms, archives, data trusts and research infrastructures that support data-driven innovation which are important for a data economy are currently lacking in Africa. This is partly because of the lack of necessary fast internet and computing resources (High Performance computing (HPC), grid and cloud computing infrastructures). Stakeholders in the industry have major roles to play here. These infrastructures or institutions can ensure that data is FAIR (Findable, Accessible, Interoperable and Reusable) and compliant. The future of many data spaces (e.g health data, mobility data, agriculture data) is dependent on this.

Create Data Governance Roles

The findings of this research show that many data-driven institutions have no data governance roles within their data processing workflow. IT experts within the organisation who are not trained for data governance are asked to fulfil data governance responsibilities. To harness the full value of the data within the organisation, it is important for data-driven institutions to proactively create data governance roles, and this involves provision of necessary resources (including funding and technologies) and being committed to capacity development of the workforce to appreciate the importance of DG.

Go beyond Regulatory Provisions

To build trust with data subjects, clients, customers or business partners, there is a need for private data-driven institutions to go beyond the provisions of the law. Most of the available jurisdictionally constrained regulations are insufficient to guide responsible actions on data. Data governance structures should touch on ethical and wider societal concerns which can influence how data is processed and shared.

Academia

Improve Data Governance skills base:

Stakeholders in academia need to understand their role in training a sufficient number of data governance experts to meet the demand in the labour market. This involves integrating modules on computer Ethics, data ethics and data governance into Data science and Computer science curricula. It also involves the efficient cross-pollination of talent and skills from diverse fields of study; an interdisciplinary collaboration with industry and policy makers that can ensure the availability and further development of reliable processes and technologies for responsible data governance managed by people with the right technical, legal and ethical knowledge or expertise.

Facilitate Data Governance Awareness

Stakeholders in academia have a duty to provide evidence-based insights into the criticality of data governance. Such robust insights based on research can become a major driver for public and private institutions, businesses and citizens to recognise the importance of data governance. A pointer to this is the role academia played in the public's understanding of health data use during the COVID-19 pandemic (Akintoye et al., 2021; Staunton et al., 2021; Li, Ma and Wu, 2022).

Citizens

Know your data rights

The understanding of data rights among African citizens is still very low. Many Africans are unaware of the value of their data, the implication of processing their data and the rights to hold over their data. It is time for Africans to become more aware of the value of their value to the institutions that process their data and the risks this has for them. Such knowledge can help citizens to ensure that their data is well protected.

Keep data-driven institutions accountable

It is important for citizens and most importantly civil society groups to ensure that data driven institutions adhere to the principles of transparency, accountability, and justice. This does not entail uninformed pressures being put on institutions but involves purpose-driven and meaningful engagement with these institutions to ensure that risks are mitigated, and benefits are harnessed and shared equitably.

7. CONCLUSIONS

This research has revealed that there are identifiable institutional gaps in the African data governance ecosystem regarding institutions that; create or make data governance laws, monitor compliance and enforcement, generate evidence-based research, apply data governance frameworks, and facilitate FAIR data principles. There are existing, albeit disparate data protection regulations/laws and no laws for governance as a whole in Africa. However, there is no evidence of African ethical principles and values at the foundations of these laws, nor is there any of the available data governance processes and procedures. What is evident is that available DPAs have significant capacity needs that form barriers to an efficient implementation of the provisions of the regulations. These include a lack of the right mix of relevant expertise, skills and knowledge, lack of resources, lack of clear policy methodology, monitoring approaches, enforcement plans, and risk assessment approaches. contribute to the existing inefficiency of data governance mechanisms. It was also evident that data-driven institutions have similar challenges including but not limited to lack of the motivation to initiate data governance processes, lack of required skills, insufficient capacity development, lack of stakeholder engagement, lack of consideration of African values and norms and finally, the lack of necessary technical infrastructure for data governance.

These findings reinforce the understanding that a functional and responsible data governance ecosystem in Africa requires close cooperation and collaboration between stakeholders: policymakers, industry, academia, and citizens. Thus, our recommendations are focused on these stakeholders to ensure maximum results. Whilst each of these stakeholders has specific roles and responsibilities within diverse institutions, a multilateral collaboration between them will lead to optimal outcomes.

REFERENCES

Akintoye, S. et al. (2021) Understanding the perceptions of UK COVID-19 contact tracing app in the BAME community in Leicester. *Journal of Information, Communication and Ethics in Society*.

Alao, O. (2022) *The Nigeria Data Protection Bureau And The Challenges Of Data Privacy Compliance In Nigeria - Privacy Protection - Nigeria*. Available from : https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-data-protection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria [Accessed 25/06/22].

Babalola, O. (2022) Nigeria's data protection legal and institutional model: an overview. *International Data Privacy Law*, 12(1), pp. 44–52.

Chen, W. (2010) *A brief history of data governance. Magnitude*.

Eke, D. et al. (2022) Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural concerns. *Journal of Responsible Technology*, p. 100039.https://doi.org/10.1016/j.jrt.2022.100039

Eke, D.O. et al. (2021) International data governance for neuroscience. *Neuron*. https://doi.org/10.1016/j.neuron.2021.11.017

Larus, J. (2020) Joint statement on contact tracing: Date 19th april 2020. *Retrieved December*, 2, p. 2020.

Li, V.Q.T., Ma, L. and Wu, X. (2022) COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia. *Policy and Society*, 41(1), pp. 01–14.

Merkus, J., Helms, R. and Kusters, R. (2019) Data Governance and Information Governance: Set of Definitions in Relation to Data and Information as Part of DIKW Filipe, J and Smialek, M and Brodsky, A and Hammoudi, S (ed.). *PROCEEDINGS OF THE 21ST INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS (ICEIS 2019), VOL 2*, pp. 143–154.

Micheli, M. et al. (2020) Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2), [Online] Available from: doi.org/10.1177/2053951720948087.

Ndemo, B. and Thegeya, A. (2022) A Data Governance Framework for Africa.

Osakwe, S. and Adeniran, A.P. (2021) Strengthening Data Governance in Africa.

Sleigh, J. and Vayena, E. (2021) Public engagement with health data governance: the role of visuality. *Humanities and Social Sciences Communications*, 8(1), pp. 1–12.

Staunton, C. et al. (2021) The governance of personal data for COVID-19 response: perspective from the Access to COVID-19 Tools Accelerator. *BMJ Global Health*, 6(5), p. e006095.

Wilkinson, M.D. et al. (2016) The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, 3(1), p. 160018.