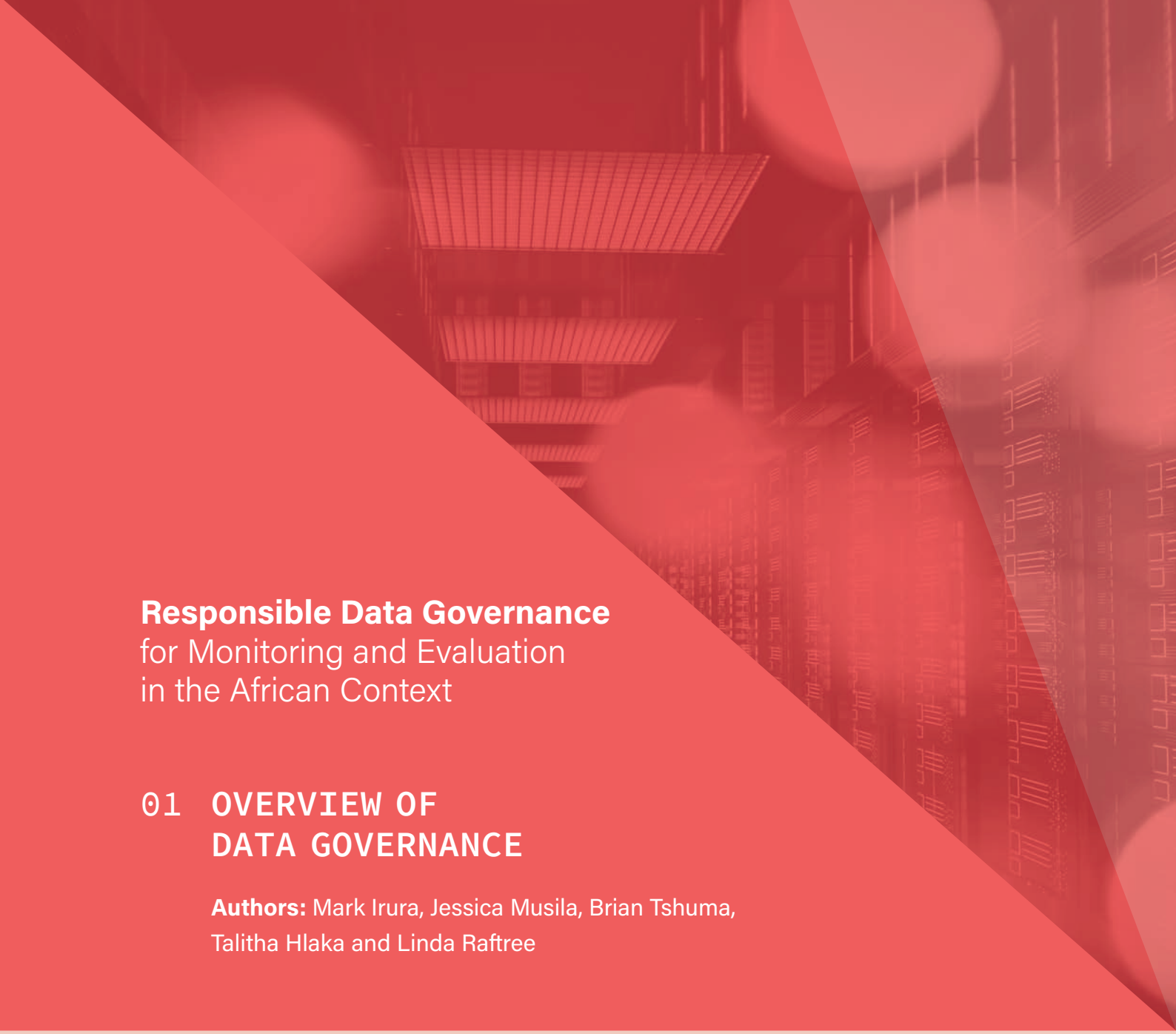
Responsible Data Governance
for Monitoring and Evaluation
in the African Context

DECEMBER 2021

01. OVERVIEW OF DATA GOVERNANCE

MERL Tech
UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
clear
Centers for Learning on Evaluation and Results
ANGLOPHONE AFRICA



Responsible Data Governance for Monitoring and Evaluation in the African Context

01 OVERVIEW OF DATA GOVERNANCE

Authors: Mark Irura, Jessica Musila, Brian Tshuma, Talitha Hlaka and Linda Raftree

Summary of the publication: This publication includes two sections. The first section gives an overview of data governance and how it relates to the field of monitoring and evaluation (M&E), with a focus on M&E in the African context. The second section provides guidance on how M&E practitioners can more responsibly manage data in their practice. The publication was developed and compiled by a group of M&E professionals and data privacy experts over the course of 2020 and 2021.

Suggested citation: Centre for Learning on Evaluation and Results – Anglophone Africa (CLEAR-AA) and MERL Tech (2021) "Responsible Data Governance for Monitoring and Evaluation in the African Context. Part 1: Overview of Data Governance and Part 2: Guidance for Responsible Data Governance in Monitoring and Evaluation." Faculty of Commerce, Law and Management | University of the Witwatersrand, Johannesburg, South Africa.

ACKNOWLEDGEMENTS

We acknowledge the working group members who contributed to the framing, writing and revisions of this document. Without their ongoing support and work, this document would not have been possible.

- Monet Durieux, Senior Associate, Genesis Analytics, South Africa.
- Ilse Flink, Researcher, VVOB, Rwanda.
- Jerusha Govender, Co-founder and Director, Data Innovators, South Africa.
- Mark Irura, Technical Advisor, GIZ Kenya.
- Desiree Jason, Director for Policy and Programme Evaluation, National Department of Social Development, South Africa.
- Jessica Musila, Founder and Lead Consultant, Shomer Consulting, Kenya.
- Brian Tshuma, Partner (Data & Capital Markets) at Deme Attorneys, Zimbabwe.
- Rachel Sibande, Programme Director, Data for Development, Digital Impact Alliance, Malawi.

We thank Talitha Hlaka, Communications Officer, CLEAR-AA, South Africa, Linda Raftree, Independent Consultant and Co-Founder of MERL Tech, United States of America, and Dugan Fraser formerly of CLEAR-AA and currently at the Global Evaluation Initiative (GEI), South Africa, for guiding and supporting this process from start to completion.

Many thanks also to Dr Candice Morkel, Director of CLEAR-AA, and Steven Masvaure, Senior Monitoring and Evaluation Technical Specialist at CLEAR-AA for funding this work and providing feedback on the various versions of the document.

FOREWORD

COVID ripped away the curtain that had veiled much of contemporary global society and revealed much that we already knew but chose not to discuss. One of the things clearly revealed by COVID is the extent to which we now rely on digital communication platforms and the essential role they will play in our lives in future.

The fuel that drives these platforms is data of various kinds. It's being widely noted that data can be understood to be the new oil: a precious resource that needs careful, prudent management and careful consideration of its use and abuse. The counterpoint is that if data is the new oil, privacy is the new climate change. States, governments, companies, institutions and individuals must be mindful of responsible data management in the knowledge economy, because if they aren't, the damage will be deep, profound and potentially irreversible.

"Big Data" and the "Data Revolution" are not just buzz-words but are real and present features of our current lives. Anyone in any position of authority needs to undertake a mindful, thoughtful consideration of the systems and frameworks that guide our management and use of data. We also need to take better account of the effects of unethical and irresponsible data governance on society, communities and individuals.

Monitoring and evaluation are at the forefront of the "data revolution" and have been since the outset of the digital era. As we become aware of the perils of weak data governance, both monitoring and evaluation need to reflect deeply on how to improve their practices and meet the emerging standards for good practice as responsible citizens in the global data ecosystem.

The sector – its practitioners and institutions who use M&E for purposes of accountability and evidence-informed decision-making – have a responsibility to ensure that the quality, relevance, accessibility and timely production and use of data ultimately improves lives and does not create opportunities for exploitation and exclusion. Data protection and integrity need to be placed front and center of these processes, given that the production and use of data is the fulcrum around which M&E revolves.

We are very pleased to present this Guide for Responsible Data Governance for Monitoring and Evaluation in the African Context. This Guide is the first of its kind for the African continent and was produced by the RDiME Alliance – a diverse team of experts in data laws, Monitoring and Evaluation, and government, together with CLEAR-AA and MERL Tech. We are very grateful to the members of the Alliance for their unflagging enthusiasm and the passionate way they approached the task. We hope the Guide will act as a call to action for responsible data governance for M&E in Africa.

Prof Dugan Fraser, Program Manager, Global Evaluation Initiative (GEI) and Dr Candice Morkel, Director, CLEAR-AA

TABLE OF CONTENTS

GLOSSARY

Consent refers to any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

Data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

Data disaggregation: Statistics are mostly disaggregated by sex (both state and non-state actors), education levels, age (both state and non-state actors), location, and in some instances, disability. Disaggregation, especially by gender, enables us to understand trends and patterns but more importantly, develop evidence-based policies.

Data ethics deals with our moral obligations regarding data. Legal obligations must be adhered to when handling data, but ethics extends beyond legal obligation. Rather than ask can we legally do something with data, an ethical approach urges us to ask whether we morally should do something with data. Data ethics require us to think about the short- and long-term implications of decisions about data and whether decisions we make about data could lead to harm, especially when working with vulnerable people and groups.

Data governance refers to the different organising, decision-making, and accountability processes utilised by organisations, companies, local and national governments, and global entities to manage, control, share and exercise power over data. Because much data is derived from or is about people, data governance decisions are also decisions about managing, controlling, influencing and protecting people.

Data literacy is critical to ensure that a continuous supply of data feeds into planning and decision making for improved service delivery. Both state and non-state actors drive data literacy. Data education and data literacy are important – whether they relate to respondents' understanding of the important role of data collection and their responses to enumerators or relates to citizens being able to interpret data.

Data ownership stipulates as data is an enterprise asset, no single individual, department or organisational area can claim ownership over data. However, to govern and manage data appropriately, organisations must identify and assign certain roles and responsibilities to staff members, a process known as data ownership. Data owners have a clearly outlined role that determines who is permitted to access data in adherence with security protocols, privacy requirements, compliance management issues, among others.

Data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data sources: Both state and non-state data producers collect and utilise data from both primary and secondary sources. All counties, county governments and Ministries, Departments and Agencies (MDAs) use primary sources of data from administrative systems such as those used in the agriculture or health sectors (for instance DHIS7) or use data obtained from surveys conducted using structured/unstructured interviews and observations, such as in the agriculture sector. Non-state actors employ both quantitative and qualitative methods, but the use of qualitative methods is more common. These include unstructured interviews, surveys, focus group discussions, public forums and observations) of data collection, and extensive desktop research.

Data stewardship: refers to the accountability and responsibility for data and the associated processes to ensure the effective control and use of data.

Data subject is an identified or identifiable natural person who is the subject of personal data collection.

Data validation: The quality of methodology and research design manifests during data validation. Data validation refers to the process of checking the accuracy and quality of data before it is processed. Methodological rigour is important if the data obtained from studies and research is intended to inform decision and policymaking.

Evaluation is the planned and periodic assessment of the results of a programme and is based on several key areas including appropriateness, effectiveness, efficiency, impact and sustainability. An evaluation focuses on assessing the extent of the short- to medium-term outcomes and the longer-term impacts; the intended and unintended effects of these achievements; and an assessment of the approaches that worked well or did not work well and identifying the reasons for success or failure and the lessons learned from each outcome. The evaluation process also provides an assessment of the value of the programme or project in terms of cost effectiveness and value for money.

Governance refers to the ways that societies or groups within societies organise themselves to make decisions. The aim of governance is to decide who has a voice in making decisions, how decisions are made, and who is held accountable.

Learning is the intentional process of applying the knowledge, evidence and learning from M&E activities to improve development outcomes and ensure accountability for the resources used to achieve programme outcomes. Learning should not be undertaken only at the conclusion of a programme but should also take place at regular intervals during the programme execution and the information obtained should contribute to the improvement of the programme. Learning should also be shared both internally and externally with relevant stakeholders.

Monitoring is the continuous and systematic process of collecting and analysing data related to a programme or project with the aim of tracking the progress against set goals and objectives. Monitoring focuses on processes (activities and outputs), but also monitors outcomes and impacts, as per the evaluation plan.

Non-traditional data is data collected from sources other than traditional and conventional sources. It includes location data from satellite imagery, data collected through e-government platforms, payment data from smartphones, traffic data from applications (apps), biometric data from wearable devices, data collected via social media platforms, and search engine data.

Personal data or Personally Identifiable Information (PII) is data that relates to an identifiable, living, natural person, for example, an identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assigned to a person.

Processing of data is any operation or set of operations which is performed on personal data or on sets of personal data either by physical or by automated means including collection, recording, organisation, structuring, storage, adaptation or alteration; retrieval, consultation or use; disclosure by transmission, dissemination, or otherwise making available; alignment or combination; restriction; erasure; or destruction.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of other information. To ensure that people are not identifiable, the complementary identifying information must be kept separately in such a format that further technical processing is necessary before it can be used.

Research is a process of new knowledge creation and/or using existing knowledge with the aim of generating new and additional understanding. Research can be used in the M&E process to determine the assumptions underlying a Theory of Change and to adapt and improve programme activities.

Responsible data and 'data responsibility' are terms that have emerged in the human rights, humanitarian and development sectors over the past decade. They describe the ethical, do-no-harm and duty of care approaches that should be in place when collecting and using data, especially data from or about vulnerable, minoritised or historically marginalised individuals or groups. A responsible data approach requires the user to define which data is sensitive and could potentially cause harm or impact negatively if accessed or disclosed without authorisation, and to make efforts to ensure that no harm is done as a result of data breaches.

Sensitive Personal Data is data that requires greater levels of protection given that it poses greater privacy risks. It includes:

- Information related to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person.
- Information related to the education or the medical, financial, criminal or employment history of the person.
- The biometric information of a person (e.g. blood type, fingerprint, DNA analysis, retinal scanning, and voice recognition).

Third parties are natural or legal persons, public authorities, agencies or other bodies, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

Traditional data refers to data collected by public organisations including household surveys, censuses, labour force surveys, administrative data records (birth registrations) or public opinion surveys conducted by private companies.

INTRODUCTION

Background

Governance of personal and sensitive data has become increasingly important in the digital age due to the abundance of data being collected – both with and without the knowledge of individuals – and the emergence of new and diverse data sources. In the world of development, the launch of the United Nation's Sustainable Development Goals (SDGs) saw an accompanying push for a 'data revolution'. This included commitments to improve the statistics and information available to citizens, to leverage technology in the improvement of monitoring systems, to document progress and shortcomings, and to support data sharing for better decisions.[1] It was suggested that to attain the SDGs and improve measurement of their achievement, a major transformation of data ecosystems at country and regional levels was needed to improve the availability of quality, relevant, accessible, and timely data that could help strengthen accountability and improve service delivery.

While there was movement towards increasing digitisation in the decade prior to the 2020 outbreak of COVID-19, the advent of the pandemic significantly hastened the adoption of digital platforms and tools that enabled activities and services to proceed, despite travel restrictions, lockdowns, quarantines, and social distancing mandates. The move to digital programmes and service implementation has meant that an increasing amount of personal and sensitive data is being collected and stored.

The increased use of digital platforms and services has prompted public concern around data protection. Data breaches, misuse of data, misinformation, and unethical use of data to manipulate social media users have prompted questions around the safety of individuals' personal and sensitive data in the hands of corporations who monetise the information for profit. In some cases, national and foreign actors have used personal data to 'micro target' individuals and direct content towards them that affects how they vote and how they perceive political and cultural agendas. Government surveillance using personal data has become a concern for many people. Both authoritarian regimes and democratically elected governments use personal data to track and monitor their populations in opaque and undisclosed ways.[2]

Civil society and service organisations such as education, health, and social welfare or protection agencies, have also increased the amount of digital data that they collect and use, often in partnership with governments and/or corporations. This has led to concerns that data from highly vulnerable individuals – children, refugees, victims of domestic abuse and COVID-19 positive persons – could potentially be used in harmful or unforeseen ways or could be accidentally shared, breached or leaked.[3] As partnerships between government, corporate, and civil society sectors multiply, the amount of data shared across these sectors increases, opening the door to potential scope or function creep when it comes to data. In other words, data collected by a civil society organisation working to protect highly vulnerable groups could feasibly be shared with a corporation for marketing or profit purposes. Data collected through an app developed by a private sector company could be shared with a government for surveillance that could potentially harm individuals from a particular race, ethnicity, political affiliation, gender, or other grouping.

Monitoring and evaluation (M&E) practitioners often collect highly sensitive personal data from vulnerable or marginalised individuals and groups, and therefore have a significant role to play in the development data ecosystem. Whether working independently, within civil society organisations, at international agencies, or within government, it is important for M&E practitioners to ensure that the data they collect is kept safe and used ethically and appropriately. In addition to the broad ethical principles that should frame any research (especially research involving human subjects), M&E practitioners should be aware of and compliant with data protection laws and other laws and guidelines in place in many African countries[4] (at national, regional and international levels). They should also consider the potential consequences of data processing, especially for those who could be at risk or harmed by data misuse or unauthorised data sharing or access.

While most M&E practitioners receive standard training on important data-related aspects such as research ethics and principles (respect for persons; beneficence/non-maleficence; justice; informed consent; confidentiality and data protection; integrity; conflict of interest)[5], gaps in knowledge and skills have emerged as a result of rapid advances

in digital technologies used for data collection, use, storage and analysis. While the uptake of data protection laws in Africa between 2000 and 2010 was slow,[6] the past decade has seen 15 African countries[7] developing data privacy bills and laws regulating how data is governed by corporations, governments, civil society, researchers, and the media, including social media.[8]

A guide to Responsible Data in Monitoring and Evaluation (RDiME)

It is in this context that the Responsible Data in Monitoring and Evaluation (RDiME) initiative was launched in June 2020. CLEAR-AA and MERL Tech, two organisations involved in strengthening capacities in M&E and digital approaches, joined forces to hold a series of events under the theme "How to conduct digital MERL during COVID-19" with the goal of understanding how monitoring, evaluation, research, and learning (MERL) were changing as they digitised. Sessions covered new data sources and types (for example, data collected online or via mobile devices, data collected on paper and subsequently digitised, and big data collected by the private sector such as mobility data and call detail records) and how these new kinds of data can be used for decision making, better development outcomes, measuring progress, and understanding impact.

While there is an abundance of guidance available on conducting M&E, the event series highlighted the knowledge gaps that exist in the use of digital data, big data, administrative data, and digital systems in the African M&E context. Notable challenges were identified in relation to the lack of awareness of data protection, data privacy laws and regulations, and the ways in which these impact M&E processes and influence donor compliance requirements. As the context shifts, there is a greater desire by national governments and donors to use digital data collection and advanced data analytics for M&E with a concomitant stronger focus on data privacy and security and emerging data regulations[9]. These trends are evident in the wider literature on the topic and are highlighted throughout this paper.

Following the event series, An RDiME working group was formed to share expertise and produce insights on data governance, data ethics, and data management for M&E practitioners. The group comprised individuals with experience in M&E, digital approaches, research, data privacy law, and data protection. The goal was to stimulate cross-disciplinary conversations and insights to help the African M&E sector improve its knowledge, skills, and capacities related to responsible data governance and data management. Two leading organisations in M&E and digital data – CLEAR-AA and MERL Tech – stewarded the process.

The RDiME working group consisted of the following individuals:

- Monet Durieux, Senior Associate, Genesis Analytics, South Africa.
- Ilse Flink, Researcher, VVOB, Rwanda.
- Jerusha Govender, Founder and Manager, Data Innovators, South Africa.
- Talitha Hlaka, Communications Officer, CLEAR-AA, South Africa.
- Mark Irura, Technical Advisor, GIZ Kenya.
- Desiree Jason, Director for Policy and Programme Evaluation, National Department Social Development, South Africa.
- Jessica Musila, Founder and Lead Consultant, Shomer Consulting, Kenya.
- Linda Raftree, Independent Consultant and Co-Founder, MERL Tech, United States of America.
- Rachel Sibande, Programme Director, Data for Development, Digital Impact Alliance, Malawi.
- Brian Tshuma, Partner (Data & Capital Markets) at Deme Attorneys, Zimbabwe.

The working group formulated guidelines aimed at providing M&E practitioners with information on responsible data governance and practical management of data in safe, secure, and ethical ways. It was evident that more needs to be done to improve understanding and promote the uptake of responsible data governance practices. It was clear that these practices should include state actors who are the main duty-bearers of governance in terms of enacting and enforcing regulations and for the implementation of M&E.

The guide aims to promote the use of a more rigorous approach to the application of data governance in M&E[10] and to frame good practices that M&E practitioners can incorporate into existing guides, practices and internal policies.

Data governance is a fundamental component of effective, ethical, and equity-driven data analytics. Sound data governance practices underpinned by a commitment to social justice and protection from harm can contribute to better decision making and better development outcomes. Whereas addressing the asymmetry problem remains a broad and complex legal consideration and research process (which is outside the scope of this paper) the guide provides M&E practitioners in the African context with a point of reference and sound recommendations for handling personal and sensitive data. Additionally, a new body of work is emerging offering counternarratives on issues related to agency, local knowledge, and the strength of cultural contributions made by African communities in terms of data gathering and sharing. Further commentary and discussion on this topic will follow in this guide.

Data is not simply passive information and statistics; for many it is a source of legitimacy and impacts daily lived experiences.[11] Because the world of digital data and technology changes rapidly and national regulations are evolving, the guide will be a living document that will be periodically reviewed and updated.

Who should use this guide?

This guide is appropriate for all levels of M&E practitioners in all sectors – public or private sector or civil society. Although many of the concepts, principles and guidelines have global relevance, it is particularly targeted at individuals and organisations working in Africa, as new laws are emerging. We have approached data governance from a project level rather than adopting a 'whole of government' or 'whole of organisation' approach. We recognise that further work is needed in the broad area of institutional data governance and how organisations involved in M&E should respond to the challenges at this level.

Overview of the guide

Part 1: Data governance in M&E in the African context

The first part of the guide focuses on the theoretical aspects of data governance with particular emphasis on personal and sensitive data and examines the present state of Africa's data ecosystem and includes the M&E practices of the various actors involved. It describes the African contextual reality in which no single, common law exists to govern data practices, unlike the European Union which is governed by the General Data Protection Regulation (GDPR). At the continental level, there are a number of regulations, including the African Union Convention on Cyber Security and Data Protection, 2014 (or the Malabo Convention),[12] the Supplementary Act on Personal Data Protection of within the ECOWAS, 2010,[13] the Internet Society and the Commission of the African Union's Personal Data Protection Guidelines for Africa[14] and the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019.[15] Overall, African countries vary significantly in terms of their political economies, administrative, technical, financial, and human resource capacities, all of which influence the adaptability and limitations of data ecosystems, thereby creating significant challenges to the notion of the viability of a single law that would be applicable across all contexts.

At the centre of the data revolution in Africa is a growing concern surrounding data rights which looks beyond privacy and ownership and which focuses on the freedom of data subjects to protect themselves from undesirable invasion of privacy from corporations, organisations and states. This is because it is almost impossible to detach data governance from the emerging technological trends of the data revolution. The ongoing debate centres on which models of data governance are best suited for the continent, considering that individual countries have varying levels of sophistication. To answer this critical question, this section discusses these issues and concludes with an examination of the European Union's (EUs) General Data Protection Regulation (GDPR) and other alternative models adapted in other countries, with specific reference to Kenya.

Note: See the glossary on pages iv-v for key definitions and concepts.

Part 2: The responsible data governance guide for African M&E practitioners

The second part of the guide provides a practical approach to responsible data governance of personal and sensitive data in Africa and shows the intersection between the M&E cycle and the data life cycle.[16] While those who work in the M&E space have varying levels of responsibility and decision-making power, all M&E practitioners should be aware of and strive to manage data ethically and responsibly. The data life cycle journey comprises seven stages, starting with the design and planning stage applicable to the full data lifecycle, including legal aspects, data sharing plans,

risk-benefit assessment, and budgeting. The second stage involves collecting or acquiring data, the risk-benefit of data collection, data minimisation, informed consent, and ethical review/institutional review boards. The third stage relates to responsible M&E data transmission and storage and includes information for practitioners on data security during transmission and storage, a review of third-party vendors, and data breach protocols. The fourth stage focuses on responsible M&E data cleaning, analysis and use, and guides practitioners through responsible processes and steps such as data quality standards and data anonymisation. The guide to the fifth stage provides an orientation on safe and responsible data sharing and open data, as well as guidance on establishing data sharing agreements based on the distinct roles that individual entities play. The sixth stage includes information on responsible M&E data visualisation and communication offering guidance on M&E communication, from identifying audience requirements to designing data visualisations that avoid biased interpretations and meet specific objectives. It includes detailed guidance on data visualisation and lessons from COVID-19 visualisations, including data visualisation considerations for effective and optimal communication. The seventh and last stage focuses on responsible data retention, maintenance and destruction, drawing the attention of practitioners to the importance of managing personal and sensitive data from data 'birth' (collection) to data 'death' (aggregation, anonymisation, or deletion).

In conclusion

It is our hope that this guide will assist African M&E practitioners in their daily interaction with M&E data and will encourages all those in the profession to insist on and implement ethical approaches to data governance and its social justice and equity imperative. We trust that ensuring more ethical and just data collection, management and use, will not only protect the privacy of data subjects but ensure the transparency and validity of the data collected thereby contributing to dignified and ethical development processes. We welcome feedback on the use of the guide and encourage readers to share the guide with fellow M&E practitioners.

SECTION 1

Data governance and M&E in Africa

Authors: Mark Irura, Jessica Musila, Brian Tshuma, Talitha Hlaka and Linda Raftree

Data governance refers to a set of rules and norms related to why and how data is captured and used, and who is responsible for the process. Extending beyond the aspects of data management, data privacy, and data protection, data governance includes the end-to-end policies, strategies, standards, rights, and accountabilities for data.

While data governance is an important concept for all types of data (including non-personal data), in this guide we focus on personal and sensitive data management and the legal and ethical frameworks applicable to its management. This is an evolving area with new challenges and has prompted new legislation and regulation at national levels. M&E practitioners have noted the need for guidance and training in this area as the foundations of M&E lie in the capture of personal and sensitive data from highly vulnerable individuals, groups, and organisations. We cover both the ethical and legal aspects of personal and sensitive data governance as it is evident that the law currently lags behind technological and digital advances. In addition, highly vulnerable groups, for example, refugees, might not have access to the same protections as less vulnerable groups. The fields of social science, including research and M&E, subscribe to a general code of ethics regulating the capture and use of data from human subjects. It is important to extend these ethics to the digital realm, yet many M&E practitioners have not been trained on the ethical aspects of digital data nor on how to protect and manage personal and sensitive data collected in the digital era.[17]

1. The data revolution in Africa

In 2013, the UN High-Level Panel of Eminent Persons on the Post-2015 Development Agenda recommended two transformational shifts in international development. The first was a data revolution for sustainable development backed by the commitment to improve the quality of statistics and information available to citizens.[18] The second was a push for a more rigorous monitoring system for Sustainable Development Goals (SDGs) that leverages technology to document progress and shortcomings and enables sharing of information with decision makers and the public.[19] The panel also called for a major transformation of data ecosystems at country and regional levels in response to the need for quality, relevant, accessible, and timely data to strengthen accountability and improve service delivery.

The Partnership in Statistics for Development in the 21st Century (PARIS21) and the Mo Ibrahim Foundation reiterated these calls for improving the production and use of data for evidence-based policymaking in Africa. Their working paper released in 2021 provides recommendations for national statistical offices and governments to bridge the data policy gap in Africa.[20] Various authors note that whereas emerging technologies and expanded access to and use of digital and mobile communications present new opportunities for Africa to harness new data sources for sustainable development, the increase in digitisation also presents new challenges. These include trust in data, privacy protection and effective data governance.

> The United Nations Independent Expert Advisory Group on the Data Revolution for Sustainable Development defines the data revolution as an "explosion in the volume of data, the speed with which data are produced, the number of producers of data, the dissemination of data, and the range of things on which there is data, coming from new technologies such as mobile phones and the 'Internet of things', and from other sources, such as qualitative data, citizen-generated data and perceptions data". In their view, the data revolution includes a growing demand for data from all parts of society (United Nations, 2014).

At the national level, commitment to the data revolution has been incorporated in long-term development plans and reforms aimed at achieving the transformation of data ecosystems. The breadth of these commitments is evident in the Africa Data Consensus, the African Charter on Statistics, and the African Union's (AU's) Agenda 2063.[21]

Yet, countries still face challenges despite investments to strengthen national statistical systems and support evidence-based decision making. Some of these challenges include:

1) Lack of disaggregated data (especially at the hyperlocal level);
2) Infrequent data collection for official statistics which makes operational planning difficult;
3) Missing data (that is simply not collected by the National Statistical Offices - NSO); and
4) Poor collaboration between state and non-state actors on the potential complementary effects of official and non-official statistics.[22; 23; 24]

It is important to note that these challenges may be rooted in a lack of regular funding as well as interference (political or other) in the production and publication of statistics. 'Official statistics' are statistics produced and published by governments or government agencies and they must be approved by a person of a certain designation in the government. Official statistics often extends to data 'produced' by UN agencies and other multilateral organisations. 'Non-official statistics' are produced by non-government organisations and/or departments, such as independent research bodies, academia, civil society organisations, the private sector and even citizens.[25] (These definitions are revisited in detail in the subsequent section that discusses the components and stakeholders of the African data ecosystem). At times, non-official statistics are also produced by government departments for their own internal use.

In terms of the responsibilities for data protection and ethics, the following specific challenges were cited at the 2020 gLOCAL Evaluation week event:

1) Poor practice of informed consent.
2) Data collection gatekeeping by government and other non-state actors leading to biased results.
3) Technology advances that allow disaggregated data to be de-anonymised.
4) Research bias – especially on data from African contexts.
5) Poor data quality and problems with research validity and reliability.
6) Inadequate automation for digitisation of records.
7) Fatigue of communities on data collection.

Technological advancements, access to information laws, the spread of open data initiatives, and the increasing involvement of non-state actors in the data ecosystem are some of the requisite core elements necessary to realise the continent's development data needs.[26] A comprehensive approach which includes both the creation of an enabling environment for leveraging data and the establishment of partnerships to generate data for the continent's various development priorities, has also been recommended.

There has been considerable innovation and experimentation in African countries, within multiple data communities and ecosystems. However, these efforts have been small-scale pilots, siloed or ad hoc initiatives.[27] For the data revolution in Africa to be truly catalytic, systematic, large-scale, integrated, and sustainable efforts are necessary.

In Africa the building blocks already exist for a data ecosystem capable of harnessing the data revolution to accelerate sustainable development. There are multiple dynamic data communities including official statistics and private-sector entities, civil society and citizen-based data groups working with data, and scientific, open, and big-data communities. The necessary legal and policy frameworks are already in place at national and regional levels to enable environments and governance frameworks for harnessing the data revolution. These include the African Charter on Statistics[28] and the Strategy for the Harmonization of Statistics in Africa.[29]

> The Africa Data Consensus, developed at the High-Level Conference on Data Revolution held in Addis Ababa, Ethiopia in 2015, defines the African data revolution as: "A profound shift in the way that data is harnessed to impact on development decision-making, with a particular emphasis on building a culture of usage. The process of embracing a wide range of data communities and diverse range of data sources, tools, and innovative technologies, to provide disaggregated data for decision-making, service delivery and citizen engagement; and information for Africa to own its narrative". The Consensus views the data revolution as a "partnership of all data communities that upholds the principles of official statistics as well as openness across the data value chain, which creates a vibrant data ecosystem providing timely, user-driven and disaggregated data for public good and inclusive development" (United Nations, Economic Commission for Africa, 2015).

Substantial investment is still required in Africa's data ecosystems to finance the human resources, technological capabilities, platforms, and tools for effective governance frameworks. The investment is necessary for the production, processing, protection, ownership, quality, openness, timeliness,

relevance, accessibility, harmonisation, interoperability and use of diverse types of data, regardless of who ultimately produces or owns data.[30]

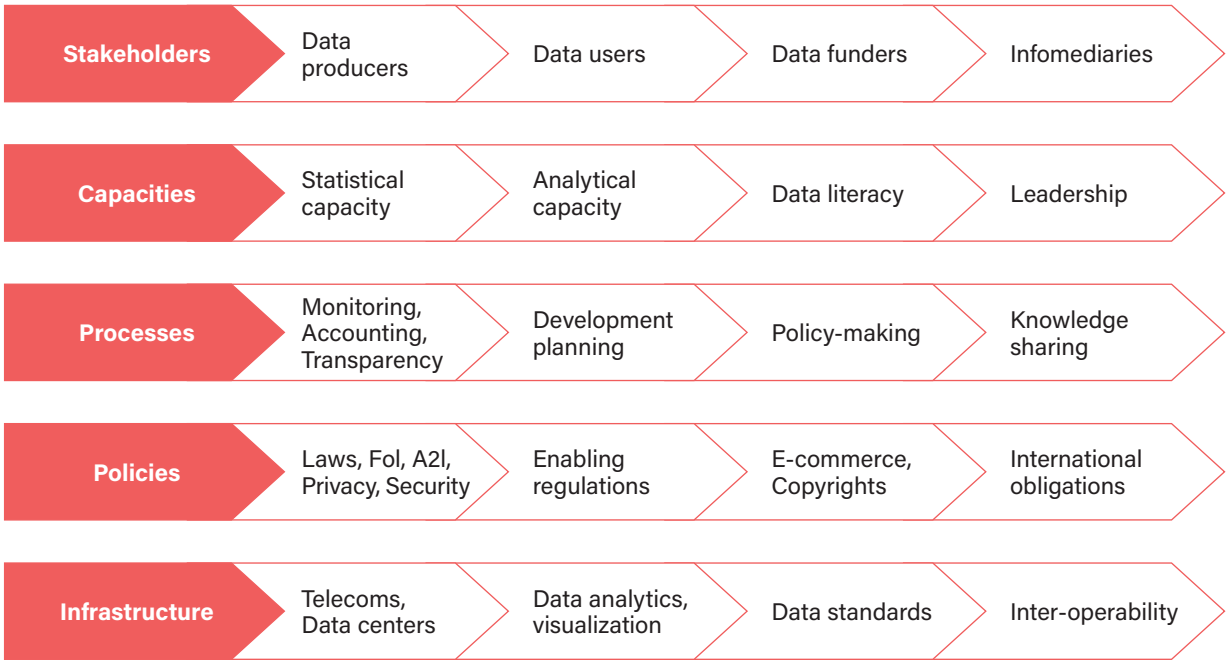
Despite these deficits, as African countries move towards their commitments to realise the AU's Agenda 2063 and the SDGs,[31] a fundamental conceptual and paradigmatic shift is taking place. This relates to who and what officially counts and is counted – how, by whom, for whom, and for what purpose.

2. The African data ecosystem

Components and stakeholders

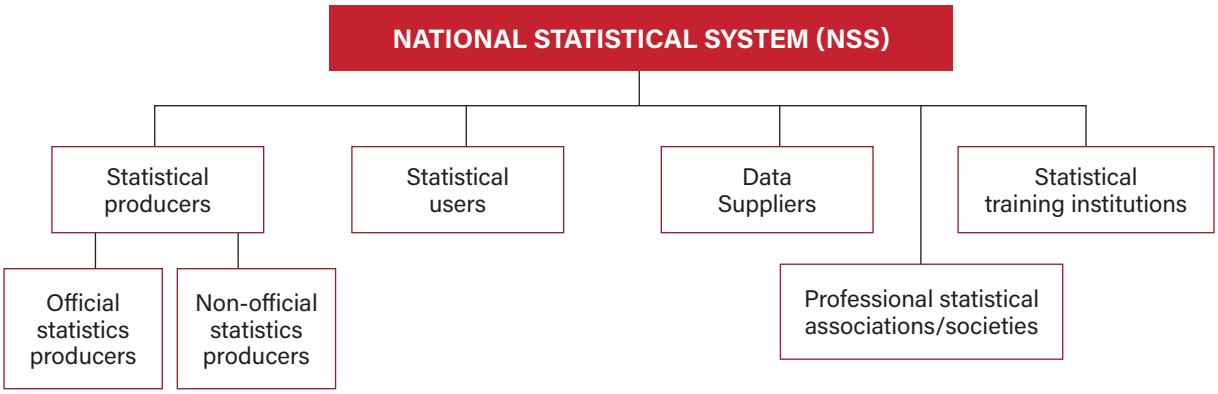
Though not unique to the African context (or homogenous within it), the data ecosystem is a complex web of relationships between individuals, organisations, datasets, standards, resources, platforms, and other elements that define the environment in which each data resource exists.[32] This ecosystem encompasses multiple data communities; distinct types of data; institutions, laws and policy frameworks; technologies, platforms and tools; and the dynamic interactions among the actors within prevailing technological, infrastructural, legal, policy and other constraints. Note that Information Technology (IT) is just an enabler; the interaction between people, processes, technology, and culture ultimately drives the success of data governance.[33] The diagram below developed by the United Nations Development Programme (UNDP) explains these components. Cultural aspects are closely related to establishment of institutional skills and capacities. Without clear identification and addressing of all components, it is not possible to move from an ad hoc state to a mature, focused process of data governance that is striving for continuous improvement.[34]

Figure 1: Components of a data ecosystem (Source: UNDP, 2017[35]).



The key stakeholders have been identified above as have their roles within the ambit of official and non-official statistics. However, there is much broader and more nuanced conversation around national statistical systems. In 2016, Msokwa identified a major problem which was that many African countries (and beyond) mistakenly regard the National Statistical System (NSS) as the producer of official statistics. Furthermore, the head of the NSO is generally appointed to be in charge of the NSS – a position that Msokwa argues is improper because it starves countries of vital statistical activities because there is no space for contributions through statistical activities by non-state actors, including M&E practitioners. This is especially the case where the government of the day is not accommodative of such activities.[36] The author advocates for five (5) pillars (each with its responsibilities) through which equilibrium could be built in the National Statistical System:

Figure 2: Components of a National Statistical System (Source: Msokwa, 2016[37]).



1) Statistics users: There is a wide range of statistics users in every country from government to non-state users and development partners.
2) Statistics producers: These can either be official or non-official. Statistical activities employ either qualitative[38] or quantitative[39] research to better understand phenomena. NSOs, ministries, departments and agencies as well as local governments are notable official statistical producers. Non-official statistical producers include CSOs, the business community, faith-based organisations as well as academic and research institutions.
3) Data providers/suppliers: Data providers – whether individuals, private or public organisations – are the sources of the data that is collected. Without providers, the reliability and quality of the data is difficult to ascertain. Therefore, data suppliers need to be to be well informed on the intention of any data collection exercises and the importance of the data and evidence to society as a whole. Communities should not be burdened with too many data requests because it may result 'survey fatigue' – especially if no accruing short- or long-term benefits are evident as a result of the survey information provided.
4) Professional statistical associations/societies: The primary objectives of a professional entity are educational and informational. They help to define and set standards for their professional fields and to promote high standards of methodological rigour and quality.
5) Statistical training institutions: These institutions assist to establish equilibrium. This prompts Msokwa's (2016) call for professional statisticians and statistical training institutions to educate the public on statistical matters to increase the national awareness of statistics and the use of evidence.

In terms of so-called official and non-official statistics, it is evident that these definitions relate largely to where the data is produced. Notwithstanding, this guide does not aim to minimise the role of NSOs; they are, and remain, key stakeholders within the NSS and other data ecosystems for sustainable development (in Africa and beyond) and they play the role of facilitator and leader in fostering collaboration, harmonisation, and coordination within national communities.[40] Thus, the role of the NSO should be to coordinate the entire National Statistical System, which includes both official and non-official data sources. The NSO should not play a role in 'curtailing' or approving data from non-state sources, as these are often critical voices which rightfully challenge the status quo with evidence.

Moreover, it is by drawing attention to these components and the various stakeholders that we hope to further recognise M&E practitioners and their role as embedded within broader data ecosystems (and the NSS of respective countries). Non-state actors play a key role in generating non-official statistics. The methods and techniques they use are vital for demonstrating the feasibility and viability of new programmes, especially those emphasising forgotten and marginalised voices so that they are included in data and evidence. They do this by forging greater collaboration in all aspects – data collection to data processing, analysis, dissemination, and storage – and can also help to complement existing gaps in the NSS and enhance data accessibility, dissemination, and use.[41] Advances in ICT have opened (or are in the process of opening) the data ecosystem in many African countries to include non-state producers.[42]

In addition to the classification of official or non-official statistics, there are also two additional but distinct classifications of data (based on how data is collected) that inform sustainable development:[43]

1) **Administrative data** refers to daily operational data collected by ministries, departments, and agencies on a particular situation such as, roads, disease burden and enrolment. As this data source represents all reported cases of a phenomenon, this data often does not require rigorous validity and reliability tests apart from spot

checks for quality control. NSOs argue that technically, administrative data that is drawn from a Management Information System (MIS) might not necessarily pass the tests of random sampling. For example, it would exclude children who do not report for school but who are of school-going age and patients who do not seek treatment from health facilities. These are important 'pockets' of population and insights would be missed if there was sole reliance on administrative data to drive policy.

2) **Survey data** is collected when a particular phenomenon is under investigation and requires responses from individuals, groups, or households. This approach requires more rigour in terms of validity/reliability tests. Sampling becomes a critical consideration when it comes to survey data so that the findings can be generalised to the broader population.

The classifications provided above are important because such data is used to influence policy and decision making. On the one hand, government's use of this data influences budget processes and ensures that resources are allocated according to needs and also provides information on which areas and sectors need urgent attention.[44] On the other hand, non-state actors mostly use official statistics (such as census data) to establish baselines that help them to design programmes (even though the information may be outdated). They also use such data to formulate policies, and to advise on legal and legislative issues that lead to increased transparency and accountability of governments.

As the purpose for which data will be used impacts how and why it is collected, M&E practitioners, both within and outside government, find themselves at a nexus where tensions may exist based on interactions between components of the ecosystem and vastly different operational paradigms.

Tensions in the African data ecosystem

The impact of open data and big data in Africa remains debatable in terms of the extent to which data is recognised as a strategic and social asset that benefits all stakeholders.[45] For example, there are noteworthy instances of peaceful and democratic elections in sensitive and fragile political environments.[46;47] Some attribute this to the openness and transparency of election data as attested to by independent observer systems, real-time and trustworthy communications, and a vibrant media community.

On the other hand, the potential for abuse of data privacy and security is very real; drawing from the same example of electoral processes, instances have been reported of disinformation being spread because personal data was leveraged.[48] And even though anonymisation[49] has been one of the key techniques employed to sanitise datasets for open access, advances in computing and technology now enable the deanonymisation of individuals' data to reveal their identities – in other words, data anonymisation is no longer enough.[50] Further, the needs of both state and non-state actors may not align when it comes to reporting in terms of 1) The Sustainable Development Goals (SDGs); 2) The Open Government Partnership (OGP) platforms (which encourage governments to transparently open their data and involve citizens in decision making); and 3) The continental African Peer Review Mechanism (APRM) which is a self-monitoring mechanism aimed at promoting good governance.

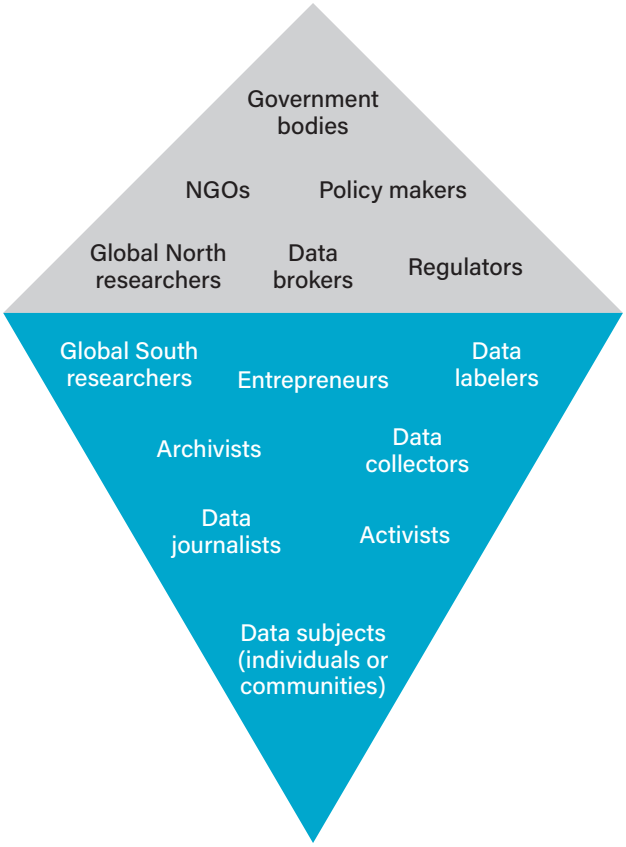
PARIS21[51] and the Mo Ibrahim Foundation[52] note that whereas statistical capacity across the continent has improved significantly over the past few decades, it has yet to catch up with other regions. Several challenges contribute to the lag in capacity of African national statistical offices (NSOs), including a lack of adequate financial and human resources and inadequate capacity to provide accessible and available data.[53] Data literacy and the digital divide are also pertinent issues. They contribute to poor data policy on the continent and limited use of different (and new) data sources in policy design and monitoring.

The expansion of the digital data ecosystem has led to vast amounts of data emanating from non-state providers compelling African NSOs to assume a new type of data stewardship role. This has put increased pressure on the capacity of NSOs as key stakeholders within the broader NSS, forcing them to take the lead in navigating the challenges previously mentioned.[54] This necessitates proper redress for the emergent data governance and data use issues and all those working with data need to be sensitive to these variances.

African countries and regions differ fundamentally in terms of the political economies and institutional, technological, financial, and human resource capabilities[55] that inform their data ecosystem adaptability and limitations. Further, whereas data sharing can support research and policy design to alleviate poverty and inequality, there is growing disquiet that even though the datasets in question are often extracted from heterogenous African communities, these communities do not reap the same benefits as those who collect the data or those who own the data infrastructures.[56] Unequal power relations inherent in the data ecosystem undermine citizens' (especially the marginalised) rights to control their data – this includes disrespect for traditional values of local communities in the collection and use of data.[57] Additionally, debates around the challenges of data collection, use and sharing in Africa are too often driven

by non-African stakeholders.[58] This leads to a third and more holistic depiction of the African data ecosystem; those at the top of the iceberg wield more power and influence than those who remain 'hidden' – with individuals/citizens (especially indigenous and marginalised communities) at the very bottom.[59]

Figure 3: Showcasing power relations within the African data ecosystem (Source: Abebe et al., 2021[60]).



This guide suggests, therefore, that a standardised approach to data governance will not serve all African countries equally (even those with similar colonial histories). The question then is how can Africa maximise the positive and mitigate the potentially negative impacts of the data revolution?[61] This, and the impact on M&E practitioners, will be discussed in depth in the following sections.

3. Data rights as human rights

As the data revolution intensifies across the continent, attention to data rights has become a central discussion. Data rights are about more than just privacy and data ownership. They ensure that individuals have certain freedoms to shield themselves from undesirable invasions of privacy or overbearing control and surveillance from state and non-state actors. They also offer a framework to provide citizens with the rights to determine what data is collected from or about them and how their data will be used.[62]

Privacy is an intrinsic human right guaranteed in the United Nations International Bill of Human Rights, which includes the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR). These rights existed long before the advent of big tech firms in the 2000s, but with the proliferation in the amount of data being collected – especially digital data – the rights of individuals have assumed a greater prominence globally.

The UN Human Rights Committee added the following to Article 17 of the ICCPR,[63] on the Right to Privacy in 1988:

> *The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. -ICCPR, Article 17 G.C. No. 16-10*
>
> *Relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. -ICCPR, Article 17 G.C. No. 16-8*

Every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes ... If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination. - ICCPR, Article 17 G.C. No. 16-10

Some 30 years later, we see a range of responses to these issues. One of the blueprints for ensuring data rights is The European Union's (GDPR)[64] which was developed in 2016. The GDPR has become a global model for countries developing national data protection laws. The GDPR applies to any entity operating within the EU, as well as any country outside the EU which offer goods or services to customers or businesses in the EU. It gives EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so that both citizens and businesses in the European Union can benefit fully. This model has been exported to countries around the world who wish to establish stronger data rights for their citizens and to curtail the indiscriminate collection and use of data by the private sector and other institutions who hold or process data.

4. Data governance in the African context

The GDPR and other data protection laws are one aspect of 'data governance.' Data governance aims to increase the value of data and minimise data-related costs and risk. It offers a cross functional framework for managing data. In doing so, it lays out decision rights and accountabilities for decision making about data. Data governance formalises data policies, standards and procedures and puts in place mechanisms for accountability. In the corporate sector and in government institutions, data governance is increasingly recognised as an important process for helping businesses and institutions make informed decisions.[65]

Data governance refers to a set of rules and norms related to why and how data is captured and used and who holds responsibility for the process. Beyond data management, data privacy, and data protection, data governance includes the end-to-end policies, strategies, standards, rights and accountabilities for the data.

As the data revolution takes hold in Africa and technology trends such as machine learning, artificial intelligence and big data emerge, discussion on the role of data governance and data responsibility has increased[66] including debates on the models of data governance that are the best fit for the continent. References to 'data as the new oil' have led many to question how data is governed on the continent, who extracts and processes the data of Africans, and who derives value from that data.[67]

Dominant data governance models have been established by the so-called 'Big Tech' monopolies based largely in the United States, China and the EU, to meet their business and financial interests. These models have been subject to increasing criticism for advancing values and practices for their own benefits that result in harm for those who rely on these technologies and to society as a whole. The Africa-focused initiatives promoted by some of these companies – such as providing financial services for the unbanked or connecting the unconnected – have been criticised for being familiar colonial narratives and resource extraction efforts (in this case, data) disguised as 'technology for good.'[68] Current private sector models have failed to engage the public in an informed discussion and debate on data collection and processing and effectively cement power within the technology companies. Private sector data governance models generally focus on transparency and accountability for data privacy or products derived from the *collection* of data through platforms and applications like chatbots, games, social media, and services like healthcare. There is a growing awareness that data governance must also mandate transparency and accountability for the *uses* of data and for the supplemental *processes and decisions* made with data, as these have a direct influence on society. For example, the High Court of Kenya halted the collection of biometric data for its national identification system, Huduma Namba, after resistance from human rights organisations and citizens who mistrusted the way that government planned to collect and use the data and additional concerns about the exclusion of groups who might have certain challenges or those who refused to provide biometric data as was required to obtain a national ID. It was ruled that the government must implement the necessary legislative framework before launching the Huduma Namba identity system.[69]

To address the deficits in corporate data governance frameworks, actors beyond Big Tech have become involved in developing alternative data governance models.

The global emergence of data privacy legislation

New data laws have emerged at national level over the past five years. These laws aim to address the digital economy and the data revolution, and to create oversight and accountability mechanisms for the corporate sector,

governments, social welfare organisations and other bodies that collect and process data. By 2021, at least 128 out of 194 countries globally had implemented legislation to secure the protection and privacy of personal and sensitive data and for the subsequent processes and decisions relating to the data.[70]

The EU's GDPR came into effect in May 2018. It is a comprehensive framework that regulates the protection of data, regardless of the sector. It builds on and modernises earlier data protection and privacy efforts, including the Council of Europe's Convention 108 which emerged in the 1980s.[71] The GDPR is currently the most well-known and influential data protection framework. Notions of individual autonomy and individual rights – dominant frameworks in the West – underpin the GDPR, which regards personal data as an extension of the individual. The GDPR therefore safeguards against the processing of personal and sensitive data by third parties without the consent of data subjects or the application of other lawful bases for data collection and processing.

The GDPR takes a technology-neutral approach to remain relevant in the face of rapid technology changes. Rather than focus on specific technology used for data processing, the GDPR focuses on regulating the effects of data processing and its potential and/or actual effects on fundamental human rights. The GDPR's technology neutrality is a major strength as emphasises the principles of law and their application to any technology, including emerging or unanticipated technology.

Data legislation in Africa

Since the emergence of the GDPR, countries around the world have developed their own national data bills, acts, laws, and regulations. These are commonly based on the GDPR's basic principles and framing, including definitions of personal and sensitive data and concepts such as informed consent and data minimisation. Many laws have also mirrored the GDPR's designation of roles and responsibilities for data. These include assigning legal responsibilities to data controllers and data processors; the appointment of national data protection authorities; and the internal assignment of data privacy/protection officer roles in certain sizes or types of organisations. The GDPR also mandates how data breaches should be handled and who should be informed about them. National Data Protection authorities are authorised to conduct investigations into violations of data protection and to impose fines as punishment for breaching the rules. The GDPR also outlines a series of 'data subject rights', including the right to object to data processing; and the right to know, correct, or request deletion of the information that an entity holds about an individual.

Twenty-eight African countries have passed data protection laws and the most recent to do so are Uganda, Kenya and Egypt.[72] Other countries, including Nigeria, have introduced data protection bills which are at various levels in the respective country legislative agendas. Newer laws are generally modelled after the GDPR, using similar language and principles. See Figure 4 below for an in-depth overview of Kenya's data protection legislation.

Figure 4: Kenya's access to information and data protection laws

Overview of Kenyan Data Laws

The Constitution of Kenya, 2010 (The Constitution) guarantees the right to privacy as a fundamental right in its Bill of Rights (Article 31). Even though there are other pieces of legislation and regulations that also regulate personal data processing, the Data Protection Act 2019 (DPA) is the primary legislation.[73] Part 2 of the Act establishes the Office of the Data Protection Commissioner (ODPC) whose mandate includes overseeing the implementation and enforcement of the provisions of the DPA. As the ODPC marked 100 days of operations on 24 February 2021, the DPC remarked that the agency has drafted a Data Protection Impact Assessment, and drafted guidelines on consent, guidelines for processing of personal data during COVID-19[74] and has also drafted the manual on complaints management and service charters on the basic rights of the individuals on matters of data privacy and protection.

The Access to Information Act 2016[75]

The Access to Information Act (ATI Act), 2016 defines 'information' as all records held by a public entity or a private body, regardless of the form in which the information is stored, its source or the date of production. This includes information held in any format, such as:

1. *Written documents, reports, memos, letters, notes, emails, and draft documents;*
2. *Non-written documentary information, such as material stored on or generated by computers and databases, video and tape recordings, maps, and photographs; and*
3. *Information which is known to an agency, but which has not yet been recorded in writing or otherwise.*

Section 8 of the Access to Information Act, 2016 requires that a request be specified with 'due particularity.' It requires that anyone making a request for information shall provide details and sufficient particulars to the public officer or any other official to understand what information is being requested. Ideally, the request should:

1 *Identify what information is being sought;*
2. *Indicate how the requester wants the information provided;*
3. *Provide any reasons for urgency (should it be requested); and*
4. *Provide a name, address, and contact phone number.*

Data Protection Act of 2019

The purpose of the Data Protection Act, 2019 (the Act/DPA) is to, inter alia, regulate the collection and processing of data in Kenya. The Act establishes the office of the Data Protection Commissioner which is to be headed by a Data Commissioner. The role of the office of the Data Protection Commissioner includes overseeing the implementation of the Act, establishing and maintaining a register of data controllers and data processors, exercising oversight on data processing operations, receiving and investigating any complaint by any person on infringement of the rights under the Act.

The Act has extraterritorial application as it applies to data controllers and processors established or resident in or outside Kenya in so far as they process personal data while in Kenya or of data subjects located in Kenya. The Act also outlines the conditions for the transfer of personal data outside of Kenya and the safeguards that must be considered. For instance, where the transfer is necessary for the performance of a contract between a person whose data is collected and the data controller or data processor or implementation of pre-contractual measures taken at the person's request.

The Act outlines the principles of data protection which are modelled on the principles set out in the EU General Data Protection Regulation. It further stipulates the rights of persons whose data is collected, including the right to: be informed of the use to which their personal data is to be put; access their personal data in custody of a data controller or data processor; to correction of false or misleading data; and to deletion of false or misleading data about them.

Processing of data is prohibited unless certain conditions set out under the Act, including the obtainment of the consent of the person whose data is processed are fulfilled. In addition, the processing of sensitive personal data is prohibited except for the stipulated permitted grounds. Further, personal data relating to the health of a person may only be processed by or under the responsibility of a health care provider; or by a person subject to the obligation of professional secrecy under any law.

Access to information versus data rights

The data-for-development constituency argues that data is a resource. Without a greater and improved understanding of the economic and political benefits of data use, it will be impossible to advocate for citizens' interests resulting in missed development opportunities[76]*. The other issue already raised is the one of 'data colonialism.' Hence the push for Access to Information and other principles of Open Government*[77] *which require that government agencies make official information more freely available.*

Herein lies the problem; consent is often not required – especially when information is used for research and statistical purposes.

Key data privacy issues remedied by the DPA

1. *Though the DPA is yet to be operationalised, consent for data use has shifted from 'implied' to 'expressed' form.*
2. *The DPA also raises the security demands (through safeguards, technical measures and mechanisms in place) on how, when and by whom data is processed – that is from collection through to analysis and storage. For example, all sensitive personal data should be password protected for restricted access.*

3. *All data controllers and data processors carrying out any processing activities involving the personal data of Kenyan data subjects must ensure that they comply with the provisions of the DPA. They must be registered with the Office of the Data Protection Commissioner and those who infringe on any part of the DPA will be prosecuted.*
4. *The DPA gives certain rights to the Data Commissioner to suspend or prohibit any cross-border transfers. Further, the Cabinet Secretary may prescribe, on grounds of strategic interests of the State or for protection of revenue, that certain types of processing make use of a server or data centre located in Kenya.*
5. *Companies collecting health data must ensure that the data is collected in accordance with the DPA. It specifically restricts processing which must only be undertaken under the responsibility of a healthcare provider or by a person subject to the obligation of professional secrecy.*

The DPA makes room for operationalisation through additional regulations and codes of practice that may be issued in the future, and which will affect the way in which the Act is implemented.

Comparisons of the DPA with the GDPR

There are several differences between the GDPR and Kenya's DPA. In terms of fines, for example, Kenya's data protection law states that culprits who infringe on the DPA would suffer up to a maximum of KES 5 m (~USD 50k) as fine for a breach (Article 63 of the DPA), the GDPR has set KES 2 b (~USD 20m) as a fine. This seems like a relatively small amount and more needs to be done in Kenya to ensure fines are hefty for deterrence.

Similarities exist in terms of issues of independence and autonomy; this is the requirement that the agency is empowered to initiate and undertake appropriate data protection work and enforce laws without having to seek permission of another agency. Independence may also be construed through considering the composition of the authority; the power and time frame for exercising oversight functions; and the allocation of sufficient resources and the ability to make decisions without external interference. By law, the ODPC in Kenya is an independent public authority that supervises by making use of investigative and corrective powers. Similarly, the GDPR built further upon the EU directive that states that data protection authorities "shall act with complete independence in exercising the functions entrusted to them." At 100 days, the DPC Kenya announced that the ODPC received a budget allocation of KES 11 m (~USD 110k) although it had requested KES 50 m (~USD 500k) – an amount that was inadequate for the recruitment of competent staff, the payments staff salaries, or the acquisition of office space, among others. Similarly, many EU DPCs complain that they have insufficient resources to do their jobs, but this may be problematic for data processing that occurs in domiciles without necessary or adequate data protection laws (Article 48(b)). Further, the GDPR and Kenya's DPA align when it comes to the following principles on data:

1. *It is processed fairly, lawfully and transparently;*
2. *It is collected and processed for specific reasons and stored for specific periods of time, and that it is not used for reasons beyond its original purpose;*
3. *Only the data necessary for the purpose it is intended is collected, and not more;*
4. *It is accurate and that reasonable steps are taken to ensure it remains accurate;*
5. *It is kept in a form that allows individuals to be identified only for as long as is necessary; and*
6. *it is kept securely and protected from unlawful access, accidental loss or damage.*

Also see the African Declaration on Internet Rights and Freedoms Coalition's *"Privacy and personal data protection in Africa A rights-based survey of legislation in eight countries" for an in-depth analysis of personal data protection legislation in several African countries.*

The global trend is towards the development of comprehensive data protection legislation, and, in most cases, existing legislation does include aspects of data governance, privacy, and protection of vulnerable people or groups: for example, cybercrime bills, consumer protection bills, ICT laws, financial regulations, and others.[78] This is the case in African countries that have not yet enacted newer laws, and it is also the case in the United States, which has yet to implement federal data protection legislation and currently relies on a patchwork of laws at the sector level (health data, financial data, education data, children's data all have separate laws) and at the state level (California, Virginia and a handful of other states have approved data protection legislation in the past three years).

Regional data protection on the African continent follows the same trends and has been strengthened over the past decade. In 2010, for example, the Economic Community of West African States (ECOWAS) adopted a Supplementary Act on Personal Data Protection.[79] In 2013, the Southern African Development Community (SADC) published a Model Data Protection Act,[80] and in 2014 the African Union adopted the Convention on Cyber Security and Personal Data Protection (the Malabo Convention), which is a comprehensive document covering electronic transactions, privacy, and cybersecurity.[81]

As per the Malabo convention, consent from a data subject (the one whose data is being collected) is the default condition for data processing.[82] Other data subject rights include the right to correct personal data and the right to object to data processing. Further, African data protection frameworks have provided for the establishment of independent data protection authorities. These statutes also require that data controllers notify the regulator of any data processing activities and some, such as the Data Protection Act (2019) in Kenya, also confer investigative powers on the office of the Data Protection Commissioner.

Other commonalities among African data protection frameworks and statutes include:

- The acts/bills apply to the collection, storage, processing and use of personal data relating to persons living in their country and persons of their nationality, and to entities that are registered and operating in these countries. Foreign entities targeting persons living in the country must also follow these laws.
- Consent of data subjects for data collection and processing is also mandated in these frameworks. Basic principles relating to processing of personal data, such as the right for an individual to know what data has been collected about them over what period of time; how much of their data has been captured or processed; what it is being used for; the right to refuse data collection or processing; the right to withdraw consent for data processing; the right to request deletion of their personal data; and the right to prevent their data from being shared with third parties without consent. A data controller must have proof that the data subject has consented to the processing of their personal data and must not coerce consent or force data collection in exchange for access to services or information.
- Establishment of a data protection commission is required. It must be led by a data protection commissioner who oversees the implementation and enforcement of the data protection act. The data protection commissioner enforces penalties and fines for anyone found responsible for the improper use of data or data breaches.
- These frameworks also embody basic privacy principles, including collecting data only for a specific purpose; limiting the amount of data that is collected; accountability; limiting the duration for which data can be stored; transparency; confidentiality; and capturing data as accurately as possible.

Figure 5: Complementary approaches for protecting data rights and use of personal data:

There are two key complementary approaches necessary to shore up data protection and data rights:

1. **Legal safeguards and practical data protection measures:** These would apply at national and subnational levels and would include all the data collection and data processing steps (at both national and subnational levels) in adherence to national and regional laws. We must, however, acknowledge the significant role that data plays in socio-economic development. Without access to information and proactive disclosure of data by government, it is difficult to measure progress of any sustainable development agenda that a government is promoting. On the contrary, some governments have equated transparency and disclosure to mean the release of personal data – a violation of data rights. Further, just providing notice and enabling consent are deemed insufficient to protect data privacy and data rights in the digital age, especially because consumers often do not have meaningful choice or are unable to decipher technical and legal jargon. In addition, given the nature of digital data, the potential uses of collected data are difficult to identify and trace. This has been referred to as 'non-violent' coercion.[83] Transparency and practical data protection measures are, however, not in conflict. Data governance processes should enable open and easily accessible accounts of methodology; the intent of data use; who will use it; for how long; and how the data and the data analyses and the learnings will be shared and with whom.

2. **Capacity strengthening of in-country data protection officers (and their respective functions).** Capacities must be developed to ensure technical safeguarding proficiency and use of appropriate ICT and legal knowledge, data access controls, data security, and safe storage when data analytics (including artificial intelligence/machine learning) are utilised. This is also a key aspect in the process of ensuring that data protection officers remain independent (and do not rely on other agencies and ministries (such as ministries responsible for ICT or State Departments of Justice) for skilled staff. In cases of international data breaches, data protection officers should also possess an understanding of the international jurisprudence that has mandate over such violations. Capacity-strengthening measures should include the necessary resource allocation to ensure that the independence of data protection offices is maintained – with direct budget allocations from parliament (or the legislature) and not from any ministries (such as the executive). In countries where the data protection laws are being operationalised, skills mapping exercises should be done and gaps in administrative safeguards identified. Thereafter the skills necessary should be provided for data protection experts/officers to effectively fulfil their mandates.

African-centred data governance frameworks: an alternative to the GDPR

While most African data privacy legislation is modelled on the GDPR, an emerging framework for data governance seeks to offer a different model for data protection in contexts that do not match that of the EU.[84] Instead of focusing on personal data, this framework places the collective interests of communities and their aggregate data at the centre.[85] Data is considered an extension of a community itself.[86] In the African context, for example, in addition to principles like transparency, accountability, responsiveness, and sustainability, existing home-grown principles are proposed that articulate and speak to a spirit of collectiveness and that serve as an organising unit in most communities.

Figure 6: African principles that could help to frame context-relevant approaches to data governance.[87]

Principle	Outline/description
UBUNTU (Humanity)	To endeavour to make practical mutual humanity as a basis of human society.
UMOJA (Unity)	To strive for and to maintain unity in the family, community, nation and race.
KUJICHAGULIA (Self-determination)	To define ourselves, name ourselves, create for ourselves, and speak for ourselves.
UJIMA (Collective work and responsibility)	To build and maintain our community together and make our brothers' and sisters' problems our problems and to solve them together.
UJAMAA (Cooperative economics)	To promote enterprise development within African communities and lobby for policies that eliminate obstacles faced by people of African ancestry in business, wealth creation and equitable distribution.
NIA (Purpose)	To make our collective vocation the building and developing of our community in order to restore our people to their traditional greatness.
KUUMBA (Creativity)	To do always as much as we can, in the way we can, in order to leave our community more beautiful and beneficial than we inherited it.
IMANI (Faith)	To believe with all our heart in our people, our parents, our teachers, our leaders and the righteousness and victory of our struggle.

Other alternatives to the GDPR are also being explored. For example, in 2019[88] the African Union assembled a team of experts to develop principles for the governance of AI on the continent. This was in response to the realisation that while emerging digital technologies such as AI, blockchain, the Internet of Things and other innovations can create immensely useful products and services, they also have the potential to be extremely disruptive to jobs, health and security. Countries like South Africa and Nigeria have done the same at the national level. Thus, the AU's programme can also be construed to be part of the global geopolitical competition around Artificial Intelligence and development of strategies for data that stress the value of extracting greater benefits from and greater control over local data. Still, the CARE Principles for Indigenous Data Governance set up by the Global Indigenous Data Alliance (inspired by the UN Declaration on the Rights of Indigenous Peoples) reaffirms local communities' rights to self-governance and authority to control their cultural heritage embedded in their data and is more aligned to emerging models.[89]

In this regard, attention turns to the practices for data access and control developed by data stakeholders. Third parties seeking to appropriate community data are required to ensure safeguards through mechanisms such as data trusts, data pools or other data sharing arrangements that are fit for the developing south and that help to guarantee greater local control and decision over data.[90]

Figure 7: The core principles of CARE[91]

Principle	Description
Collective benefit	Data governance systems should be designed and function in ways that enable local communities, in whose values the data is grounded, to derive benefit from the data. Any value created from this data should benefit the concerned communities in an equitable manner and contribute to local peoples' aspirations for wellbeing.
Authority to control	Local communities' rights and interests in data must be recognised and their authority to control their own data empowered. Data governance must enable local people to determine how their communities, territories, resources, knowledge and geographical indicators are represented and identified within data.
Responsibility	Organisations working with local data have a duty to share how the data are used to support local communities' self-determination and collective benefit.
Ethics	Local peoples' rights and wellbeing should be the primary concern at all stages of the data life cycle and across the data ecosystem.

These emerging models emphasise power relations between actors. They are built around questions of:

1) What configurations of roles and relationships between stakeholders can be identified in data governance?
2) What is the extent to which other actors beyond corporate data platforms are able to participate?
3) What is the value that is proven and how is it redistributed across actors and society?
4) What mechanisms and arrangements are in place to generate value from the data? Each data model is a situated, contingent and relational instantiation of the stakeholder roles, their interrelationships, their articulations of value, and the organisations of governance principles, instruments and mechanisms.[92]

Figure 8: Emerging models and the power relations with regard to data governance

Model	Description
Data Sharing Pools (DSPs)	A key mechanism of this instrument is the contract, legal and policy framework that defines the modalities for data sharing, how data can be handled and for which purposes. The contracts can be repeatable frameworks of terms and conditions to facilitate the sharing of data between entities which are useful for organisations that do not have the know-how and legal support to leverage data. DSPs are used in horizontal joint initiatives among data holders to aggregate data from diverse sources to create more value through their combination.
Data Cooperatives (DCs)	DCs are an explicit mechanism to rebalance the relationship between data subjects, data platforms and third-party data users. DCs facilitate and enable decentralised data governance, creating a common pool for mutual benefits. Access or rights to the data are distributed among actors providing higher involvement of data subjects. Examples are bottom-up data trusts, agreements and contracts that provide the means for citizens to be informed, to express their preferences, and to decide how to share their data and for what purpose.
Public Data Trusts (PDTs)	PDTs are established by public actors to access, aggregate, and use data about its citizens, including data held by private entities with which it establishes a relationship of trust. The public actors assume the role of trustees to guarantee that citizens' data is handled ethically, privately and securely. PDTs are involved in the establishment of a relationship of trust between citizens and public bodies. An underlying assumption of a PDT is that all data with a public interest component – even if controlled by private entities – is part of a nation's infrastructure, and therefore the information it attracts must be socialised to produce value for citizens and society at large. A key enabler would be a legal framework mandating private entities to grant access to data of public interests to public actors under conditions specified by law. Examples are pilot projects by the Open Data Institute using real-time data to improve public service delivery.
Personal Data Sovereignty Model (PDS)	The PDS model is characterised by data subjects having greater control over their data, both in terms of privacy management and data portability, compared to the current dominant model. This model has two goals: granting more opportunities to access, share and use personal data; and engendering a more balanced relationship between data users and other stakeholders. It is expected to foster the socially beneficial usage of data through the development of new data driven services centred on user needs.

Pioneering work in this area by the Data Governance Network[93] suggests that low- and middle-income countries need to enact Data Sharing and Public Ownership Acts[94] (Data Protection Legislation in Africa was mentioned above – including the SADC model data protection law published in 2013).

5. Data governance and M&E

As noted above, lower- and middle-income countries are at the forefront of adopting new data privacy laws. However, there is a big gap between laws on paper and laws in practice, and strong data governance systems are urgently needed to address this gap. To better support governments in managing data responsibly, the global development sector has recently shifted its focus from that of merely promoting digital tools and the use of data to a more holistic approach in which data is managed responsibly across the full data lifecycle – from data design to data use, storage, retention or destruction.[95]

M&E teams are key in promoting and executing data governance systems, as they play the role of 'data stewards' by ensuring that data policies and data standards are adhered to in daily practice. To help the development sector move forward and better support governments in their data governance efforts, M&E practitioners need to be equipped with up-to-date knowledge on data governance and data protection.

Because M&E practitioners and the departments that they work with deal with several types of data, they should be fully aware of their responsibilities and accountabilities to the various stakeholders. During the M&E process, for example, accountabilities are mandated to the following:

- **Individuals:** Their data is collected and used to measure programme impact or to predict outcomes.
- **Communities:** They have a stake in the data collected about them and the decisions made using that data.
- **Peer organisations:** They hold the collectors of data accountable for peer-ethical and transparent governance processes.
- **National governments:** They need to keep the data of those living within their borders safe and secure.
- **Other country governments:** They may receive or have access to data sets and need to ensure that this data is protected.
- **Donors:** They play a strong role in determining what data is collected and processed and use data to determine whether programme goals have been met.
- **Evaluation commissioners:** Since the work of M&E practitioners is framed within a particular context or country, they must operate within national laws, including data protection and privacy laws and research ethics laws. Regulatory authorities like professional associations or public sector data authorities and research bodies (e.g. national ethics committees) can provide further support by setting standards or principles. The data governance system should always be guided by those laws and standards.

M&E practitioners in the development sector are often torn between prioritising 'upward' accountability towards donors over 'downward' accountability to individuals and communities who are participating in programmes and services. The Centre for Global Development, for instance, found that while the value of data should lie in providing actionable insights that can improve services and policy, the benefits of this data are seldom felt by the individuals, communities and organisations that initially provided it.[96] This often results in data collection and decisions made from data that are of little practical value for the community. In addition, donors may choose to work outside national data systems, resulting in paternalistic relationships and poor country ownership.

Data governance challenges for M&E

While new legislation is strengthening certain data rights and data privacy protections, challenges remain in several areas. In general, legislation has been unable to keep pace with changes in technology and, as the sophistication of data use grows, new issues will continue to emerge. For example, only now is legislation is being formulated to regulate the use of facial recognition and to address government use of private sector location and mobility data without a specific warrant to do so. A 2021 report highlighted the urgent need to legally restrict the sale of tools sold by the private sector to governments to spy on human rights activists and others who voice dissent.[97] Additionally, enforcement of data laws has been uneven and has been heavily dependent on the strength of the rule of law and on the capacity and funding of data protection authorities.

M&E units and individual professionals play a role in ensuring that data collected is put to good use and does not compromise the safety and security of those whose data is collected. In Section 2 of this document, guidelines will be provided for responsible data management for M&E units and practitioners. While Section 1 provided an overview of these topics, Section 2 will provide information on how to put good data governance and responsible management of personal and sensitive data into practice.

ENDNOTES

1 United Nations (2015). "A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development" https://www.un.org/sg/sites/www.un.org.sg/files/files/HLP_P2015_Report.pdf.

2 Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*." Oxford.

3 UNICEF (2021). "The Case for Better Governance of Children's Data: A Manifesto" UNICEF Office of Global Policy and Insights. https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto

4 For example, in Kenya there is the National Commission for Science and Technology (NACOSTI - https://www.nacosti.go.ke/mandate-functions/), Tanzania has the Tanzania Commission for Science and Technology. (COSTECH – https://costech.or.tz/)South Africa has the National Research Foundation (NRF - https://www.nrf.ac.za/about-nrf/mandate). These institutions have a broad mandate to advice, coordinate, promote and sometimes even regulate scientific research systems.

5 Office of the Secretary (1979). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

6 Cape Verde (2001), Seychelles (2003), Burkina Faso (2004), Mauritius (2004), Tunisia (2004), Senegal (2008), Morocco (2009), Benin (2009), Gambia (2009), Zambia (2009).

7 Gabon (2011), Angola (2011), Ghana (2012), Lesotho (2012), South Africa (2013), Mali (2013), Cote d'ivoire (2013), Madagascar (2014), Chad (2015), Equatorial Guinea (2016), Malawi (2016), Sao Tome and Principle (2016), Kenya (2019), Uganda (2019), and Egypt (2019).

8 Daigle, B. (2021). *Data Protection Laws in Africa: A Pan-African Survey and Noted Trends.* United States International Trade Commission (USITC). https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

9 Pisa, M., Dixon, P. Ndulu, B. and Nwankwo, U. (2020). *Governing Data for Development: Trends, Challenges, and Opportunities*. Center for Global Development Policy Paper 190. https://www.cgdev.org/sites/default/files/governing-data-development-trends-challenges-and-opportunities.pdf#page=9&zoom=130,18,588

10 Pisa, M., Dixon, P. Ndulu, B. and Nwankwo, U. (2020).

11 Iyer, N., Chair, C. and Achieng, G. (2021). AfroFeminist Data Futures. Pollicy. https://pollicy.org/wp-content/uploads/2021/03/Afrofeminist-Data-Futures-Report-ENGLISH.pdf

12 African Union (2014) "African Union Convention on Cyber Security and Personal Data Protection" https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

13 Economic Community of West African States (2010). "Supplementary Act on Personal Data Protection within ECOWAS" http://www.ictpolicyafrica.org/en/document/z69cbq7b51?page=1

14 Internet Society (2020). "Personal Data Protection Guidelines for Africa" https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

15 African Commission on Human and Peoples' Rights (2019). "Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019". https://www.achpr.org/legalinstruments/detail?id=69#:~:text=The%20Declaration%20of%20Principles%20of,2019%20in%20Banjul%2C%20The%20Gambia.

16 While the term "M&E Practitioners" encompasses varying levels of decision making and influence, there are responsibilities at every level for protecting data and managing it ethically.

17 MERL Tech and CLEAR Anglophone Africa (2020). "Event Report Back: How to Conduct Digital MERL in the Time of COVID-19" https://merltech.org/wp-content/uploads/2020/06/Detailed-report-covering-the-3-gLOCAL-2020-Events.pdf

18 United Nations (2015).

19 United Nations (2015).

20 The Partnership in Statistics for Development in the 21st Century (PARIS21) and the Mo Ibrahim Foundation (2021). Working Paper: "Bridging the Data-Policy Gap in Africa. Recommendations to national statistical offices and governments to enhance the production and use of data for evidence-based policymaking" https://mcusercontent.com/e3ad8097ecf1a36cabd12a3fb/files/5661f488-fd7b-4bbd-879d-4f06b4adb9c6/Data_Policy_Gap_Africa_FINAL.pdf.

21 United National Development Programme (2016) The Africa Data Revolution Report https://www.africa.undp.org/content/rba/en/home/library/reports/the_africa_data_revolution_report_2016.html.

22 Msokwa, Z.E. (2016).

23 Lämmerhirt, D. Gray, J., Venturini, T. and Meunier, A. (2019). *Advancing sustainability together? Citizen-generated data and the Sustainable Development Goals*. Global Partnership for Sustainable Development Data. https://www.data4sdgs.org/sites/default/files/2018-12/Advancing%20Sustainability%20Together%20Summary%20Report_0.pdf

24 Cázarez-Grageda, K., Schmidt, J. and Ranjan, R. (2020). *Reusing Citizen Generated Data for official reporting: A quality framework for national statistical office-civil society organisation engagement*. PARIS21 Working Paper. https://paris21.org/sites/default/files/2021-02/CGD_FINAL_reduced.pdf

25 Msokwa, Z.E. (2016).

26 UNDP (2017). Data ecosystems for sustainable development: An assessment of 6 pilot countries. https://www.undp.org/publications/data-ecosystems-sustainable-development.

27 UNDP (2017).

28 African Union (2009). African Charter on Statistics. https://au.int/en/treaties/african-charter-statistics.

29 African Union (2009). Strategy for the Harmonization of Statistics in Africa. https://au.int/en/ea/statistics/shasa.

30 UNDP (2017). *Data ecosystems for sustainable development: An assessment of 6 pilot countries*. https://www.undp.org/publications/data-ecosystems-sustainable-development

31 UNDP (2017).

32 This definition draws from both the Open Data Charter (opendatacharter.net) and the Africa Data Consensus.

33 Buttles-Valdez, P., Svolou, A. and Valdez, F. (2008). A holistic approach to process improvement using the people CMM and the CMM-DEV: Technology, process, people, & culture, the holistic quadripartite. In SEPG 2008 Conference, Software Engineering Institute.

34 Smits, D. and van Hillegersberg, J. (2015). *IT Governance Maturity: Developing a Maturity Model using the Delphi Method*. 2015 48th Hawaii International Conference on System Sciences. https://ris.utwente.nl/ws/portalfiles/portal/5519896/07070361.pdf

35 UNDP (2017).

36 Msokwa, Z.E. (2016).

37 Msokwa, Z.E. (2016).

38 In a qualitative approach, the researcher is not detached from the subject. Rather they delve to understand 'why' phenomena (and behaviour) observed are the way they are. Data is collected through unstructured interviews, observation, and content analysis. Topics may include experiences of women, children, youth and populations who are often marginalised in society.

39 A quantitative approach will likely involve a high degree of objectivity, structured questions, and structured analysis. It is best for explanatory research that explains phenomena and focuses on priorities.

40 UNDP (2017).

41 UNDP (2017).

42 In Kenya CSOs collaborated with the Kenya National Bureau of Statistics to develop to develop guidelines for the production of quality Citizen Generated Data (https://www.data4sdgs.org/resources/citizen-generated-data-kenya-practical-guide)

43 UNDP (2017).

44 For example, in Kenya, data produced by county governments mainly informs planning, policy formulation and budgeting; it also serves for engagement with the public and educating communities.

45 Van Belle, J. (2018). *Africa data revolution report 2018: The status and emerging impact of open data in Africa*. https://webfoundation.org/docs/2019/03/Africa-data-revolution-report.pdf

46 Scott, A. (2016). *Burkina Faso's open elections*. The Open Data Institute. https://theodi.org/project/case-study-burkina-fasos-open-elections/

47 In the case of Burkina Faso, the case study is clear that the claim by open data is not an empirical one and that it can lead to an increased trust in the election process; rather that open data helps to improve information flows and transparency to all stakeholders, especially citizens, during a critical period of political transition and which improves overall credibility of the process.

48 Bax, P. and Prinsloo, L. (2020). *Online Disinformation Campaigns Undermine African Elections*. https://www.bloomberg.com/news/articles/2020-10-13/disinformation-campaigns-on-facebook-twitter-google-undermine-african-election

49 Data anonymisation is the process of removing personally identifiable information from data sets in order to maintain the privacy of the people described.

50 Rocher, L., Hendricks, J.M., and de Montjoye, Y. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications (10); https://www.nature.com/articles/s41467-019-10933-3

51 Chen, S., Fonteneau, F., Jütting, J., and Klasen, S. (2013). *Towards a Post-2015 Framework that Counts: Developing National Statistical Capacity*. PARIS21 Discussion Paper No. 1. https://www.paris21.org/sites/default/files/PARIS21-DiscussionPaper1-MDG.pdf

52 Mo Ibrahim Foundation. (2019). Agenda 2063 and 2030: *is Africa on track? African Governance Report*. https://mo.ibrahim.foundation/sites/default/files/2019-10/African_Governance_Report_2019.pdf

53 PARIS 21 and Mo Ibrahim Foundation. (2021). *Bridging the data policy gap in Africa*: *Working Paper*. https://paris21.org/sites/default/files/inline-files/Data-Policy%20Gap_Africa__FINAL_20210430.pdf

54 PARIS 21 and Mo Ibrahim Foundation. (2021).

55 UNDP (2017) .

56 Abebe, R., Alureba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S.L., and Sadagopan, S. (2021). Narratives and Counternarratives on Data Sharing in Africa. In Conference on Fairness, Accountability, and Transparency (FAccT '21), March 3–10, 2021, Virtual Event, Canada. ACM, New York, NY, USA, 12 pages. https://dl.acm.org/doi/10.1145/3442188.3445897

57 Pawelke, A., Bellavista, G. and Liu, S. (2021). *Rethinking Data Governance: Reimagining data governance for inclusive and sustainable development and exploring emerging data governance models.* https://medium.com/@undp.innovation/rethinking-data-governance-at-undp-274be074f690

58 Abebe, R., Alureba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S.L., and Sadagopan, S. (2021).

59 Abebe, R., Alureba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S.L., and Sadagopan, S. (2021).

60 Abebe, R., Alureba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S.L., and Sadagopan, S. (2021).

61 UNDP (2017)

62 Tisne, M. (2018). *It's time for a bill of data rights*. MIT Technology Review. https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/

63 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. https://www.refworld.org/docid/453883f922.html

64 European Union (n.d.) "What is GDPR, the EU's new data protection law?" https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU

65 Abraham, R., vom Brocke, J., and Schneider, J. (2019). Data Governance: A conceptual framework, structured review, and research agenda. Journal of Information Management. 49. https://www.researchgate.net/publication/334653735_Data_Governance_A_conceptual_framework_structured_review_and_research_agenda

66 Bennet, C., and Raab, C.D. (2018). "Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective." Regulation & Governance, Vol 14:3. P 447-464. Wiley. https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12222

67 Birhane, A. (2020) "Algorithmic Colonization of Africa." Scripted. Vol 17(2) https://script-ed.org/article/algorithmic-colonization-of-africa/

68 Peña, P. "Free Basics and the Internet's Political Battles" Derechos Digitales, January 14, 2016. https://www.derechosdigitales.org/9678/free-basics-and-the-internets-political-battles/

69 Privacy International, "Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons." February 24, 2021. https://www.privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

70 UNCTAD (2020). "Data Protection and Privacy Legislation Worldwide" https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

71 Council of Europe (n/d). "Convention 108 and protocols." https://www.coe.int/en/web/data-protection/convention108-and-protocol

72 UNCTAD (2020)

73 As examples, the Kenya Information and Communication Act, 1998 (KICA) which came into effect in February 1999 is the overarching law for the information and communications technology industry in Kenya. The management personal data in the field of health is regulated under the Public Health Act 2012, the Health Act 2017 and HIV and AIDS Prevention and Control Act 2006, as well as the Health Information System Policy which guides the collection and processing medical data of patients. The processing of financial data is regulated under the National Payment System Act 2011 and the National Payment System Regulations 2014, among others.

74 Republic of Kenya, Office of the Data Protection Commissioner (2020) "Guidance Note on Access to Personal Data during COVID-19 Pandemic" https://ict.go.ke/wp-content/uploads/2021/01/Draft-Data-Request-Review-Framework-Jan-2021.pdf

75 Kenya Gazette (2019). "Data Protection Act" http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

76 Aaronson, S.A. (2018). Data Is Different: Why the World Needs a New Approach to Cross-border Data Flows. CIGI Paper No. 197. Waterloo, ON: CIGI. www.cigionline.org/publications/datadifferent-why-world-needs-new-approachgoverning-cross-border-data-flows.

77 Open government is the governing doctrine which holds that citizens have the right to access the documents and proceedings of the government to allow for effective public oversight.

78 DLA Piper (n/d). "Data Protection Laws of the World" https://www.dlapiperdataprotection.com

79 Economic Community of West African States (2010). "Supplementary Act on Personal Data Protection within ECOWAS" https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

80 International Telecommunications Unit (2012). "DRAFT Southern African Development Community (SADC) Model Law on Data Protection" http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf

81 African Union (2014)

82 Deloitte (2017). "Privacy is Paramount, Personal Data Protection in Africa Report". https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

83 Govender, D. (2019). *POPI versus technology: Did you consent to your toothbrush spying on you?* Without Prejudice https://www.withoutprejudice.co.za/free/article/6766/view

84 Abraham, R., vom Brocke, J. and Schneider, J. (2019).

85 Singh, P.J. (2019). Data and Digital Intelligence Commons. Making a Case for their community Ownership ITFC Working Paper 05

86 Milan, S., and van der Velden, L. (2016). The Alternative Epistemologies of Data Activism Digital Culture and Society. Vol. 2, Issue 2

87 Seven principles of Kwanzaa established by Dr. Maulana Karenga in 1965: https://nmaahc.si.edu/blog-post/seven-principles-kwanzaa

88 African Union (2019). "The Digital Transformation Strategy for Africa (2020-2030)" https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

89 Global Indigenous Data Alliance (2019). "CARE Principles for Indigenous Data Governance" https://www.gida-global.org/care

90 Mertens, Donna M., (1999). Inclusive Evaluation: Implications of Transformative Theory for Evaluation American Journal of Evaluation, Vol. 20, No. 1, pp. 1-14.

91 Global Indigenous Data Alliance (2019).

92 Micheli, M., Ponti, M. Craglia, M. and Suman, A.B. (2020). Emerging models of data governance in the age of datafication. https://journals.sagepub.com/doi/full/10.1177/2053951720948087

93 The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy https://datagovernance.org/

94 Parminder Jeet Singh (2019). Data and Digital Intelligence Commons. Making a Case for their community Ownership ITFC Working Paper 05

95 Pisa, M., Dixon, P., Ndulu, B. and Nwankwo, U. (2021).

96 Pisa, M., Dixon, P., Ndulu, B. and Nwankwo, U. (2021).

97 Forensic Architecture (2021). "New investigation shows global human rights harm of NSO Group's spyware" Amnesty International and Citizen Lab.

CLEAR-AA

Centre for Learning on Evaluation and Results – Anglophone Africa

The Oval Building
University of the Witwatersrand
2 St David's Place, Parktown,
Johannesburg

Telephone: +27 11 717 3157
Fax: +27 86 765 5860
Email: CLEAR.AnglophoneAfrica@wits.ac.za

www.wits.ac.za/clear-aa

MERL Tech

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

clear
Centers for Learning on Evaluation and Results
ANGLOPHONE AFRICA