



SUBMISSION BY THE AFRICAN INTERNET RIGHTS ALLIANCE (AIRA)

on the Draft

African Guidelines on Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age

In fulfilment of ACHPR/Res.620 (LXXXI) 2024

Submitted to the Secretariat of the African Commission on Human and Peoples' Rights,
Banjul, The Gambia

For the attention of the Special Rapporteur on Freedom of Expression and Access to
Information in Africa, Honourable Commissioner Ourveena Geereesha Topsy-Sonoo

July 2026

About the African Internet Rights Alliance

The African Internet Rights Alliance (AIRA) is a coalition of ten civil society organisations working across the continent to protect and advance digital rights: Amnesty International Kenya; ARTICLE 19 Eastern Africa; BudgIT (Nigeria); the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University (Kenya); the Collaboration on International ICT Policy for East and Southern Africa (CIPESA); Co-Creation Hub; KICTANet (Kenya); the Legal Resources Centre (South Africa); Paradigm Initiative; and Pollicy (Uganda).

Between them, AIRA's members hold decades of experience in strategic litigation, policy advocacy, applied research and community programming on freedom of expression and access to information; afrofeminist approaches to technology and women's rights online; children's rights, including the right to education; surveillance and digital authoritarianism; and the governance of artificial intelligence and data-driven systems. Members of the Alliance have litigated and analysed the leading African data governance cases of the past five years, produced continental research on gender data and technology-facilitated gender-based violence, documented network disruptions and state surveillance, monitored fiscal transparency and open data practice, and developed African methodologies for auditing algorithmic systems. This submission draws directly on that body of litigation, research and on-the-ground experience.

AIRA welcomes the opportunity to contribute to this consultation and stands ready to participate in validation convenings, to support the Special Rapporteur's continued consultations, and to assist member states and the Commission in the implementation phase.

Executive Summary

AIRA strongly welcomes and endorses the draft African Guidelines on Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age. The draft is, to our knowledge, the first continental normative instrument to treat access to data – including data held by private actors and dominant digital platforms – as a component of the human right of access to information, and to do so from the standpoint of a region whose people have too often been the objects of data extraction rather than the beneficiaries of data use.

Our endorsement is accompanied by substantial proposals for strengthening.

First, the Guidelines must be fortified against inversion. That is, an instrument built to open the state's data to the people must not be capable of being read to open the people's data to the state.

Second, the Guidelines should network disruptions and internet shutdowns as an issue. This is because a right of access to data has no meaning for a population that has been disconnected.

Third, the gender, child-rights and disability dimensions of data access should be deepened from welcome clauses into operative frameworks.

Fourth, the pioneering provisions on platform data access and AI accountability should be tightened in light of hard lessons from other jurisdictions, where voluntary access has collapsed and statutory access has been territorially fenced in ways that exclude African researchers.

Fifth, implementation must be designed for African institutional realities such as financing, capacity, languages, and the informal and offline lives of most Africans, rather than transplanted from regulatory contexts with fundamentally different endowments.

Part I: Overall Assessment

AIRA supports the draft's architecture: its principles, general measures, legal and programmatic measures, exemptions and safeguards, enforcement, AI-specific provisions, and appendices on specific data categories and institutional design. Beyond these, we particularly welcome: the protection of public interest disclosures and whistleblowers (paragraphs 15 and 22); the duty to create, keep and maintain data (paragraph 16); the prohibition on requiring requesters to demonstrate an interest (paragraph 20(a)(iv)); the narrow, harm-based construction of exemptions with a public interest override (paragraph 21); the tiered enforcement framework with judicial authorisation as a precondition for severe sanctions (paragraph 27), which guards against the weaponisation of enforcement; and the environmental transparency provisions extending to data centres' energy use and electronic waste (general measure 10 and Appendix A).

Our proposals below are therefore offered to strengthen an instrument whose direction we endorse.

Part II: Cross-Cutting Priorities

2.1 Guarding against inversion: access to data must never become access to people

The single most important structural risk in any data access instrument is inversion: that provisions designed to open the state's data to the people are read, in practice, to open the people's data to the state. This risk is not hypothetical on our continent. Research on the implementation of African data protection laws has identified broad exemptions for state agencies and limited regulator independence as the two principal deficits, citing, for example, Kenyan amendment legislation empowering security services to access personal

data held on any phone or computer.¹ The same period has seen a record intensification of state control over digital space: 2024 was the worst year ever recorded for internet shutdowns in Africa, with 21 shutdowns across 15 countries.² An instrument adopted into this environment must be drafted defensively.

Two provisions require attention. General measure 7 permits public sector bodies to gain access to data held by private bodies in situations of 'genuine and demonstrable overriding public interest'. The draft's safeguards – strict necessity and proportionality, 'independent oversight or judicial review', security protocols – are welcome but insufficient. The disjunctive 'or' allows a state to route such access through an administrative body it controls. Our members' litigation experience, from Huduma Namba to Worldcoin, teaches that ex ante judicial control is the safeguard that actually bites in African legal systems: it was courts, not administrative structures, that halted unlawful biometric collection in Kenya.³⁴ State access to privately held data about identifiable persons should therefore require prior judicial authorisation as a rule, with narrow urgency exceptions subject to prompt post hoc judicial confirmation; it should be recorded, subject to periodic transparency reporting, prohibited in bulk or generalised form, and expressly unavailable as a route around legal frameworks governing surveillance and communications interception.

¹See International Association of Privacy Professionals, 'Report examines state of African nations' data protection laws, implementation efforts' (2026), discussing an Access Now policy paper identifying broad exemptions and limited authority independence as the principal implementation deficits, and citing Kenya's Statute Law (Miscellaneous Amendments) Act 2020 as an example of legislation enabling security services to access personal data, <https://iapp.org/news/a/evaluating-african-nations-comprehensive-privacy-laws-and-their-implementation>.

²Access Now and the #KeepItOn coalition, *Emboldened Offenders, Endangered Communities: Internet Shutdowns in 2024* (February 2025) (recording 296 shutdowns in 54 countries globally and 21 shutdowns across 15 African countries – the highest annual figure ever recorded for the region – with protests as the leading trigger; documenting long-running disruptions including on Annobón island, Equatorial Guinea, and continued sub-normal connectivity in Tigray and Amhara, Ethiopia), <https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2024/>.

³ *Republic v Joe Mucheru, Cabinet Secretary, Ministry of ICT and Others, ex parte Katiba Institute and Yash Pal Ghai*, High Court of Kenya, judgment of 14 October 2021 (Ngaah J) (declaring the Huduma card rollout ultra vires section 31 of the Data Protection Act 2019 and issuing mandamus compelling a data protection impact assessment; noting that the processing of biometrics and children's data implicated high risks to data subjects); see Privacy International (n above); Open Society Justice Initiative, 'New Kenya High Court Judgment Sets Important Precedent for Digital ID Privacy Protections and Processes' (15 October 2021).

⁴ *Katiba Institute and Another v Worldcoin Foundation / Tools for Humanity Corp and Others*, High Court of Kenya, judgment of 5 May 2025 (Aburili J) (declaring Worldcoin's biometric data collection unlawful for want of a data protection impact assessment and valid consent – holding that cryptocurrency inducements to economically vulnerable persons vitiated informed consent – and for unlawful cross-border transfers; ordering permanent deletion of all Kenyans' biometric data within seven days under the supervision of the Office of the Data Protection Commissioner). The supervised deletion, carried out on servers in Germany, was confirmed by the ODPC in late 2025 and early 2026. See CIPIT (Strathmore University), 'Kenya High Court's Worldcoin Determination: Upholding Consent, Accountability and Data Sovereignty in Biometric Data Processing' (2025), <https://cipit.strathmore.edu/kenya-high-courts-worldcoin-determination/>; 'Worldcoin: Intrigues of data privacy', Daily Nation (December 2025); 'Worldcoin deletes Kenyans' biometric data after court order', Business Daily (January 2026).

Second, paragraph 14(g) provides that where access to data serves an overriding public interest such as health, environment, elections, disaster response and countering gender-based violence, 'disclosure obligations should be absolute'. AIRA understands and shares the impulse, but 'absolute' is dangerous drafting. Data generated in precisely these domains is often data about people at their most exposed: survivors of gender-based violence, patients, displaced persons. An absolute disclosure obligation invoked in the name of countering gender-based violence could compel the release of data that identifies survivors, their locations or their health status – a catastrophic outcome for the people the clause exists to protect, in contexts where disclosure can mean violence. The clause should instead establish a strong presumption of disclosure of the relevant data in aggregated, anonymised or otherwise protective form, never displacing the safeguards in paragraph 22 or the personal-data exemption in paragraph 21(d)(i).

Recommendation 1. Amend general measure 7 to require prior judicial authorisation for public-body access to privately held data concerning identifiable persons, with narrowly defined urgency exceptions subject to prompt judicial confirmation; add duties of record-keeping and periodic public transparency reporting; prohibit bulk or generalised access; and state expressly that measure 7 may not be used to circumvent legal frameworks governing surveillance, communications interception or national security access.

Recommendation 2. In paragraph 14(g), replace 'disclosure obligations should be absolute' with language establishing a strong, expedited presumption of disclosure subject to the safeguards in paragraph 22, and add that data enabling the identification of survivors of gender-based violence, patients, children or persons in situations of vulnerability shall not be disclosed under this provision.

Recommendation 3. Add to the Key Principles a 'do no harm' principle: data access frameworks shall be designed and applied so that they cannot be used to facilitate surveillance, persecution, discrimination or the exposure of persons at risk, and any ambiguity shall be resolved in favour of the protection of persons in situations of vulnerability.

2.2 Connectivity and continuity: a right of access to data has no meaning offline and without consideration of the local communities.

The draft is comprehensive on formats, timelines, APIs and dynamic data, yet silent on the practice that most totally extinguishes access to data in Africa today: the network/internet shutdown. In 2024, authorities and warring parties imposed 296 shutdowns across 54 countries globally; Africa's 21 shutdowns across 15 countries were the region's highest annual figure since records began, with protests the leading trigger and several disruptions – including on Annobón island in Equatorial Guinea and in Tigray and

Amhara in Ethiopia — persisting for a year or longer.⁵ The economic cost to sub-Saharan Africa in 2024 alone has been estimated at over US\$1.6 billion.⁶ The Commission itself responded with Resolution 580 (2024), calling on states to keep the internet open before, during and after elections.⁷ The Guidelines' provisions on real-time access to dynamic data of public interest such as environmental monitoring, public health, disaster response (paragraph 20(c)), are nullified in their entirety by a shutdown.

Furthermore, data centres are a new form of development that is barely, if at all, regulated within African states and will take a massive strain on already struggling impoverished communities, local electrical grids and water sources⁸. These guidelines therefore need to emphasise that data infrastructure in Africa must be developed in line with a human rights framework and ensure that vulnerable communities are not sacrificed for it. We note that one of the purposes of the Guidelines is to promote the decrease in "unequal access to digital infrastructure". We do not disagree with this goal; however, we note that the rapid and irresponsible development of digital infrastructure, given the realities of data centres outlined above, will only worsen inequality in Africa. Africans cannot eat, drink or live in data centres⁹.

We therefore propose an express provision, in the Key Principles or the General Measures, recognising that network disruptions, throttling and platform blocking constitute interferences with the right of access to information and data under Article 9, recalling Resolution 580, and requiring that any restriction on connectivity satisfy the three-part test and never extend to periods of elections, public emergencies or armed conflict in a manner that deprives people of access to safety-critical data. The same logic extends to the quieter exclusions of the analogue divide: the draft's provisions on oral requests, support for non-literate persons and alternatives to online portals (paragraph 20) are commendable and should be reinforced with obligations to publish key datasets and metadata in widely used national and local languages and to maintain offline and community-mediated access channels, including through community radio, libraries and local government offices.

Recommendation 4. Insert an express provision recognising that internet shutdowns, throttling and the blocking of platforms or services violate the right of access to information and data under Article 9 of the African Charter; recalling ACHPR

⁵See note 2 above.

⁶Institute for Security Studies, 'Offline and silenced: Africa's quiet rise of internet repression' (2025) (estimating economic losses to sub-Saharan Africa from 2024 shutdowns at over US\$1.6 billion), <https://issafrica.org/iss-today/offline-and-silenced-africa-s-quiet-rise-of-internet-repression>.

⁷ACHPR, Resolution 580 (2024), calling on member states to ensure open and secure internet access before, during and after elections and to refrain from shutting down the internet during democratic processes; see Access Now (n above).

⁸ Reuters, 'Equinix faces challenge to Cape Town data centres over environmental concerns' <https://www.reuters.com/world/africa/equinix-faces-challenge-cape-town-data-centres-over-environmental-concerns-2026-06-04/>

⁹ Daily Maverick, 'New data centres set to swallow 34% of Cape Town's current electricity supply' <https://www.dailymaverick.co.za/article/2026-04-28-new-data-centres-set-to-swallow-34-of-cape-towns-current-electricity-supply/>

Resolution 580 (2024); and providing that dynamic data of significant public interest must remain accessible during elections, emergencies and conflicts.

Recommendation 5. Strengthen paragraph 20 and Appendix B with obligations to make proactively disclosed datasets, catalogues and metadata available in widely used national and local languages, and to maintain offline, analogue and community-mediated access channels for persons without connectivity or digital literacy.

Recommendation 6. The data centre considerations in General Measures 9 and 10 must be emboldened to acknowledge that creating safe and environmentally friendly data centres is a far more complex task and therefore these centers cannot be developed without a proper regulatory framework that considers all necessary factors, most importantly the socioeconomic impact on vulnerable communities.

2.3 Gender and intersectional data justice

AIRA welcomes Appendix A's requirements on sex-disaggregated data and safeguards against the stigmatisation of marginalised groups. The evidence base for going further is strong. Gender data on the continent remains under-collected and under-used: a study of national databases in 15 African countries, including Kenya, Nigeria and South Africa, found gender-disaggregated data available for barely half of gender-relevant indicators.¹⁰ What is not counted is not planned for, and also not budgeted for. At the same time, feminist scholarship and African feminist practice caution that visibility in data is not the same as protection by data: datasets can encode and amplify the very hierarchies they measure, and for women human rights defenders and survivors of violence being rendered visible in accessible datasets can itself be a source of danger.¹¹¹² Pollicy's Afro-Feminist Data Futures research and the 2023 Manifesto developed with feminist movements across the continent articulate the alternative: data governance in which African women are participants in design, not objects of collection.¹³

We propose three refinements.

¹⁰A 2019 Data2X study of national databases in 15 African countries — including Kenya, Nigeria and South Africa — found gender-disaggregated data available for only 52 per cent of gender-relevant indicators. Cited in Pollicy and My Data Rights, 'Shifting the Data Highway: Introducing the Afro-Feminist Data Governance Project' (2023), <https://mydatarights.africa/shifting-the-data-highway-introducing-the-afro-feminist-data-governance-project/>.

¹¹Catherine D'Ignazio and Lauren F Klein, *Data Feminism* (MIT Press, 2020).

¹²Linnet Taylor, 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4(2) *Big Data & Society*.

¹³Pollicy, Afro-Feminist Data Futures (research project, 2021–) and the Afro-Feminist Data Futures Manifesto (July 2023), developed with feminist activists, legal scholars and human rights defenders from across the continent, <https://pollicy.org/projects/afro-feminist-data-futures/>.

First, move from 'sex-disaggregated' to gender-responsive and, where safe and feasible, intersectionally disaggregated data (sex, age, disability, location, income), with an explicit safety test: disaggregation must never proceed where cell sizes or context create a real risk of identifying members of groups at risk.

Second, guarantee the participation of women's rights organisations and feminist movements in the stakeholder processes the draft already mandates (paragraphs 17(a) and 30(b)), and in the National Data Advisory Councils proposed in Appendix C.

Third, name technology-facilitated gender-based violence within the categories of legitimate public interest research for which platform data access must be available under Appendix A(8), so that the African researchers documenting online violence against women – including around elections – can obtain the data that documentation requires.

Recommendation 6. Revise Appendix A(1)(d) to require gender-responsive and, where safe, intersectionally disaggregated data, subject to an explicit safety threshold prohibiting disaggregation that creates a real risk of identifying persons or small groups at risk; and add data revealing sexual orientation or gender identity to the definition of sensitive data requiring heightened protection against disclosure.

Recommendation 7. Guarantee the representation of women's rights organisations and feminist movements in the participatory mechanisms under paragraphs 17(a) and 30(b) and in the National Data Advisory Council under Appendix C; and include technology-facilitated gender-based violence expressly among the fields of legitimate public interest research under Appendix A(8)(c)(iii).

2.4 Children first: from a protection clause to a governance framework

Africa is the world's youngest continent, and in the coming decades sub-Saharan Africa will be home to the majority of the world's children.¹⁴ Any African data instrument is therefore, to a degree unmatched anywhere else, a children's instrument. The draft's single clause on children's data (Appendix A(1)(b)) – alignment with the UN Convention on the Rights of the Child and child-sensitive governance – is welcome but slender for a continent in this demographic position.

Four additions are needed.

First, the African anchor: the clause should cite the African Charter on the Rights and Welfare of the Child and the work of the African Committee of Experts on the Rights and Welfare of the Child alongside the UNCRC, and should incorporate the standards of General Comment No 25 (2021) on children's rights in the digital environment, including

¹⁴UNICEF, The Right Start in Life: Global Levels and Trends in Birth Registration, 2024 Update (December 2024) (150 million children under five unregistered globally; sub-Saharan Africa's registration rate of 51 per cent accounts for roughly 90 million of these; on current trends the region could hold over 100 million unregistered children after 2030), <https://www.unicef.org/press-releases/birth-registration-steadily-increases-worldwide-150-million-children-still-invisible>.

the best-interests principle as a primary consideration in all processing and disclosure decisions affecting children.¹⁵¹⁶

Second, education data: as schooling digitises, learning platforms, school management systems and examination bodies are accumulating rich behavioural records of African childhoods. The Guidelines should require that children's education data be governed by the best-interests principle, prohibit its use for commercial profiling or advertising, and prohibit its disclosure under any public interest override absent a heightened, child-specific test – while preserving access to aggregated education data, which is indispensable for accountability in the delivery of the right to education.

Third, the exclusion problem: roughly 90 million children under five in sub-Saharan Africa are unregistered and 'invisible' to government systems, and on current trends the region could hold over 100 million unregistered children after 2030.¹⁷ The duty to create and maintain data in paragraph 16 should expressly encompass inclusive, safeguarded civil registration and vital statistics, because a child who was never counted cannot benefit from any right the Guidelines confer.

Fourth, the biometric lesson: the Kenyan High Court specifically identified the processing of children's biometric data within a national identity system as implicating high risk;¹⁸ the Guidelines should presumptively exclude children's biometric data from collection and from any access or reuse regime.

Recommendation 8. Expand Appendix A(1)(b) into a fuller children's data provision that: anchors children's data governance in the African Charter on the Rights and Welfare of the Child and General Comment No 25 alongside the UNCRC; makes the best interests of the child a primary consideration in processing and disclosure decisions; prohibits commercial profiling of children and the use of children's education data for advertising; establishes a heightened test before any disclosure of children's data under public interest provisions; and presumptively excludes children's biometric data from collection and reuse. Add a definition of 'child' to the Definitions section.

Recommendation 9. Amend paragraph 16 to state expressly that the duty to create, keep and maintain data includes inclusive and safeguarded civil registration and vital statistics systems, so that data access frameworks do not entrench the invisibility of the unregistered.

2.5 Platform data, artificial intelligence and researcher access: Africa's opportunity to lead

¹⁵African Charter on the Rights and Welfare of the Child (1990); African Committee of Experts on the Rights and Welfare of the Child (ACERWC).

¹⁶UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.

¹⁷See note 12 above.

¹⁸See note 3 above.

Appendix A(8) which mandates robust, secure, non-discriminatory access mechanisms to platform data for public interest research, protecting good-faith scraping of publicly accessible data where no alternative exists, and proposing a continental Code of Conduct negotiated on a pan-African basis is, in AIRA's assessment, the most globally significant part of the draft. Our support is grounded in painful comparative experience. Voluntary access has collapsed: Meta sunset CrowdTangle, the most widely used public-data tool for researchers and journalists, in 2024; X placed its research API behind prohibitive paywalls; and successor tools such as the Meta Content Library have been confined largely to academic researchers, excluding many of the journalists and civil society organisations who do the continent's platform accountability work.¹⁹ Statutory access elsewhere has been territorially fenced: Article 40 of the EU Digital Services Act conditions researcher access on the study of systemic risks 'in the Union', a scoping that offers no entitlement to researchers studying harms to African users in African contexts.²⁰ Africa cannot borrow its way to platform transparency. It must legislate it, and because no single African state has the market weight to compel compliance alone, the draft's insistence on a pan-African approach (general measure 12 and Appendix A(8)(b)) is exactly right.

The stakes of platform opacity on this continent are not abstract. The petition now proceeding before the Kenyan High Court alleges that recommender systems amplified content that contributed to killings during the conflict in northern Ethiopia – litigation made possible only by whistleblower disclosures and investigative journalism because independent researcher access to the relevant data did not exist.²¹

AIRA's own research on algorithmic influence in African elections has repeatedly confronted the same wall.

We accordingly propose tightening Appendix A(8) in five respects: (i) access must be available to vetted civil society researchers and journalists, not only academics; (ii) the scraping safe harbour should be framed as a legal protection enforceable before courts and the oversight body, not merely a platform 'commitment'; (iii) the Code of Conduct should carry compliance timelines and be enforceable through the tiered framework in

¹⁹See Tech Policy Press, 'What Does CrowdTangle's Demise Signal for Data Access Under the DSA?' (March 2024) and 'The Demise of CrowdTangle and What It Means for Independent Technology Research' (June 2024); Platformer, 'How CrowdTangle predicted the future' (March 2024) (documenting Meta's sunset of CrowdTangle, X's imposition of paywalls on its research API, Reddit's API restrictions, and the limitation of successor tools such as the Meta Content Library largely to academic researchers, excluding many journalists and civil society organisations).

²⁰Regulation (EU) 2022/2065 (Digital Services Act), Article 40, which conditions vetted-researcher data access on the study of systemic risks 'in the Union'. See Platformer (n above); Mathias Vermeulen and others in Internet Policy Review, 'Can we fix access to platform data?' (2024).

²¹Abraham Meareg, Fisseha Tekle and Katiba Institute v Meta Platforms Inc, High Court of Kenya, ruling of 3 April 2025 (Mugambi J) (affirming Kenyan jurisdiction over a constitutional petition alleging that Facebook's recommender systems amplified content that contributed to grave harm during the 2020–2022 conflict in northern Ethiopia, in part because content moderation for the region was conducted from Nairobi). The petitioners seek remedial funds of approximately GBP 1.8 billion and algorithmic changes. See Amnesty International, 'Kenya: Meta can be sued in Kenya for role in Ethiopia conflict' (April 2025); The Bureau of Investigative Journalism (April 2025)

paragraphs 23 to 27; (iv) 'legitimate public interest research' should expressly include research on harms to users in Africa, technology-facilitated gender-based violence, children's online safety, and electoral integrity, with expedited access procedures during electoral periods; and (v) the regime should be developed in explicit coordination with the forthcoming Resolution 630 guidelines to avoid fragmentation.²²

On artificial intelligence, the draft's Section on Access, Ethics and AI rightly ties AI accountability to data access: human rights impact assessments, bias reporting and public access to both. Two additions would future-proof it.

First, training data transparency: those deploying AI systems in public service delivery, and providers whose systems materially affect rights in Africa, should be required to disclose meaningful information about the provenance, composition and African representativeness of training datasets – a matter of acute concern given the underrepresentation of African languages and contexts in frontier systems.²³

Second, benefit-sharing: as global firms move to build datasets and voice models across dozens of African languages,²⁴ and as community efforts such as Masakhane build African language technologies from the ground up,²⁵ the Guidelines should provide that access to and reuse of community and linguistic data respects the collective rights of the communities concerned – operationalising the draft's own community 'data subject' definition and its citation of the CARE principles – including through consent, attribution and equitable benefit-sharing arrangements. Without this, 'open data' risks becoming a one-way extraction pipeline, a dynamic African scholars have described as algorithmic and data colonialism.^{26,27}

Recommendation 10. Strengthen Appendix A(8) so that: access mechanisms are open to vetted civil society researchers and journalists as well as academics; the protection

²² ACHPR, Resolution on Developing Guidelines to Assist States Monitor Technology Companies in Respect of Their Duty to Maintain Information Integrity Through Independent Fact Checking, ACHPR/Res.630 (LXXXII) 2025; and Resolution on Working Towards the Assessment of Public Interest Content in this Digital Era, ACHPR/Res.631 (LXXXII) 2025.

²³ Institute for Security Studies (African Futures), 'Data centre investments are a gamble for Africa' (December 2025) (estimating that Africa requires roughly 700 additional data centres for a digitally inclusive future, against a current stock concentrated in Kenya, Nigeria and South Africa; linking weak domestic data systems to the underrepresentation of African languages in frontier AI), <https://futures.issafrica.org/blog/2025/Data-centre-investments-are-a-gamble-for-Africa>.

²⁴ Data Centre Magazine, 'What is Google's Strategy for AI Data Centres in Africa?' (September 2025) (reporting plans for datasets and voice models spanning over 50 African languages by 2026, supported by 24 open speech datasets).

²⁵ TechCabal Insights, 'Africa's AI sovereignty problem is really an energy problem' (May 2026) (describing the Masakhane community's open-source natural language processing work for African languages, framed explicitly against 'algorithmic colonisation'; and observing that Kenya's 2026 Artificial Intelligence Bill largely reproduces the EU AI Act's framework), <https://insights.techcabal.com/africas-ai-sovereignty-problem-is-really-an-energy-problem/>.

²⁶ Abeba Birhane, 'Algorithmic Colonization of Africa' (2020) 17:2 SCRIPT-ed 389.

²⁷ Nick Couldry and Ulises A Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20(4) Television & New Media 336.

for good-faith scraping of publicly accessible data for public interest purposes is a legally enforceable safe harbour; the continental Code of Conduct is subject to compliance timelines and enforceable through the tiered enforcement framework; legitimate public interest research expressly includes harms to users in Africa, technology-facilitated gender-based violence, children's online safety and electoral integrity, with expedited procedures during electoral periods; and the regime is developed in coordination with the guidelines under Resolution 630.

Recommendation 11. Add to the Access, Ethics and AI section: (a) a duty to disclose meaningful information about the provenance, composition and African representativeness of datasets used to train AI systems deployed in public service delivery or materially affecting rights in Africa; and (b) a provision that access to and reuse of community and linguistic data shall respect the collective rights of the communities concerned, including consent, attribution and equitable benefit-sharing, consistent with the Guidelines' community-inclusive definition of data subject and the CARE principles.

Recommendation 12. Preserve and reinforce the accountability proviso in exemption 21(e)(ii) and the public-interest proviso in 21(e)(iv), and add that where algorithms, models or trade secrets are legitimately withheld from public disclosure, they must nonetheless be examinable by the oversight body, courts and vetted researchers within secure processing environments or in camera, so that intellectual property can never operate as a complete accountability shield.

2.6 Context, capacity and the limits of transplantation

Parts of the draft's vocabulary such as high-value datasets, data intermediaries, secure processing environments, marginal-cost charging, descend recognisably from European open data and data governance legislation. AIRA does not object to learning from elsewhere; we object to copying without adaptation, a pattern already visible in African AI lawmaking, where national bills have been observed to reproduce the EU AI Act's framework largely wholesale.²⁸ African scholars have warned that importing technological and regulatory frameworks built on other regions' assumptions, without local grounding, reproduces dependency rather than remedying it.²⁹ The Guidelines' own commitment to reflecting 'the diversity of African experiences' should be carried through into implementation design.

Concretely, this means four things.

First, financing: the Guidelines assign heavy new mandates to Information Commissions, statistical offices and courts. The continental evidence is that oversight bodies without protected funding cannot act independently.³⁰ The Guidelines should require legally

²⁸See note 23 above.

²⁹See note 24 above.

³⁰Code for Africa, 'Africa's data protection laws began to bite in 2025' (May 2026) (44 AU member states with data protection laws by end-2025; 38 operational data protection authorities; noting that regulators dependent

protected budget lines for oversight bodies, and the Commission should champion an AU-level technical assistance and peer-learning facility for implementation.

Second, statistical integrity: the enhanced stewardship role given to National Statistical Offices in Appendix C is sensible, but an NSO placed at the centre of a National Integrated Data Management Framework must be insulated from political direction; the Guidelines should incorporate the UN Fundamental Principles of Official Statistics, including professional independence and impartiality, as conditions of that role.³¹

Third, sequencing: states start from radically different baselines; the Guidelines should invite differentiated, published implementation roadmaps rather than implying uniform immediate compliance, while holding the normative bar constant.

Fourth, infrastructure realism: general measure 9's preference for storing open government data in national or regional data centres serves sovereignty, but strict physical localisation carries costs for energy, water, resilience and, in some political contexts, easier state seizure. Africa's data centre stock remains small and concentrated in a handful of markets, and large AI-grade facilities impose heavy electricity and water demands on already strained systems.³²³³ We recommend framing measure 9 around African legal and operational control and jurisdictional accountability, with regional (not only national) options, rather than rigid physical localisation, and pairing it with the draft's own environmental transparency provisions.

Recommendation 13. Require, in Appendix C, that the independence guarantees of the oversight body include a legally protected budget line insulated from the ministries it supervises; and recommend the establishment of an AU-level implementation support and peer-learning facility for these Guidelines.

Recommendation 14. Condition the National Statistical Office's data stewardship role in Appendix C on compliance with the UN Fundamental Principles of Official Statistics, including professional independence, impartiality and statistical confidentiality.

Recommendation 15. Reframe general measure 9 in terms of African legal and operational control over open government data, with national or regional hosting options and jurisdictional accountability, rather than strict physical localisation; and link it expressly to the environmental disclosure obligations in general measure 10 and Appendix A.

on donor grants or on budgets controlled by supervised ministries struggle to pursue politically sensitive enforcement),

<https://medium.com/code-for-africa/africas-data-protection-laws-began-to-bite-in-2025-322285625315>.

³¹United Nations Fundamental Principles of Official Statistics, endorsed by the UN General Assembly in Resolution 68/261 (2014).

³²See note 6 above.

³³See, eg, 'AI boom drives new wave of energy and data centre investment in Africa', Sunday World (May 2026) (reporting expert estimates that a single frontier-scale AI facility could consume electricity on the order of a large share of a major African city's supply, alongside millions of litres of water daily).

Part III: Consolidated Recommendations

For ease of reference, AIRA's twenty-four recommendations are grouped below; full text appears at the indicated points in Parts II and III.

- **Preventing inversion and protecting persons at risk:** Recommendations 1-3 (judicial pre-authorisation and transparency for state access to privately held data; replacement of the 'absolute disclosure' formulation in paragraph 14(g); a 'do no harm' principle).
- **Connectivity and inclusion:** Recommendations 4-5 (express treatment of internet shutdowns as violations of Article 9; language, offline and community-mediated access channels).
- **Gender and intersectional data justice:** Recommendations 6-7 (gender-responsive and safely disaggregated data; sensitive-data protection for sexual orientation and gender identity; guaranteed participation of women's movements; TFGBV research access).
- **Children's data governance:** Recommendations 8-9 (a full children's data framework anchored in the ACRWC and General Comment 25; inclusive civil registration within the duty to create data).
- **Platforms, AI and researcher access:** Recommendations 10-12 (a strengthened, enforceable Appendix A(8) open to civil society and journalists; training data transparency and community benefit-sharing; secure examinability of withheld algorithms and trade secrets).
- **Institutions, capacity and context:** Recommendations 13-15 (protected funding for oversight bodies and an AU implementation facility; UN Fundamental Principles safeguards for statistical offices; a control-based rather than strictly localisation-based reading of measure 9).
- **Text-specific strengthening:** Recommendations 16-24 (preambular additions; definitions of 'child' and dynamic anonymisation; Malabo ratification; interim enforcement powers; AI procurement conditions; a three-year review cycle with ACERWC coordination; data-centre metrics and the voluntary/mandatory relationship; Africanised high-value dataset categories; and a technical edit of the final text).

Conclusion

The Special Rapporteur's foreword states that the right to access data 'is not a luxury to be deferred'. AIRA agrees. The past three years have shown that access regimes designed elsewhere will not, of their own force, reach African researchers, African journalists, African women, or African children, and that when voluntary access becomes inconvenient, it is withdrawn. Africa's answer must be its own: anchored in the Charter, alert to the ways data power is abused by states and corporations alike, designed for the

institutions and languages and connectivity realities of this continent, and ambitious enough to lead where others have hesitated. The draft Guidelines are that answer in the making. With the strengthening proposed here, they can stand alongside the Declaration of Principles as one of the defining African human rights instruments of the digital age.

AIRA remains at the disposal of the Special Rapporteur and the Commission for validation processes, technical drafting support, and implementation partnership across our members' countries of operation.

Submitted on behalf of the African Internet Rights Alliance

Amnesty International Kenya

ARTICLE 19 Eastern Africa

BudgIT

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University

Co-Creation Hub/iHUB

KICTANet

Legal Resources Centre

Paradigm Initiative

Pollicy

Contact:

Coordinator, African Internet Rights Alliance - coordinator@aira.africa