Blog

Data Governance Echoes

Leveraging digital technologies to enhance data governance practices in Africa

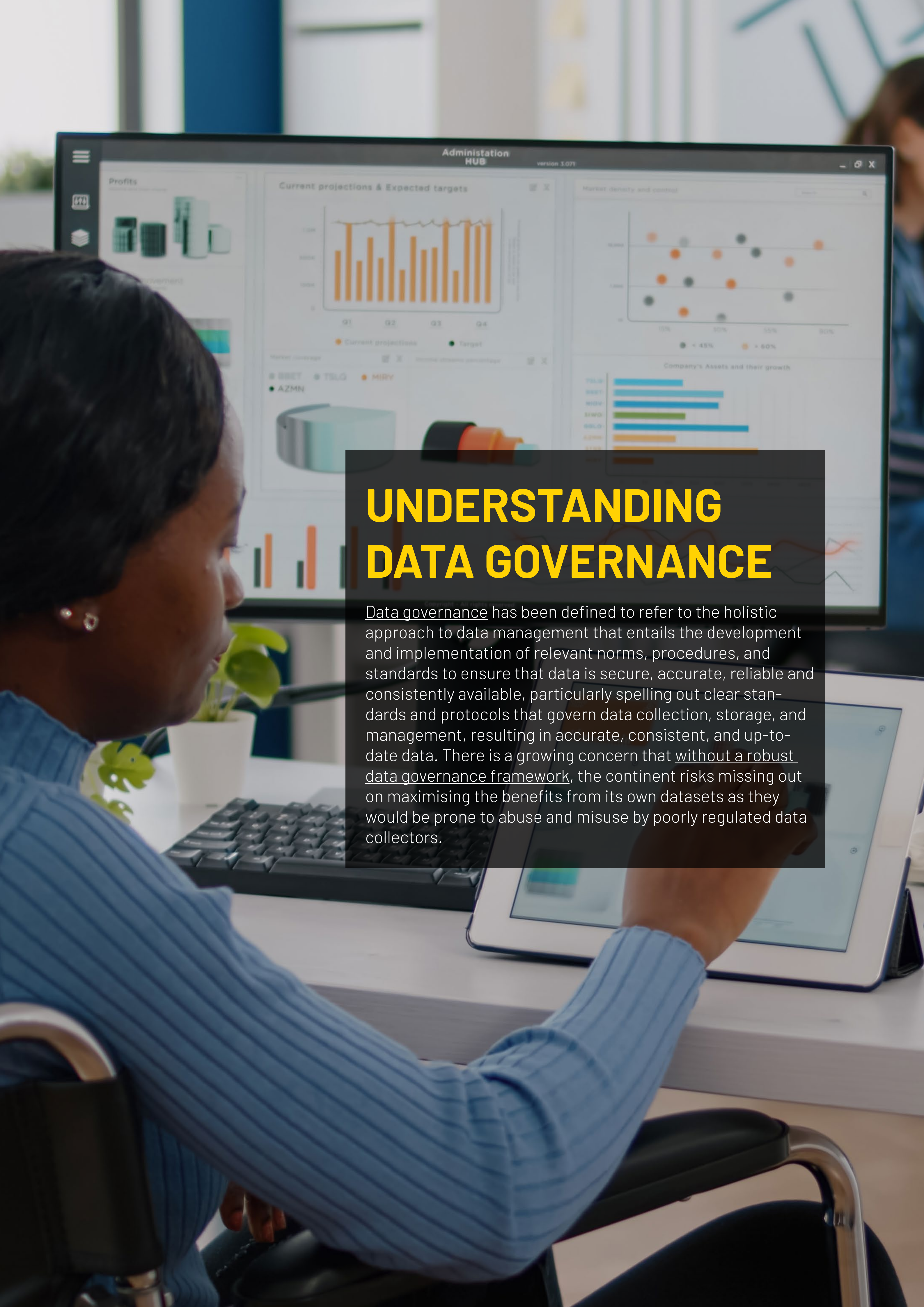
niYel
CHANGE CREATORS

CIPESA

LUX MEA LEX
SIGILLUM UNIVERSITATIS CHEIKH ANTA DIOP DAKARENSIS

The current data governance policies and practices in Africa have continued to attract attention due to their inadequacy in ensuring the protection and respect for the rights of individual data subjects. Key concerns have been raised regarding the data management practices, particularly related to biometrics, that have undermined the safety, confidentiality, accuracy, accessibility, and reliability and of personal data, which are critical principles in data governance. Several studies have documented cases of misuse of digitalised personal data including data breaches, surveillance, misuse of personal information, unwarranted intrusion, and financial harm. Despite these misgivings, digitisation of data has been recognised within the African Union's Digital Transformation Strategy for Africa (2020-2030) as critical in promoting and building confidence for the continent's digital economy. For many governments, the desire to transform service delivery and enhance public participation has been in a key driver for their adoption of biometric data collection and digital identities for purposes of issuance of National Identity cards, updating of biometric voter registration and identification programmes.

In this blog, we highlight the critical areas in which advances in digital technologies can enhance data governance practices in Africa.


Administration HUB
Profits
Current projections & Expected targets
Q1
Q2
Q3
Q4
Current projections
Target
AZMN
MIRY
Company's Assets and their growth

UNDERSTANDING DATA GOVERNANCE

Data governance has been defined to refer to the holistic approach to data management that entails the development and implementation of relevant norms, procedures, and standards to ensure that data is secure, accurate, reliable and consistently available, particularly spelling out clear standards and protocols that govern data collection, storage, and management, resulting in accurate, consistent, and up-to-date data. There is a growing concern that without a robust data governance framework, the continent risks missing out on maximising the benefits from its own datasets as they would be prone to abuse and misuse by poorly regulated data collectors.

DEMAND FOR A ROBUST DATA GOVERNANCE

In Africa, the demand for a robust data governance framework has gained traction as a response to several countries moving away from paper-based to more digitised data management practices, raising serious concerns about the rights of data subjects, particularly the safety and confidentiality of user data.

While progress has been registered normatively – with the adoption of the regional instruments such as the African Union Convention on Cyber Security and Personal Data Protection and the AU Data Policy Framework, both of which provide frameworks for rights' respecting data protection practices, and with several countries adopting relevant privacy and data protection frameworks, full implementation has remained a challenge.

In addition, African Union's Digital Transformation Strategy for Africa (2020-2030), calls upon to "promote open data policies that can ensure the mandate and sustainability of data exchange platforms or initiatives to enable new local business models, while ensuring data protection and cyber resilience to protect citizens from misuse of data and businesses from cybercrime."

Unfortunately, several laws contain problematic and vague provisions that provide for sharing of sensitive information and data localisation that are prone to abuse and misinterpretation. For example, legal provisions such as section 18 of Algeria's Law No. 18-07 of 2018 on the protection of personal data, Part V (section 44-47) of Kenya's Data Protection Act 2019, and section 9 of Uganda's Data Protection and Privacy Act, 2019, provide for circumstances under which sensitive personal information can be accessed, such as safeguarding national security, public interest, enforcement of the law, and conduct of criminal investigations. In addition, in many countries, biometric data collection programs were initiated before the enactment of relevant data protection laws.

LEVERAGING DIGITAL TECHNOLOGIES

While for the most part digital technologies have been used by states to undermine the legitimacy and enjoyment of digital rights through surveillance and interception of communication, internet shutdowns, and data breeches, there is a growing belief that these technologies can be instrumental in building a robust data governance framework if applied correctly.

Ease of Authentication

Recent technological advancements including the multifactor authentications (MFA) that enable secure access to services on the go are critical in facilitating seamless data collection, processing, verification and enhance the authenticity and reliability of data compared to paper-based identifiers. Data subjects can easily request access to and verify their digitised data in the possession of data controllers. As technology becomes more accessible and affordable, governments and private entities can leverage biometrics and biometric technologies for functional and foundational identity purposes, and for an expanding array of applications.

Improving Data Storage and Confidentiality

Data storage is a key pillar within the data governance framework as it easily allows data subjects to exercise their individual rights to request and obtain their personal data in the hands of data controllers in a structured, commonly used, and machine-readable format, as well as request that their data be transferred directly to another organization. With advances in technology, data controllers can easily encrypt, deidentify and destroy personal data in their possession. Technologies such as the Identity Management Systems (IDMS) facilitates for interoperability, allowing seamless integration between different data management systems used by data controllers. In addition, new technologies such as blockchain facilitate the secure storage of datasets in blocks that are connected through cryptography.

Ease of Data Rectification

One of the fundamental rights of data subjects is the right to request data controllers to correct any inaccurate and incomplete data the data controller may have collected. Under Principles 5 and 16 of the European Union's General Data Protection Regulation (GDPR), data controllers are required to keep personal data accurate and up to data (where necessary), including taking "every reasonable steps" to ensure that inaccurate personal data is erased or rectified. In many countries, data controllers, have been accused of collecting and processing inaccurate and incomplete personal data due to the analogue way data is collected. The adoption of digital technologies and use of biometric data identifiers such as fingerprint, facial, or iris recognition become critical forms of authentication in issuing different forms of identities as well as easing on the verification and rectification processes by both data subjects and controllers.

As Africa strives to improve its data governance-framework, it is important that we leverage on the new and emerging technologies such as biometric data collection, blockchain, identify management systems to enhance the safety, security, accuracy, reliability and confidentiality of personal data.

Paul Kimumwe
Senior Program Officer/ CIPESA

CONTACTS:

Paul Kimumwe
E mail: paul@cipesa.org
https://cipesa.org

Niyel
E mail: info@niyel.net
www.niyel.net