**Report on the public responses to shaping access to data.**

**For input into the ACHPR Resolution 620 guidelines**

African Alliance for Access to Data

Author: Taryn De Vega

26 September 2025

---

## Overview of the report

The African Commission on Human and Peoples' Rights (ACHPR) are developing resolutions on access to data in Africa. The African Special Rapporteur on the Freedom of Expression and Access to Information, Commissioner Ourveena Geereesha Topsy-Sonoo, with the assistance African Alliance for Access to Data (AAAD), conducted numerous public consultations on the drafting and implementation of the ACHPR Resolution 620. The consultations supported digital participation through an online questionnaire ACHPR Resolution 620, which received responses analysed for discussion in this report.

The African Alliance for Access to Data (AAAD) received 227 responses from participants interested in shaping the Access to Data guidelines. The largest number of responses was received from participants in the technology/ICT and civil society sectors, with further responses received from academia, health, governmental agencies, the media, research organisations, and non-governmental organisations. Most of the submissions were in English, with 3 submissions in French (these 3 were not included in the analysis). The survey included a section on demographic data (in future, this could include a section on location). The survey asked participants to respond to 7 questions around data, policies and infrastructure in Africa. The segment below details the answers to the 7 questions and a brief description of how these relate to the current draft of the guidelines

## The public responses and their alignment with the existing policy draft

The current draft of the policy (Version 2) has captured many of the core issues related to data access and governance in Africa. The public comments have mentioned many of the guidelines covered in the existing draft. The comments also point to potential considerations and gaps in the current formulation. A few considerations which could bridge the gaps in the current draft relate to:

1. The transparency of data handling, use and accountability
1.1 Transparency of how states access, store, share and use data should be prioritised.
1.2 Capacity for data handling should be built into the local information ecosystem.
1.3 Data shared should be handled with integrity and stored in a manner that promotes data security, user confidentiality, and protects personal data from leaks, hacks or misuse.
1.4 Data should be harnessed with informed consent, with the right to opt out of data sharing.

1.5 Guidelines should offer clarity on the protections and liabilities of public/private bodies around data security and the misuse of data by third parties. Guidelines should explain the liabilities and protections for data misuse, misinterpretation and disinformation by third-party data users.

2. Policy and legal frameworks should prescribe systems and technical expectations:
2.1 Mandate impact assessments for large data systems. Impact assessments should be mandated before the introduction of major public or private sector data projects (e.g., digital ID systems, health surveillance), to evaluate risks to privacy, equity, and inclusion. These assessments should be publicly available when they relate to the environment or health issues.
2.2 The use of blockchain technology to trace transactions, secure electoral data, and ensure accountability and transparency on how data is shared. By leveraging this technology to ensure verifiable provenance and digital traceability.

3. Incentivising the participation of public bodies and private bodies
3.1 For public bodies, this can include having participation and compliance as a performance metric in the evaluation of public body performance.
3.2 For private bodies, public recognition for contributors could take the form of citations in research projects, public certificates, and other visible forms of recognition.

4. Infrastructural and environmental considerations should
4.1 Promote African cloud and data hosting services. Continental hosting services would localise sensitive data and support data sovereignty. These centres should prioritise data for the public good.
4.2 Respond to Africa's digital disparity, prioritise investment in rural digital infrastructure for data generation, access, and cloud storage.

5. Interventions for data literacy
5.1 Literacy campaigns should be accompanied by a toolkit to equip stakeholders with the skills to transform data into readable and explainable formats. Sector-specific toolkits to guide practitioners on how to use data effectively should be developed for health, agriculture, education, etc.

6. Regional prescriptions
6.1 Establish clear legal frameworks for regional data sharing, regional data flows, and address cross-border data transfers.
6.2 Data sovereignty and African data ownership should be considered.

7. Protections
7.1 Protect actors who use data to expose abuse and rights violations. For example, naming specific protections for whistleblowers.

The additional responses speak to the current draft of the policy. Some responses echo and validate the statements made, whilst others offer new or nuanced perspectives on the policy for consideration. The questions and responses follow below.

**Question 1: What core principles should inform Guidelines for states on data collection, deployment and access in Africa?**

The responses suggested the following principles: a) data as a public good, b) centralising a human rights approach, c) protecting marginalised groups, d) consent, e) data sovereignty, f) ethics, g) transparency and accountability for data handling and use, h) capacity building of local ecosystems, and i) promote user confidentiality and highlight the liabilities of public/private bodies around data security and the misuse of data by third parties.

a) Responses value data as a public good and call for proactive disclosure and access.

b) Responses value a human rights-centred approach, upholding commitments to privacy, dignity, freedom of expression, information access and other rights espoused globally. The human rights approach should be complemented by relevant national constitutions and international legal frameworks on human rights. "Data practices must comply with the African Charter on Human and Peoples' Rights and other international human rights standards" (Respondent).

c) The Guidelines should allow access to data for all. It should safeguard marginalised groups and rural communities from being exploited or discriminated against.

d) Data should be harnessed with informed consent, with the right to opt out of data sharing. "Individuals must have control over their data, with informed consent as a non-negotiable standard" (Respondent). Data collection procedures should be clearly defined to allow users to make informed choices. Minimum versus maximum data sharing possibilities should be evident.

e) Data sovereignty and African data ownership should be considered. "African states and communities should own and control their data, avoiding extractive practices by external actors" (Respondent). This need for sovereignty should be balanced with calls for fair use and national interest claims, allowing these to be used legitimately and not for manipulative purposes.

f) Responses call for ethical standards to be embedded in the Guidelines. These should promote fair use of data and prevent algorithmic bias, manipulation, and harm.

g) Transparency on how states access, store, share and use data is valued. Audits and oversight bodies should be put in place to monitor access. Accountability measures should be included to prevent abuse of data and the power it can hold.

h) The capacity for data handling should be built into the local information ecosystem, developing strong processes and data systems.

i) Data shared should be handled with integrity and stored in a manner that promotes data security and user confidentiality; it should "protect personal data from leaks, hacks or misuse" (Respondent). Guidelines should address the liabilities and protections for public and private bodies after data sharing. "There must be provision of liability protection for organizations that share data in good faith and in compliance with data protection laws to reduce fear of legal exposure" (Respondent). Guidelines should clarify issues of data misuse, misinterpretation, and disinformation by third-party data users.

**Question 2: What concrete points about new or existing policy and legal frameworks should go into Guidelines for African states for the collection, deployment and access to data?**

The responses raise various points for consideration related to African states, including the need for: a) laws around disclosure and consent, b) developing of independent authorities for data monitoring, c) harmonisation of regional law, d) cross broader data sharing, e) training systems, f) minimising harm around automated decision making, g) protection for whistle-blowers, h) mandatory impact assessments on data systems, and the use of i) blockchain technology.

a) Responses call for open data to be prescribed as a principle in national law. The law should mandate public disclosure by public bodies, align with data rights, and allow individuals to consent to include their data or remove their data at will.

b) Responses suggest the creation of independent national authorities for data monitoring, protection and oversight.

c) Guidelines should align with national data protection laws and existing laws, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

d) Guidelines should establish clear legal frameworks for data sharing. It should allow for regional data sharing, regional data flows, and address cross-border data transfers. It is important to "establish shared rules for secure and lawful cross-border data flows, which are essential for regional integration, digital trade, and Africa's collective digital sovereignty" (Respondent).

e) States should have access to systems and the necessary training to promote ethical data storage, use and processing.

f) Guidelines should highlight the concerns related to data use for automated decision-making, to ensure minimal harm by algorithms and Artificial Intelligence. It should include "strong protections against misuse of data through surveillance, AI or other emerging technologies" (Respondent).

g) Respondents call for the Guidelines to protect actors who use data to expose abuse and rights violations, naming specific protections for "whistleblowers, journalists, and civil society actors" (Respondent).

h) Others highlight the importance of mandatory impact assessments for large data systems. Requests include that assessments be mandated "before major public or private sector data projects (e.g., digital ID systems, health surveillance), to evaluate risks to privacy, equity, and inclusion" (Respondent). Assessments should be publicly available, as they affect health and environmental issues.

i) Blockchain technology could be useful to trace transactions, secure electoral data, and ensure accountability and transparency on how data is shared. This would support "leveraging technologies such as blockchain to ensure verifiable provenance and digital traceability" (Respondent).

**Question 3: What concrete points about incentivising data sharing should go into the Guidelines?**

Responses note the value of incentivising participation and suggest that incentives could be in the form of a) financial incentives, b) funding opportunities, and c) recognition for compliance. The recommendations also highlight considerations around d) protections and partnerships, and the responsibilities of e) publicly funded beneficiaries.

a) Financial incentives could be awarded to private bodies that participate freely. This could extend to tax breaks, tax incentives, subsidies, and innovation grants. "Offer innovation challenges, incubator support, or preferential procurement for startups and SMEs that use shared data to solve public problems" (Respondent).

b) Funding subsidies could be made available for public bodies to upgrade their data systems and enhance their capacity for data handling and storage. Opportunities could support "funding and training to civil servants and local governments to improve data literacy and management" (Respondent).

c) Public recognition for contributors and organisations which comply should be awarded. Systems to award those who contribute should be put in place. Rewards can be in the form of citations in research projects, public certificates, and other visible forms of recognition. Recognition for public bodies should also be included as a performance metric in the evaluation of public body performance.

d) Data sharing should be protected, and the potential for partnerships with other bodies around data sharing should be encouraged through clear frameworks for data ownership, data sharing and acceptable use.

e) Private companies which benefit from public funding should be mandated to make their data publicly available.

**Question 4: What concrete points about infrastructural and environmental data concerns should be in the Guidelines?**

The responses on how the Guidelines should reflect infrastructural and environmental concerns, foreground issues of a) ethics, b) digital rights and the ethical use of geospatial data, c) environmental data and geospatial systems, d) standards and formats for data e) indigenous communities, f) compliance for corporations that affect environmental health, and considerations for g) sustainable practices for infrastructure development and waste disposal, h) African cloud hosting services, and i) digital disparity,

a) Infrastructure should be ethically procured and used.

b) Ensure the ethical use of geospatial data in line with digital and privacy rights. These should "ensure that environmental and geolocation data collected does not violate individual or community rights, especially when linked to land, resources, or cultural heritage".

c) Environmental data, including water levels, air quality and climate disasters, should be made publicly available. These should be integrated with Geospatial Information Systems.

d) Include recommendations for infrastructure capabilities, standardised formats, cybersecurity considerations, and support data interoperability across departments and agencies.

e) Recognise and integrate data from local communities and Indigenous peoples in environmental monitoring and policy-making processes.

f) Environmental data should be mandated from companies whose efforts directly impact the land and environment, by making it a requirement for "construction, mining, oil and gas, and agro-industrial companies to submit and publish environmental and infrastructural data as part of their licensing and compliance obligations" (Respondent).

g) Promote sustainability and energy-efficient infrastructure, drawing on renewable sources of energy. "Encourage environmentally sustainable practices in the development and operation of data infrastructure (e.g., renewable-powered data centres)" (Respondent). These should also prioritise a sustainable system for the recycling and disposal of technological waste.

h) African cloud and data hosting services should be promoted. This approach of continental hosting services would localise sensitive data and support data sovereignty. These centres should prioritise the public good.

i) Respond to Africa's digital disparity. Guidelines should "prioritise investment in rural digital infrastructure for data generation and accessibility" (Respondent). These should recognise inequitable digital infrastructure in rural and urban spaces and suggest investment in digital infrastructure for data centres, cloud storage and other systems.

**Question 5: What concrete measures should the Guidelines present that can enhance the demand side of data, including data literacy, so that the range of stakeholders can meaningfully utilise data that becomes available?**

Many concrete measures have been highlighted, including the need for a) literacy and b) education, c) capacity building, d) training initiatives for marginalised communities, and e) sector-specific training initiatives. The responses also value user support through f) user-friendly data portals, and accompanying g) toolkits.

a) Guidelines should promote data literacy and education. National literacy campaigns should address the varying needs of citizens, policymakers, governments and relevant stakeholders. Campaigns should "run outreach to show how data can solve real problems, improve services, and support decision-making, encouraging more people and organizations to seek out and use data" (Respondents).

b) Literacy should be embedded into the school curriculum at primary, secondary and tertiary levels. This can include information on digital rights to support a data-informed generation, so "that future generations understand how to interpret, question, and use data" (Respondent). At higher education institutions, this curriculum should be tailored to various disciplines, for example, through "support for data journalism and storytelling: partner with media and journalism schools to strengthen data storytelling techniques that make public data more relatable and actionable".

c) Guidelines should promote capacity building through training programmes offered for those who will work with, maintain, store and process data, as well as those who could use data for evidence-based planning. This training is necessary for public bodies, as "governments must actively promote a data-driven culture across public administration" (Respondent).

d) Training through community data labs can also be extended to the general population, with a special focus on underserved communities. "These efforts should prioritize inclusive access delivered in multiple languages, in low-bandwidth settings, and geared toward women, youth, and underserved groups to ensure no one is left behind" (Respondent).

e) Training should be made available to relevant sectors to support decision-making through the provision of "sector-specific tools for key economic areas (e.g., agriculture, health, finance)" (Respondent).

f) Online platforms should be easily accessible and inclusive. Data portals should be functional and allow easy possibilities to visualise data in multiple languages. "Design with users in mind – dashboards and websites should be simple, visual, and available in local languages" (Respondent). Platforms should "provide real-time public dashboards showing status of FOI requests and departmental compliance rates".

g) Implementation guidelines could be accompanied by a toolkit to equip stakeholders with the skills to transform data into readable and explainable formats. "Encourage Sector-Specific Data Use Toolkits for health, agriculture, education, etc., to guide practitioners on how to use relevant data effectively" (Respondent).

**Question 6: What specialised sectoral measures should the Guidelines propose for different aspects of African states: eg, Parliamentarians, Data protection authorities, Access to information bodies, Election Management Bodies, national science councils, judicial services, health authorities, etc.?**

The respondents made multiple and lengthy inputs on sector-specific guidelines, calling for a) adaptable policy frameworks, b) well-resourced oversight committees, c) proactive disclosure, and d) data-informed legislative decision-making. Further responses note the value of e) data for evidence-based research, and f) sector-specific guidelines for various areas, including the media and civil society.

a) Policy frameworks should support regular review and updating of data governance guidelines and policies. Noting the need to be responsive to the changing digital ecosystem, and to "pass and review progressive data laws (privacy, access, AI, open data)" (Respondent).

b) Ensure oversight committees and data/information commissions are sufficiently resourced with the technical, financial and legal expertise and powers to enforce compliance

c) Public bodies should publish high-value data sets proactively.

d) Mandate the use of national data in impact assessments before passing significant legislation, especially in sectors like health, education, environment, and digital rights. This should "mandate data-driven legislation" (Respondent).

e) Promote the use of data to combat misinformation and enhance evidence-based research.

f) Develop sector-specific data protocols and considerations for civil society, media, national statistics agencies, health authorities, judicial services, science councils, election management bodies, access to information commissions, data protection authorities and parliamentarians. Multiple recommendations have been made, including the considerations for the media and civil society sectors. Recommendations include partnering with fact-checking coalitions for verification, by having "coalitions: partner with EMBs/DPAs to verify public data" (Respondent), and encouraging civil society organisations to monitor public data sets for accountability, and to "fund tools to analyse government/corporate data for accountability" (Respondent).

**Question 7: Do you have any additional input regarding Resolution 620?**

Responses include the need for a) human rights data governance frameworks, b) recognition of the unequal global data economy, the inclusion of c) implementation roadmaps and d) continental compliance monitoring. Responses call for e) special guidelines for women and children, and f) a multi-stakeholder consultation approach.

a) Resolutions should be grounded in a human rights-based data governance framework. With multiple responses calling for "a human rights-based approach to data governance" (Respondent). Guidelines should foreground digital inclusion and digital rights.

b) Guidelines should recognise the unequal global data economy and safeguard against international extractive practices.

c) Implementation roadmaps should be included with timelines and recommendations for compliance. Implementation plans should include youth, women and grassroots organisations. Responses request that "the Resolution explicitly promote youth inclusion in data governance" (Response).

d) Guidelines should be followed by a continental monitoring mechanism to evaluate nation-states' onboarding and compliance. Noting "it must be followed by a binding instrument or a continental monitoring mechanism to ensure its implementation". (Respondent).

e) Guidelines should include the safety provisions for women and children in the law and cybersecurity plans. Explicating that "protection from online gender-based violence must be treated as a national security" (Respondent).

f) The role of digital platforms and their obligations should form part of the Guidelines. It should prescribe platform accountability for data practices and content moderation policies. "Guidelines for African states should include regulatory obligations for social media platforms and telecom providers to prevent, respond to, and report digital violence. This includes fast-tracking content takedown processes, flagging abusive behavior, and improving transparency in algorithmic moderation" (Respondent).

g) The Guidelines must be the outcome of a multi-stakeholder process, promoting collaboration of all stakeholders.