Globethics Repository



African Union data policy framework

This page was generated automatically upon download from the Globethics Repository. More information on Globethics see https://www.globethics.net. Data and content policy of Globethics Repository see https://repository.globethics.net/pages/policy.

Item Type	Book chapter
Publisher	Globethics Publications
Rights	2022. African Union
Download date	2026-11-26 11:16:46
Link to Item	http://hdl.handle.net/20.500.12424/4276069

34

AFRICAN UNION DATA POLICY FRAMEWORK

African Union, Ethiopia

The African Union, representing its 55 member states from the whole African continent, endorsed its "African Union Data Policy Framework" by the AU Executive Council during its 40th Ordinary Session on 2-3 February (Ref EX.CL/Dec.1144/XL) and published in February 2022. The below excerpt are Executive Summary (pp VI-X) and the recommendations and actions of chapter V (18-64). The full text is available for free download[455].

In addition, a very helpful interactive website provides the national legislations on data protection for each African country.[456]

The Editor CS

[455] African Union Data Policy Framework. 2022. Documents, https://au.int/en/documents/20220728/au-data-policy-framework.

[456] Africa Data Protection, Liste des lois, https://africadataprotection.com/liste-des-lois.html.

34.1 Executive Summary

Data is increasingly recognised as a strategic asset, integral to policy-making, private and public sector innovation and performance management, and creating new entrepreneurial opportunities for businesses and individuals. When applied to government services, emerging technologies can generate massive amounts of digital data and significantly contribute to social progress and economic growth. The central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives - from unleashing the economic and social potential of data to the prevention of harms associated with mass collection and processing of personal data.

The purpose of this document is to provide the policy framework for African countries to maximise the benefits of a data-driven economy by creating an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation. This enabling environment refers both to the collaboration between in-country sectors, institutions and stakeholders, an alignment of their development priorities, and the harmonisation of policy across the continent in a manner that provides the scale and scope required to create globally competitive markets.

From a policy perspective, the approach adopted is people-centred, locating them in relation to the role of data in contemporary economy and society by identifying the elements and linkages in what can be called the “data ecosystem” in order to identify the exact points of policy intervention. This allows for a systemic assessment of the interrelated challenges arising from global developments that impact emerging national data economies and those arising within the context of nascent data-driven economic activity, uneven institutional endowments, and human development in many African countries. This enables the design of a contextually grounded but forward-looking data policy framework that uses economic regulation to guide policy makers in realising oppor-

tunities for data-driven value creation. The framework points to how opportunities can be realised and how associated risks could be mitigated by creating an enabling and trusted environment.

Building a positive data economy national and regional will require unprecedented levels of collaboration between stakeholders to disrupt the economic, political, and policy pressures already being felt from the global data economy. In order to ensure equitable and safe access to data for innovation and competition, Member States should establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. Existing legal instruments and institutions should be revisited where necessary to ensure that they are not in conflict with one another and that they offer complementary levels of protection and obligations.

A comprehensive data strategy will necessarily include the harmonisation between competition, trade, and taxation policies and laws both at the national and regional levels. This is so an optimised data ecosystem for Africa balances revenue mobilisation and the need to avoid distortions to local markets and the global tax system. Intellectual property laws should also be revised to clarify that they do not generally impede the flow of data or data protection. At the same time, governments need to develop transversal digital policies and strategies to coordinate activities across the public sector and between the public and private sectors to meet national objectives.

While there are multiple competing definitions of data, common to all is the recognition that there are many different types of data. There are also numerous ways that data can be categorised that affect the appropriate policy and regulation of that category in order to mitigate any potential risk associated with the processing, transfer or storage of it. A primary distinction is between personal data and non-personal data, with data protection referring to ensuring the privacy of data subjects. Data categorisation guidelines should be one of the first actions of the data information regulator, a key institution for the development of an inte-

grated national data system, which should be established in partnership with all relevant stakeholders. Essential to the development of an enabling environment for the data economy is ensuring the necessary foundational digital infrastructure and the human resources necessary to develop data as a strategic asset. Due consideration needs to be given to developing robust Digital ID systems for the delivery of public and private value to citizens and consumers.

As the framework also emphasises, this can only be properly achieved through instilling a culture of trust in the data ecosystem. This is done through the establishment of safe and secure data systems based on effective cybersecurity and data protection rules and practices, and ethical codes of conduct for those who set data policy, implement it and those who use data – whether in public, private or other sectors. This is not sufficient, however. Trust in data governance, and a national data system is established through legitimacy. This includes systems and standards that guarantee public and private sector compliance, government itself adhering to personal data protection rules, and government sharing public data.

The framework instils the importance of collaborative and evidence-based policy processes for the domestication of the policy proposed. The governance and institutional arrangements should assign clear roles to the government as policy maker and independent, agile and capacitated regulators to implement policy and effectively regulate the data economy to ensure that fair competition produces positive consumer welfare outcomes. The creation of data and information regulators to promote and safeguard the rights of citizens and their participation and fair representation in the data economy and society will need to be a priority for those countries that have not yet established these. Coordination with other regulators to achieve this will be essential. The legal ecosystem must be harmonised and rebalanced.

Access to data is a prerequisite for value creation, entrepreneurialism and innovation. When data are of poor quality or not interoperable, they

limit the capacity of firms and the public sector to engage in the sharing and analytics that can provide economic and social value to data. These processing frameworks should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity. Security models also need to be transversal, with specific emphasis on cloud storage and processing of sensitive/proprietary data, API management, and support of equitable data economies.

Attention needs to be paid to access to quality, interoperable and reliable data – primarily from the state but also from the private and other sectors – with a reinvigoration of the principles of open governance across the continent. Capacity-building should be a key national and regional priority, and resources will need to be allocated in this regard in the areas of data protection, cybersecurity and institutional data governance in relevant agencies. Skills and an understanding of the data ecosystem will also need to be built in state institutions, amongst other sectors and communities.

The framework is guided by the broad principles of transparency, accountability of institutions and actors, the inclusion of stakeholders, equity among citizens and fair competition amongst market players. The principles guiding the framework include trust, accessibility, interoperability, security, quality and integrity, representativity and non-discrimination.

As the framework emphasises, transversal collaboration needs to be underpinned with mechanisms to stimulate demand for data, which includes incentivising innovative data communities, and, on the supply-side, ensuring the quality, interoperability, and relevance of data in both the public and private sectors and civil society.

As the framework suggests, there are several regional processes, mechanisms and instruments that can and should be leveraged in the

continent's efforts to develop a cohesive data policy framework. These include the African Continental Free Trade Agreement (AfCFTA), which provides an opportunity for cooperation on a number of important aspects of the policy framework. Collaboration between national and regional stakeholders is also necessary for African countries to become more competitive in global policy setting forums where regulations for the global data economy are set and where African states have largely been "standard takers".

It is recognised that different African states have different economic, technical, and digital capabilities, and the recommendations and actions need to be read in this light. It is nevertheless envisaged that the different demands of building a data ecosystem will be progressively realised by countries. At the same time, there are several areas that can be attended to independently of economic or technical capabilities, including establishing regulatory independence, promoting a culture of trust and ethics, building collaborative frameworks for relevant sectors, developing transparent, evidence-based and participatory policy and regulations, participating in collaborative regional processes and mechanisms, and ratifying the AU Convention on Cybersecurity and Personal Data Protection.

The Framework presents a set of detailed recommendations and arising actions to guide member states through the formulations of policy in their domestic context, as well as recommendations to strengthen cooperation among countries and promote intra-Africa flows of data. The main high-level overarching recommendations are included here. It is recommended that Member States:

- cooperatively enable data to flow on the continent while safeguarding human rights, data protection, upholding security and ensuring equitable sharing of the benefits;
- cooperate to create the necessary data capabilities to take advantage of data-reliant technologies and services, including the

capacity to govern data so that it benefits African countries and citizens and enables development;

- promote transversal data policy and agile regulation to navigate the emergence of new dynamic data-driven business models that can foster intra-Africa digital trade and data-enabled entrepreneurship;
- create co-jurisdictional frameworks for the coordination of autonomous competition, sector, and data regulators to regulate the data society and economy effectively, formulate, implement, and review data policy in a dynamic, forward-looking and experimental way;
- develop national legislations on personal data protection and adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment;
- establish or maintain independent, well-resourced and effective Data Protection Authorities, strengthen cooperation with DPAs from members of the African Union and develop mechanisms at the continental level to develop and share regulatory practices and support institutional development to ensure a high level of protection of personal data;
- promote interoperability, data sharing, and responsiveness to data demand through the setting of open data standards in data creation conform to the general principles of anonymity, privacy, security and any sector-specific data considerations to facilitate non-personal data, and certain categories of personal data are accessible to African researchers, innovators and entrepreneurs;
- promote data portability so that data subjects are not locked into a single provider and, in so doing, promote competition and consumer choice and enable gig workers to move between platforms;

- improve unevenly developed infrastructure across the continent, leveraging existing REC regional efforts to support efficient broadband network coverage, reliable energy supply, and foundational digital (data) infrastructure and systems (FDI) (digital identity (Digital ID)), interoperable trustworthy payments, cloud and data infrastructure, and open data sharing systems, for cross border digital trade, e-commerce;
- establish an integrated national data system to enable data-driven public and private value creation, operating on the basis of harmonised governance frameworks that facilitate the flow of data necessary for a vibrant data economy, but with sufficient safeguards to be trusted, safe and secure;
- govern the integrated national data system according to the principles of access, availability, openness (where anonymity can be preserved), interoperability, safety, security, quality, and integrity;
- integrate sector-specific and specialists data codes or guidelines into national and continental data governance regimes; those who have not yet ratified the AU Convention on Cyber Security and Personal Data Protection, do so as soon as possible to serve as the foundational step for the harmonisation of data processing; and in the forthcoming negotiations on Trade in Services and E-commerce protocols, as well as the Competition and Intellectual Property protocols, in the African Continental Free Trade Area provide guidelines to promote access to data to support local innovation, entrepreneurialism and pro-competitive purposes;
- prioritise politically neutral partnerships that take into account individual sovereignty and national ownership to avoid foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States;

- promote research, development and innovation in various data-based areas, including Big Data Analytics, Artificial Intelligence, Quantum Computing, and Blockchain.

It is further recommended that The African Union Commission, RECs and Regional Institutions:

- facilitate collaboration between the various entities dealing with data across the continent through the establishment of a consultation framework within the digital ecosystem community to safeguard the interest of each actor;
- promote and facilitate data flows within and among AU Member States by developing a Cross Border Data Flows Mechanism that takes into account the different levels of digital readiness, data maturity as well as legal and regulatory environments of countries;
- facilitate data circulation across sectors and cross borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security;
- work in close collaboration with national authorities in charge of personal data protection of AU members, with the support of the African Network of Authorities (RAPDP), to establish a coordination mechanism and body that oversees the transfer of personal data within the continent and ensures compliance with existing laws and rules governing data and information security at national level;
- establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards;
- establish mechanisms and institutions , or empower existing ones, within the African Union to build capacity and render technical assistance to AU Member States for the domestication

of this data policy framework; and support the development of regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and Artificial Intelligence) and the necessary enabling environment and data-sharing mechanism to ensure the circulation across the continent;

- work towards building a secure and resilient cyberspace on the continent that offers new economic opportunities through the development of an AU Cyber Security Strategy and establishment of Operational Cybersecurity Centres to mitigate risks and threats related to cyberattacks, data breaches, and misuse use of sensitive information;
- enable data sharing and enhanced interoperability among AU Member States and other AU mechanisms, including the African Union Mechanism for Police Cooperation (AFRIPOL);
- establish an Annual Data Innovation Forum for Africa to raise awareness amongst policy makers about the power of data as the engine of a digital economy and society so as to facilitate exchanges among countries and enable knowledge sharing on data value-creation and innovation and the implications of data usage on peoples' privacy and security;
- strengthen links with other regions and coordinate Africa's common positions on data related international negotiations to ensure equal opportunities in the global digital economy;
- develop an implementation plan that takes into consideration the digital sovereignty of states as well as the different levels of development, the vulnerability of populations and digitisation within AU Member States, namely aspects related to ICT infrastructure gap and lack of cybersecurity policies and legislations.

34.2 Guiding Principles of the Framework

(Chapter 5.1 original text) The Data Policy Framework needs to align with the AU values and International law to achieve greater unity and solidarity between African countries and their people, ensuring balanced and inclusive economic development, including promoting and protecting peoples' rights through the African Charter on Human and Peoples' Rights and other relevant instruments.

In the spirit of fostering regional prosperity, economic growth and development, social progress and coordinating continental efforts, the following high-level principles guide the framework.

Cooperation: African Union Member States shall cooperate in exchanging data, acknowledging data as a central input of the global economy and the importance of the interoperability of data systems to a flourishing African digital single market.

Integration: the Framework shall promote intra-Africa data flows, remove legal barriers to data flow, subject only to necessary security, human rights and data protection.

Fairness and inclusiveness: in the implementation of the Framework, Member States shall ensure it is inclusive and equitable, offering opportunities and benefits to all Africans, and in so doing, seek to redress national and global inequalities by being responsive to the voices of those marginalised by technological developments.

Trust, safety and accountability: Member States shall promote trustworthy data environments that are safe and secure, accountable to data subjects, and ethical and secure by design.

Sovereignty: Member States, AUC, RECs, African Institutions and International Organisations shall cooperate to create capacity to enable African countries to self-manage their data, take advantage of data flows and govern data appropriately.

Comprehensive and forward-looking: the framework shall enable the creation of an environment that encourages investment and innovation

through the development of infrastructure, human capacity and the harmonisation of regulations and legislation.

Integrity and justice: Member States shall ensure data collection, processing and usage are just and lawful, and data should not be used to discriminate unfairly or infringe peoples' rights.

34.3 Recommended Actions

These are the recommended actions of chapter 5 on "Data Policy Framework"[457].

34.3.1 Foundational Data Infrastructure

Broadband and Data Access and Use (5.3.1.1). Actions:

Member States will need to evolve policies that:

- proscribe prohibitive 'right of way' broadband cable fees and support infrastructure sharing;
- prevent anti-competitive practices arising from dominance in infrastructure markets;
- invest in public Wi-Fi and complementary technologies;
- adopt innovative spectrum utilisation techniques such as dynamic spectrum allocation and access, and the leverage of digital dividend (spectrum bands largely expedited by the analogue to digital broadcasting migration) to expand broadband access for under-served rural areas;
- promote the transition and adoption of IPv6[7], as IPv4 resources become more depleted globally;
- invest in national backbone and cross-border connectivity infrastructure such as Internet Exchange Points (IXPs) at both national and regional levels to leverage available international bandwidth, lower in-

[457] *Pages 18-64.* Full text: https://au.int/en/documents/20220728/au-data-policy-framework.

ternet access cost and enhance data access speeds within the region; and

- leverage innovative models for data infrastructure funding.

Data Infrastructure (5.3.1.2). Actions

- As opposed to focusing on the significant upfront investment to replace depreciating legacy ICT equipment, Member States should leverage economies of scale and scope to adopt infrastructure that supports facilitating benefits offered by cloud services and other new technologies that support data value creation.
- Tax, trade (including investment and innovation) and competition policies must be coherent, complementary, and adapted to the data-driven digital economy, particularly to inform infrastructure development strategies.
- Member states must ensure local firms participate in value chains of foreign software as a service (SaaS), infrastructure as a service (IaaS) and platforms as a service (PaaS) providers for state procurement and create incentives to have local SMMEs in data value chains across industries. This can be done by ensuring tax, trade (including investment and innovation), and competition policies are coherent, complementary, and adapted to the data driven digital economy.
- Adopt more sustainable electricity generation models domestically and across the region, to ensure foundational digital infrastructure supports sustainable domestic and cross-border data activities that have fewer extractive impacts on the natural environment.
- Creating data portability rights - including for non-personal data, to make it easier for customers of cloud services to switch between providers.
- Develop contractual standards for public organisations (that can be used by SMEs too) that protect their rights to access, retrieve, delete, etc., the data (including non-personal, again) that is processed by cloud providers.

- Develop Fair, Reasonable and Non-Discriminatory (FRAND) licensing obligations for platforms and cloud providers who have access to datasets that become a vital resource to enter a market.

Creating Legitimate, Trustworthy data Systems (5.3.2). Actions:

- Safeguard basic human rights in the digital environment through the rule of law.
- Ensure institutional arrangements and regulations are established only through inclusive, consultative and transparent processes.
- Ensure institutions responsible for overseeing the use of data, as well as public and private data producers, are accountable for the use of public and personal data to those whose data is used.
- Strengthen cooperation with other DPAs to ensure sufficient safeguard and reciprocal protection of personal data as well as individual and collective digital rights across the continent.
- Strengthen Mutual Legal Assistance Agreements and activities across states for the investigation and prosecution of cybercrimes.
- Ensure institutions responsible for overseeing the use of personal data are empowered to have powers of entry and inspection for purposes of enforcement of privacy and data protection laws and regulations.
- • Further ensure institutions responsible for overseeing the use of personal data have the following corrective powers in relation to correcting infringement of aspects of misuse and abuse of personal data:
- Issue warnings to a data controller or data processor that intended processing operations are likely to infringe provisions of the relevant data protection laws and regulations.
- Issue reprimands to a data controller or a data processor where processing operations infringe provisions of the relevant data protection laws and regulations.
- Order a data controller to communicate a personal data breach to affected data subjects.

- Impose a temporary or definitive limitation, including a ban on personal data processing.
- Order the suspension of data flows to a recipient in a third country or to an international organisation that does not provide adequate protection similar to that of the data exporting country.
- Institutions responsible for overseeing the use of personal data should be empowered to either assist or seek a court's indulgence to assist a person who has suffered material damage as a result of an infringement of their personal data to receive compensation from a data controller or data processor for the damage suffered.

Data Ethics (5.3.2.5). Actions:

- The data industry and research communities using data need to formulate and implement codes of practice, including the principles of responsibility and ethics by design through processes that include those whose data is affected.
- Member States must require rights-compliant ethical frameworks in public procurement processes.
- Members should include the assessment of data codes of ethics in the mandates of existing human rights bodies such as Human Rights Commissions.

Institutional Arrangements for Regulation (5.3.3) Actions:

- Members with data regulators should assess whether the existing enforcement powers are sufficient.
- Members creating data regulators should consider a range of enforcement powers and in addressing resource constraints, how data regulators could potentially rely on other agencies for enforcement.

Rebalancing the Legal Ecosystem (5.3.4)

- Contracts that purport to give up digital rights, personal data protection and that inhibit competition should, as a general rule, be unenforceable. This can be articulated in data protection and competition regulation, which can also consider on a case by case basis whether

the pro-competitive effects of such contracts outweigh the anticompetitive effects.

- National law reform commissions or similar expert legal institutions should investigate and consider how to harmonise different branches of laws, regulatory regimes and supervisory authorities that deal with data.
- Member States should support the update or adoption of competition law frameworks and regulations that consider the challenges of analysing competition issues, designing remedies and enforcing their powers to safeguard competition in data-driven markets, as well as building the capacity of competition regulators to implement these rules.
- Intellectual property laws should be amended to provide:
  that if copyright applies to databases and compilations of data at all, it shall apply only to the work of human authors that exhibit originality/creativity and that the copyright extends only to the original selection and arrangement of data in a database or compilation and not to the data itself;
- that any copyright or other intellectual property right, including trade secrets that enables control of data, does not apply to personal data;
- that any copyright or other intellectual property right, including trade secrets that enables control of data, is limited by the provisions of competition regulation and alternative rights that offer protection to local innovations not envisaged in current frameworks;
- adaptations to existing IPR regimes to leverage next frontier technologies, such as enabling AI to use data;

Consultative and Evidence-Based Regulations (5.3.4.2) Actions:

- Clearly distinguish between the roles of the state as policy maker and the regulator, which should be sufficiently independent of the state and industry, so as to implement policy in the public interest.
- Create or maintain competition authorities to deal with dominance in the market and concentration through mergers and acquisitions.

- Implement clear procedures for co-jurisdiction between sector and competition authorities to ensure the coordinated regulation of digital infrastructure and services sector and to avoid 'forum-shopping'.
- Data regulators should collaborate at the regional and continental levels to harmonise their frameworks, particularly in support of the AfCFTA.
- Those subject to decisions of regulatory authorities should have clear mechanisms of appeal and redress heard by a different body from the regulator, making the decisions in line with the rules of natural justice and fair administrative action.

Creating Public Value (5.3.5) Actions:

- Sector regulators and public data stewards must operate within specific guidelines on how data quality assessments should be implemented, depending on common use cases, algorithms, and type of data used. These guidelines can be informed by global best practices (including data and AI governance) but should be adapted to the context of African data use cases. Due to the exchange, combinations, strategic storage, and repurposing are required to create data value. An effective data quality strategy across the public sector should be informed by technical/practical/operational realities and should outline the roles, responsibilities, and mandates of various government agencies in collecting and maintaining high-quality data in a manner that safeguards citizens.
- Member States need to participate in efforts to establish and adopt a normative framework for harmonised data standards and systems aimed at establishing national, regional, and international interoperability. These may include targeted human, technical, and institutional training interventions, sub-regional infrastructure projects, and REC regulatory sandboxes.
- A continental approach facilitates economies of scale to incentivise private investments in foundational digital infrastructure, including cloud-based technologies. Regional harmonisation of regulations for

data governance could further reduce compliance costs and reduce uncertainty and operational risk for major ICT related infrastructure investments.

- Public institutions that curate data should be adequately resourced in order to contribute to multilateral fora regarding data and to be stewards of inclusive access and responsible use of data guided by appropriate industry technical and regulatory norms, standards, and best practices that underpin both the informational and economic characteristics of data in priority industries.

Data Governance (5.4) Actions:

- Data protection authorities (DPA) need full empowerment, including the remit on data sovereignty.
- DPAs are encouraged to adopt international and regional cooperation practices taking note of different stages of implementation and enforcement across the Member States.
- Risk assessment and multi-stakeholder engagement should be used to design data localisation solutions in policy by drafters, which includes civil society participation.
- Data infrastructure policy should be aligned with data control imperatives by policy drafters but must consider cybersecurity, personal data protection, environmental risks and cost.
- Public administration and investment policy should align with data control capacities as a priority.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation.

Data Processing and Protection (5.4.2)

- Data processing frameworks should be established in partnership with all relevant multi-stakeholder partners but driven ideally by the DPA. These should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limi-

tation; data quality; security safeguards; openness (including incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity.

- DPAs should be established as a matter of urgency alongside national legislation on personal data protection.

Data Access and Interoperability (5.4.3). Actions:

- Member States should establish an open data policy which sets open standards for the production and processing of data so that when decisions are made to open the data, the high costs of ensuring it is usable and manipulatable are avoided.
- Sectoral laws and codes of conduct from DPAs should be reviewed to ensure lawful data access in conjunction with the data policy.
- DPAs should have dual access to information and privacy function.
- Multi-sectoral open data initiatives should be implemented in priority data sectors like health, research and planning.

Data Security (5.4.4). Actions:

- Member States, who are yet to develop cybersecurity measures, should immediately develop cybersecurity plans and streamline them within government governance structures to promote robustness and reduce vulnerabilities.
- Cybersecurity institutions like CSIRTs should be incorporated into data policy development.
- Data processing roles as a form of security protection should be specified in policy by policymakers.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation and could be supported by DPAs.

Cross-Border data Flows (5.4.5). Actions:

- DPAs should ascertain minimum standards for data transfer.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured

through policy and asset allocation and driven ideally by DPAs in conjunction with educational facilities and government skills programmes and units.

Data Demand (5.4.6). Actions:

- Data communities should be incorporated into data policy-making processes by policymakers.
- Data communities should be drawn into the establishment of open government data initiatives by departmental implementers.
- Universities should be included as relevant policy stakeholders to help establish the "knowledge-base" from which the local data economy can draw sufficient scientific and technological knowledge.

International and Regional Governance (5.5).
Continental Data Standards ((5.5.1). Actions:

- Establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards.

Continental Instruments (5.5.3). Actions:

- Member States should ratify the AU Convention on Cybersecurity and Personal Data Protection and develop additional protocols, as required, to reflect changes since the original drafting.
- Establish, or empower a mechanism within the African Union for centralising regional engagements on data standards.
- Once adopted, alignments with the AfCFTA process should immediately be explored.
- Include data in negotiations on the AfCFTA chapters on competition and intellectual property.
- Agree on common and consistent criteria for assessing adequacy in the levels of protection of personal data across the continent to facilitate and enable trans-border transfer of data and standardise protection.