African School on Internet Governance (AfriSIG) 2025 Output Document: An African Perspective on Data Governance At All Levels

Presented for the consideration of the Commission on Science and Technology for Development (CSTD) Working Group on Data Governance

Finalised version - 30 June 2025

Preamble: About this document

This document was developed by a group of individuals from different sectors and stakeholder groups across Africa who were gathered together in Dar es Salaam, Tanzania, from 23 to 28 May 2025 for the 13th annual African School on Internet Governance (AfriSIG)[1]. People who contributed to this text include government officials, journalists, policy analysts, digital and human rights defenders, women's rights groups, national and regional internet governance forum organisers, telecommunications regulators, members of parliament, data governance professionals and members of the technical community. The structure of the document draws on the text on data governance in the Global Digital Compact (2024). The document has three sections: Section A covers principles that apply to data governance. This section draws on the 2022 African Union Data Policy Framework but we believe they have universal relevance. Section B looks at interoperability between data governance systems and Section C at sharing

1 AfriSIG is a joint project of the African Union Commission, the Association for Progressive Communications and Research ICT Africa - http://afrisig.org

the benefits of data. Section D proposes options for safe, secure and trusted cross-border data flows.

While the suggestions in this document represent an African perspective and address African stakeholders, we believe it will be of value to the CSTD Working Group on Data Governance.

Section A: Fundamental principles of data governance

The group endorses the principles of the African Union (AU) Data Policy Framework (AUDPF) accepted by the AU Executive Council in February 2022.[2] These principles align with international law and aim to achieve greater unity, solidarity, and inclusive development across the continent while protecting human and peoples' rights as enshrined in the African Charter on Human and Peoples' Rights.[3] They include:

Cooperation: Data exchange and interoperability to support a robust digital single market.

Integration: Promoting intra-Africa data flows with strong data protection.

Fairness and inclusiveness: Ensuring responsiveness to marginalized voices.

Trust, safety, and accountability: Creating safe, ethical, and secure data environments.

Sovereignty: Enabling African countries to self-manage and govern their data.

Comprehensive and forward-looking: Encouraging innovation, harmonization, and investment.

Integrity and justice: Ensuring fairness and legal safeguards in all data processes.

The AfriSIG group also proposes the inclusion of five additional principles which they believe complements the AUDPF principles, namely:

2 https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf
3 https://au.int/en/treaties/african-charter-human-and-peoples-rights

Multistakeholder participation: Systems and policies must intentionally incorporate the perspectives of different stakeholders, and, in particular, reflect the needs of underrepresented groups such as women, youth, persons with disabilities, and rural populations.

Regulatory clarity: Legal and regulatory frameworks should be transparent, coherent, and enforceable across sectors and borders.

Data justice: The entire data lifecycle - collection, processing, use, and governance - must promote fairness, equity, and inclusivity. Data practices can reinforce or disrupt existing power asymmetries and must therefore be designed to uphold dignity, equality, and the rights of all people. Data justice calls for participatory governance, equitable access to data, and redress mechanisms to address harm and exclusion.

Sustainability and environmental justice: Sustainability and environmental justice require that data governance frameworks emphasize green data infrastructure, circular economy practices, and climate-aligned policies.

Data access as a tool for advancing human rights: Equitable access to data, encompassing statistics, datasets and research findings, is essential for nurturing a just, informed, and inclusive society in the digital era and is an extension of the right to access to information.[4]

Section B: Interoperability of data systems

While both the AU Data Policy Framework and the African Continental Free Trade Area (AfCFTA) Protocol on Digital Trade stress the need for harmonized data governance, fragmented legal environments remain a critical barrier. The following can help address this:

Common public standards: Policymakers should prioritize the adoption and implementation of common public and internationally recognized data standards to enhance system

4 From the 2024 African Commission on Human and Peoples' Rights resolution on "Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age. https://achpr.au.int/en/adopted-resolutions/620-data-access-tool-advancing-human-rights-and-sustainable-development ACHPR/Res.620 (LXXXI)

interoperability. Standards for interoperability must be adaptable and accommodate language diversity and accessibility for people with disabilities. They should ensure that systems across sectors and borders can interact efficiently while safeguarding data privacy and security. This should be complemented by robust encryption and authentication mechanisms to protect data integrity and privacy.

Data stewardship, citizen participation, and the inclusion of mechanisms for redress in interoperability frameworks: This will foster public trust and encourage compliance.

Capacity building: Capacity is needed in regional bodies involved in harmonization, such as the AUC and Regional Economic Communities (RECs) to enable them effectively coordinate the development and adoption of joint standards, accountability mechanisms and digital integration initiatives. Capacity is needed at the level of data systems, but human capacity building is an even more important dimension of interoperability. Capacity is needed at the level of communities who generate data, civil society and data justice defenders, civic education groups, the media, schools and universities - nationally, regionally and internationally. Parliamentarians also need capacity to be able to play their oversight role effectively. Peer learning and technical assistance are powerful means of strengthening capacity and should be encouraged and supported within stakeholder groups but also at multistakeholder level.

Partnerships: Partnerships between governments as well as between government and civil society, government and the private sector as well as multistakeholder collaborations should be encouraged to support capacity development and facilitate interoperability.

Investing in interoperability: Investment priorities should include:

- Shared regional data centers
- IPv6-ready infrastructure
- Peering databases and neutral IXPs
- Public-private partnerships to boost infrastructure gaps
- Multistakeholder collaborations between governments, researchers, the private sector, and civil society

Section C: Sharing the benefits of data

The African Commission on Human and Peoples' Rights' 2024 resolution (*ACHPR/Res.620 (LXXXI)*) affirms access to data as an extension of the right to information. It recognizes data's transformative potential to strengthen democracy, drive innovation, enhance public participation, and advance evidence-based policymaking—critical for achieving the Sustainable Development Goals (SDGs) and Agenda 2063: The Africa We Want.

To ensure benefits are widely shared, the following considerations must guide data governance:

Accessibility, openness and data as a public good: Data must be recognised as a public good, particularly where it enables innovation and inclusive development in sectors such as health, education, climate resilience, and public infrastructure.

Governments should promote open data initiatives that allow secure access to non-personal and anonymised datasets for public interest research and advocacy, while maintaining strong data protection safeguards to prevent misuse and harm.)

Maximum disclosure and data commons: Public interest data held by state or private actors (where overriding public interest exists) should be available by default, limited only by justifiable human rights protections. This fosters a *data commons* serving collective needs.

Data sharing: Data sharing practices must be transparent and rights-respecting, ensuring non-discriminatory data use and proactive safeguards against bias. The use of value-sharing agreements to ensure security and fair data exchange should be explored.

Equitable value-sharing: Equitable benefit sharing should include fair compensation and recognition for communities and individuals who generate or contribute data, especially those whose experiences are often excluded from digital systems.

Ensure that communities and individuals have a say in how their data is collected, used, and deleted to foster trust and data integrity.

Underserved communities must receive compensation or recognition for data contributions.

Inclusive monetization models are needed to address regional content gaps and prevent exploitation by dominant actors (e.g., global tech firms).

Cross-border data policies (e.g., seamless "data roaming") should support the *African Free Trade Area* and *Digital Single Market*, enabling affordable interoperability.

Privacy and accountability: Strong safeguards—transparent consent, grievance mechanisms, and anti-bias protocols—must accompany data access. Governance frameworks should include public oversight, enforceable redress systems (e.g., online dispute resolution), and clear rules for data deletion.

Data literacy: Resources should be directed toward both community-based and institutional data literacy programs, with a focus on empowering women, youth, and marginalized groups. These initiatives are necessary to promote equitable participation in the digital economy and ensure informed consent in data sharing. Prioritize data literacy for women, youth, and marginalized groups through community/institutional programs and ensure grassroots, media, civil society, and SMEs can participate in data economy initiatives.

Inclusive governance: Stakeholders must co-develop governance models that confront power asymmetries and distribute data's economic/social value equitably.

Communities should have agency over how their data is collected, used, and deleted.

Global and regional collaboration: Global collaboration is as important as regional collaboration and the international community and organisations need to advance better data benefit-sharing systems.

Fair taxation policies: Digital taxation policies must avoid overburdening local innovators while prioritizing local value creation and ensuring that multinational operators pay sufficient taxes proportionate to the profit they make from data gathered from African jurisdictions.

Section D: Safe, secure and trusted data flows

To achieve digital transformation, Africa must establish robust frameworks that facilitate safe, secure, and trusted data flows, while ensuring economic growth and the protection of fundamental rights. Cross-border data governance is critical for Africa's integration into the global digital economy while safeguarding sovereignty, security, and equitable access. The following recommendations outline key measures necessary to achieve secure and interoperable data governance across the continent.

A Human Rights-Based Approach (HRBA) to data governance: Africa's approach to cross-border data flows must be anchored in human rights principles, inclusive governance, and equitable access. Data governance mechanisms should be designed to uphold individual rights, foster transparency, and mitigate risks related to misuse, surveillance, and exploitation. Regional digital cooperation must be inclusive and built on ethical considerations, and data protection frameworks should empower citizens rather than merely serve corporate or state interests.

Building trust and security through governance and technical safeguards: A robust and harmonized regulatory framework is essential for fostering trust in cross-border data flows. The establishment and operationalization of national and regional data protection laws that align with African and global standards—such as the Malabo Convention, GDPR, and OECD Guidelines—will provide much-needed clarity and accountability. Effective enforcement by independent and empowered data protection authorities will guarantee transparency and regulatory compliance.

From a technical standpoint, Africa must incorporate Zero Trust Architecture (ZTA)[5] principles, ensuring that no entity—whether internal or external—is automatically trusted. This model enforces rigorous authentication, granular access control based on the principle of least privilege, and micro-segmentation to mitigate security threats. Privacy-Enhancing Technologies (PETs) such as end-to-end encryption, anonymization protocols, secure data centres, and layered security measures must be deployed to safeguard sensitive personal and biometric data.

5 "ZeroTrust Architecture (ZTA)" means no user or device is trusted by default; access is based on identity verification and minimal privilege.

Moreover, Africa should develop regional trust frameworks and certification mechanisms, enabling mutual recognition of compliance and standards across jurisdictions. These frameworks will reduce legal uncertainty, promote interoperability, and facilitate seamless digital transactions.

Strengthening governance structures and cross-border collaboration: African states should domesticate the AUDPF and establish similar institutional structures to ensure implementation at the national level. To enable seamless data exchange, standardized technical protocols should be promoted, ensuring consistency in data formats, interoperability, and digital infrastructure.

To foster bilateral and multilateral cooperation, African regional economic communities should negotiate enforceable cross-border data-sharing agreements that integrate cybersecurity provisions from the AfCFTA digital trade provisions, AUDPF, and the Malabo Convention. This action will enhance interoperability, strengthen trust between states, and provide legal clarity regarding data sovereignty.

Additionally, dispute resolution mechanisms must be developed to address violations and abuses, ensuring that cross-border data flows uphold the dignity of individuals. A system for public redress and complaint resolution will bolster confidence in Africa's digital governance framework.

Capacity building, digital inclusion, and equitable access: For cross-border data governance to be effective, it must be inclusive and participatory. Trusted data sharing must be anchored in multi-stakeholder governance, ensuring that marginalized communities have a voice in decisions regarding how data about them is used and shared. Digital inclusion is critical for ensuring equitable access to the benefits of data-driven innovation, strengthening public trust, and mitigating risks related to surveillance, exploitation, and discrimination.

Security depends on collaboration: African nations must invest in cybersecurity infrastructure and digital capacity-building programs that empower institutions and individuals across governments, civil society, and the private sector. By fostering digital literacy, stakeholders will gain an understanding of data rights, informed consent, risk awareness, and ethical data handling, ensuring that Africa's data governance ecosystem is transparent and accountable.

Additionally, Africa must strengthen the maturity of its cyber defence capabilities through cross-border cooperation between Security Operation Centres (SOCs), Cyber/Computer Security Emergency Response Teams (CSERTs), and Information Sharing Analysis Centres (ISACs). These structures will play a pivotal role in incident response, data security monitoring, and safeguarding against cyber threats that undermine trust in digital governance.

Common public standards: Policy frameworks must prioritize standardized technical protocols to ensure system interoperability and data portability. By implementing these measures, Africa can build a data governance model that is inclusive, resilient, and forward-looking, enabling both innovation and human rights protections within a secure digital ecosystem.

END