

**ACHPR/Res.620 (LXXXI) 2024**

**GUIDELINES**

**ON PROMOTING AND HARNESSING DATA ACCESS AS A TOOL FOR ADVANCING  
HUMAN RIGHTS  
AND SUSTAINABLE DEVELOPMENT IN THE DIGITAL AGE.**

**DRAFT v.4**

3 February 2026

## Table of Contents

<b>Table of Contents</b>	2
<b>Section A: Preamble</b>	2
<b>Section B: Background</b>	4
<b>Section D: Key Principles</b>	5
<b>Section D: Definitions</b>	6
<b>Section F: Measures</b>	10
F1: General Measures	10
F2: Legal, Policy and Programmatic Measures	11
F3: Measures for Specific Data	13
F4: Institutional Measures for Public Bodies	18
F5: Institutional Architecture	19
F6: Exemptions and Safeguards	21
F7: Enforcement	22
F8: Ethical Data Governance and AI	23
<b>Section G: Implementation</b>	25
<b>Appendix A: Acknowledgements</b>	26
<b>Appendix B: Drafting Process</b>	26

## Section A: Preamble

The African Commission on Human and Peoples' Rights (the African Commission) meeting at its [...] Ordinary Session, held [...]: *[Text to be added once the ACHPR considers final adoption of its approved version of the Guidelines]*

**Affirming** the Commission's mandate of promotion and protection of human and peoples' rights pursuant to Article 45 of the African Charter on Human and Peoples' Rights (the African Charter);

**Recalling** Article 9 of the African Charter, which guarantees every individual the right of access to information;

**Recognising** Articles 19 and 21 of the Universal Declaration of Human Rights and Article 19 and 25 of the International Covenant on Civil and Political Rights, which guarantee the right of access to information and the right to participate in genuine periodic elections that are free, fair and credible, by equal and universal suffrage respectively;

**Recalling** Resolution 620, "Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age" adopted by the African Commission on Human and Peoples' Rights (ACHPR) during its 81st Ordinary Session in October–November 2024 in Banjul, The Gambia.

**Recalling** the ACHPR's Model Law on Access to Information for Africa, the Guidelines on Access to Information and Elections in Africa, and the Declaration of Principles on Freedom of Expression and Access to Information in Africa;

**Recognising** the African Union Convention on Cyber Security and Personal Data Protection and the African Union Data Policy Framework;

**Reaffirming** that access to data for a public good can foster human rights, innovation, encourage collaboration, and empower the public to engage actively in democratic governance and decision-making, as well as support progress towards achieving the right to development and the Sustainable Development Goals;

**Concerned** that there is no tailored guidance for African governments on promoting and harnessing data access as a tool for advancing human rights and sustainable development;

**Recognising** the obligations, and guiding law and principles, contained in the legal instruments, general comments, guidelines, principles, declarations, resolutions and other normative documents of the African Commission on the protection and promotion of human and people' rights, and the need to consider their application in promoting and harnessing data access;

**Recognising** that the rights enshrined in the African Charter are indivisible, interdependent and interrelated and apply in all times, and reiterating the need for measures to recognise human and peoples' rights as mutually reinforcing;

Hereby adopts the following Guidelines on adhering to human and peoples' rights standards under the African Charter as an instrument for promoting and harnessing data access as a tool for advancing human rights and sustainable development in the digital age.

## Section B: Background

1. The ACHPR in its Resolution from the 81st Ordinary Session in October–November 2024 in Banjul, The Gambia, established a clear mandate for its Member States to advance data access as a key part of data governance. The Resolution, ACHPR/Res.620 (LXXXI) 2024, is titled Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age (Resolution 620).
2. Resolution 620 emerged from growing recognition of data’s potential in Africa’s digital transformation. It was inspired in part by the UNESCO global conference commemorating the International Day for Universal Access to Information held in Accra in October 2024, which emphasised data’s indispensable role in facilitating access to information, and contributing to the Sustainable Development Goals and Africa’s Agenda 2063.
3. The Resolution recognises that equitable access to data (encompassing statistics, datasets, and research findings) is fundamental for creating just, informed, and inclusive African societies in the digital era.
4. It urges States Parties to ensure that data collection, processing, storage and access practices are transparent, accountable and in line with regional and international standards in this era of digitalisation and increasing use of AI; and to ensure that data held by public institutions and bodies receiving public funds, as well as that held by private actors where there is an overriding public interest in access, should be made publicly available by default, in alignment with the principle of maximum disclosure, except where justified by regional and international human rights standards;
5. Acknowledged in the Resolution are risks of data misuse, privacy violations, discrimination, and unequal access that can exacerbate existing inequalities. It emphasises the need for ethical data collection and usage principles aligned with international human rights standards, while addressing biases in automated decision-making processes.
6. In terms of the Resolution, the Special Rapporteur on Freedom of Expression and Access to Information in Africa is mandated to consult broadly around the continent to examine and develop appropriate normative standards to guide data collection, deployment and access issues concerning data, and to support efforts that promote and protect access to data across Africa.
7. As the selected normative instrument, the Guidelines presented here are grounded in human rights primacy, ensuring that all data collection, access, and use must serve to advance, not undermine, the dignity and rights of individuals and communities
8. Building upon foundational ACHPR instruments, including the *Model Law on Access to Information for Africa* and the *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, these Guidelines establish a human rights-based framework for data access that builds upon, but goes beyond, traditional access to information.
9. The Guidelines prioritise uplifting marginalized communities, including women, persons with disabilities, rural populations, and children - through access to data that is inclusive, affordable, and available in multiple languages and through strategies, policies and regulation with regional and international human rights standards in the digital era.
10. Acknowledging the critical role of data in public interest research, the Guidelines recognise the need to access platform-held data for public interest research and to mandate digital platforms to actively develop and provide robust, secure, auditable, and non-discriminatory alternative access mechanisms for researchers and other stakeholders seeking non-publicly accessible data or more structured access to public data.

## Section D: Key Principles

These Guidelines embody norms and principles that are informed directly by Resolution 620:

11. **Data for Public Value:** Data is a strategic public asset with the transformative potential to promote democracy, good governance, and contribute to the Sustainable Development Goals (SDGs) and Agenda 2063: The Africa We Want. Data should therefore serve to support policies, services, or interventions that improve societal well-being, transparency, and accountability. This public value perspective informed the process involving the African Union and several African invited states, within the 2025 G20 hosted by South Africa, which culminated in [Guidelines for access to data for researchers and start-ups, through data sharing with and by the public and private sectors](#).
12. **Maximum Disclosure:** The principle of maximum disclosure should be the default for all public data and for relevant private data. Disclosure by default should be presumed, unless demonstrably harmful. Restrictions on access must be a narrow exception, such as for legitimate purposes like privacy, confidentiality and national security, with each concrete case being strictly justified by international human rights standards of necessity, proportionality and legality.
13. **Data Justice and Equity:** Data initiatives must be designed to address structural inequalities and ensure that marginalised and vulnerable communities have equitable access to data, the governance of data including participatory governance and community data ownership, and the benefits derived from its use. This implies a duty for States to provide targeted support and capacity-building measures to enable meaningful societal engagement with, and benefit from, data-driven initiatives. These initiatives should address power asymmetries, historical inequalities, gender equity, and Global South data extraction concerns.
14. **Transparency, Accountability, and Ethical Use:** Data collection, processing, and use must be transparent and accountable. Ethical principles must be embedded in all data initiatives, with clear mechanisms to address biases in data and automated decision-making. All entities handling data are accountable for responsible management, transparent decision-making, and mechanisms for redress.
15. **Data for Public Accountability:** Data is an indispensable tool for public accountability. To this end, governments and private entities must ensure that data is accessible to researchers, civil society watchdogs, and journalists for the purpose of investigating matters of public interest, holding power to account, and fostering a well-informed public discourse.
16. **Data Access by Design:** Systems for data collection, storage and dissemination must be built with proactive disclosure features, accessibility standards and interoperability by default, as well as security provisions.

## Section D: Definitions

### Information:

**Information** means any original or copy of documentary material irrespective of its physical characteristics, such as records, correspondence, memoranda, statistics, books, drawings, plans, maps, diagrams, photographs, audio or visual records, and any other tangible or intangible material, regardless of the form or medium in which it is held, in the possession or under the control of the information holder.

### Data categories:

**Data** designates signals and records in any form, collected, stored, processed, or shared in structured, or unstructured formats, including text, images, sound, video and sensor pulses. It incorporates personal data (relating to an identified or identifiable individual) and non-personal data (such as environmental or statistical data). AI model parameters, weights and algorithms may all be considered as data. Much "raw" data can be processed to produce meaningful results, including becoming a higher-level information resource. Information itself may be treated as data for further knowledge conversion operations.

**Dataset** means a collection of data typically organised in tables, arrays or specific formats, such as CSV or JSON for easy retrieval and analysis. Datasets are essential for data analysis, machine learning, Artificial Intelligence (AI) and other applications that require reliable, accessible data. With newer data analysis tools, such as generative AI, datasets can also be constituted from unstructured data, expanding ways in which this resource can be organised and utilised.

**Personal data** means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, including through identifiers such as name, identification number, location data, or online identifier or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

**Sensitive data** refers to personal data revealing racial or ethnic origin, political opinions, religious beliefs, health information, biometric or genetic data, or other information that requires heightened protection.

**Anonymisation** covers the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, as well as rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable.

**Pseudonymisation** means the processing of personal data in such a manner that this data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

**Dynamic data** means signals in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data.

**Research data** means records in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results.

**High-value datasets** mean records the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and where there is a significant number of potential beneficiaries.

**Metadata** is a subset of data that refers to secondary structural or descriptive information about a body of primary data. Metadata can include personal data.

### Data actors:

**Data ecosystem** means the integration of and interaction between different relevant stakeholders including data holders, data producers, data intermediaries and data subjects, who are involved in, or affected by, related data access and sharing arrangements, according to different roles, responsibilities and rights, technologies, and business models.

**Data processing** means any operation performed on data, including collection, recording, storage, modification, retrieval, use, disclosure, or deletion.

**Data subject** means an identifiable natural person or identifiable group to whom data relates, including communities under customary or national law, and whose data is processed, usually requiring their active consent. Such data is a very specific subset within wider data processing and datasets.

**Data holders** means entities or individuals who, according to applicable rules, have the authority to allow data sharing and data access and can be data controllers under data protection laws, with accountability for data processing operations and data intermediaries.

**Data controllers** refers to the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of data.

**Data intermediaries** means entities appointed in data access and sharing arrangements to facilitate data access and/or data sharing between data holders and data processors.

**Data access** refers to the right and ability to obtain and use data from public and private data holders, and is enabled by availability and usability of such data. Access thus entails retrieval and/or processing, in the context of institutional, regulatory, policy, legal, and contractual frameworks. This may be achieved either through the download of data sets or the processing of data online where only conclusions are downloadable.

**Data sharing** is a form of data access that involves transfer of data for use by others, subject to applicable technical, financial, legal, or organisational use requirements. Sharing may be done directly or through an intermediary, and may take place under diverse licence conditions.

**Open Data** refers to data that is made available in a machine-readable format, free of charge, and under an open license that permits unrestricted use, reuse, and redistribution

**Data literacy** means the ability of the public to recognise and act on the opportunities and risks at stake in data creation, flows, use and storage as part of their knowledge and skills as well as within their understanding of applicable legal, ethical and institutional parameters.

#### **Technical aspects:**

**Interoperability** means the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions.

**Machine-readable format** means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure.

**Open format** means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents.

**Standard licence** refers to a default open licence with re-use conditions, usually in a digital format and available online.

**Data breach** means accidental or unauthorised destruction, loss, alteration, disclosure of, or access to, data.

**Artificial Intelligence (AI)** designates software capable of performing tasks that typically require human intelligence, including exhibiting capacity to emulate human learning, reasoning, and decision-making. Automated decision-making under AI refers to decisions made without meaningful human intervention. All AI systems depend on data for both training models and subsequent applications such as real-time inferences and generative outputs.

### **Institutions:**

**Private body** means (a) a natural person who carries on or has carried on any trade, business or profession or activity, but only in such capacity; (b) a partnership which carries on or has carried on any trade, business or profession or activity; or (c) any former or existing juristic person or any successor in title; but excludes public bodies and relevant private bodies.

**Public authorities** mean legislative bodies and judicial authorities, insofar as they perform administrative functions, as defined by national law. Natural or legal persons are also covered insofar as they exercise administrative authority. In order to enhance data openness, these Guidelines include specific measures for public authorities.

**Public body** means, for the purposes of these Guidelines, any administrative authorities at national, regional and local levels (for example, central national government, provincial government, and other municipal bodies, the police, public health and education authorities, public records offices, etc.) and public authorities.

**Public interest** is a criterion that designates shared benefits to society as a whole (for example, public services and infrastructure) rather than advancing only individual, group or private interests. The concept implies that such benefits should be promoted and protected by all, and especially by the public bodies. Determining public interest entails weighing up competing assessments of potential impact and possible harm, and considering trade-offs over time.

**Public value** refers to value created for the wider public and social benefit, including the public sector, such as use of data for participation in public policy and other public interest purposes, to ensure sustainability, equity or inclusivity, and positive impact on society, the economy, and the environment.

**Relevant private body** means any body that would otherwise be a private body under these Guidelines that is (a) owned totally or partially or controlled or financed, directly or indirectly, by public funds, but only to the extent of that financing; or (b) carrying out a statutory or public function or a statutory or public service, but only to the extent of that statutory or public function or that statutory or public service. Other private bodies outside these categories may be required or encouraged to enable data access where there is an overriding public interest to do so, such as adverse impact on human rights including environmental and equality rights.

## **Section E: Scope and Application**

17. These Guidelines apply to data collected and processed in both digital and non-digital (offline) contexts. They include specific provisions for natural or legal persons, meaning that application may differ from State to State according to legislative or administrative conceptions of a public function.
18. States remain responsible for ensuring that the provisions of the African Charter, these Guidelines, other relevant instruments developed by the ACHPR pursuant to the Charter, and other international human rights standards are applicable to any national measures for promotion and harnessing data access as a tool for advancing human rights and sustainable development.
19. Data protection and access to data are not incompatible imperatives. Advancing them together requires reference, when necessary, to considerations of proportionality, necessity and legitimate purpose such as public interest. This ensures the application of the least restrictive limitations on the right to privacy and the right to access information. Balancing data access with interests in intellectual property and national security concerns entails a similar approach.
20. The Guidelines come in a time where AI is highlighting the importance of data governance as never before, and implementation should accordingly align with global instruments such as UNESCO's Recommendation on the Ethics of Artificial Intelligence.
21. The final Guidelines will necessitate the subsequent development of an implementation strategy. This is required to ensure optimum awareness and abilities of stakeholders for ensuring positive impact. Pilot initiatives, sharing of best practices, and ongoing capacity building programmes should be part of follow-up to what the ACHPR adopts. Steps will further be needed to integrate the Guidelines into domestic legal frameworks, while at the same time such a lengthy process can be complemented by significant short-term actions within existing dispensations as well as through "soft law" developments.

## Section F: Measures

### F1: General Measures

States must establish a robust, coherent framework for data governance that aligns with regional and international standards, committing to:

22. Harmonise and domesticate the African Union Convention on Cyber Security and Personal Data Protection and the African Union Data Policy Framework into national law to ensure consistency and facilitate regional interoperability.
23. Demonstrate strong leadership, ideally at the highest level of government, combined with a whole-of-government approach that enables effective policy coordination and implementation of these frameworks with multi-stakeholder participation that includes access to data.
24. Create or strengthen a National Integrated Data Management Framework (elaborated below) that enables the production of data relevant to development, and fosters the equitable and safe flow of data between government, individuals, civil society, academia, and the private sector, placing people at the centre and promoting the use and reuse of data by all participants while safeguarding against illegal data misuse.
25. Develop and implement a national Open Data Policy that mandates public institutions and bodies receiving public funds to proactively make data publicly available. This policy should be a cornerstone of a state's digital transformation agenda.
26. Standardise access processes for public and private data requests including consistent justification requirements.
27. Ensure that data controllers and processors must obtain informed consent where required, limit data use to defined purposes, and respect data subjects' rights to access, correction, and deletion.
28. Establish a clear and legitimate legal framework that narrowly defines the circumstances under which public sector bodies and other stakeholders may request, and gain, access to data held by private bodies, applicable to situations of genuine and demonstrable overriding public interest (such as declared in public emergencies, verified health crises, or for legally mandated electoral oversight). Such access must be subject to strict necessity and proportionality tests, independent oversight or judicial review and robust data security protocols and accountability safeguards to prevent misuse or overreach.
29. Create or formally designate a state institution such as an Information Commission or Data Protection Authority (or hybrid or equivalent), and provide it with sufficient legal powers, technical capacity, and financial resources to oversee data governance. This institution should ensure that all data collection, processing, and sharing activities must comply with applicable national and international laws, foster a balance between privacy, access and other issues, and offer effective redress for violations of the right to information.
30. Create a central data access point for the public to access and download datasets, subject to strong safeguards for protecting human rights. This portal should provide a single point of access, ensure data is accessible in open format(s), under an open licence and be free of charges for general access.
31. Publish transparent and accessible documentation of data processing and publication workflows.
32. Prioritise storage of open government data within national or regional data centres to promote African data sovereignty.
33. Promote environmentally sustainable data practices by encouraging the use of renewable and clean energy sources for data centres, energy-efficient data storage and processing systems, and the responsible management, recycling, and disposal of electronic waste. Such measures should be integrated into national

data and digital transformation strategies to minimise environmental impact and support green digital development.

34. Take actions to ensure that datasets used for AI and algorithmic decision-making must be representative, validated for accuracy, and monitored for bias, with clear documentation of data provenance and usage constraints.

## F2: Legal, Policy and Programmatic Measures

35. Data forms an essential part of the right to information, is vital for democracy and essential to promote more transparent, accountable, efficient, and responsive institutions, as well as being essential for sustainable development. Its governance should be within a human rights-compliant legal framework. Accordingly, states should:

### **Interpret or reform existing legislation and regulation to encompass data:**

36. Ensure existing access to information dispensations are understood to encompass "data" and "datasets" as forms of information subject to the right of access.
37. Create coherence across legal instruments such as through legal audits or gap analyses to identify conflicting provisions in existing laws (e.g., Official Secrets Acts, cybersecurity laws) which may impact on access to data.

### **Encoding the right of access to data:**

38. States shall ensure that the right of access to information, guaranteed by law, shall be in accordance with the following principles:
39. Every person has the right to access data held by public bodies and relevant private bodies expeditiously and inexpensively.
40. Every person has the right to access data of other private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.
41. The right of access to data shall be guided by the principle of maximum disclosure, limited by narrowly defined exemptions, which shall be provided by law and shall comply strictly with international human rights law and standards.
42. States shall strengthen legal measures governing consent to include clear and accessible data collection, processing and access opt-in and opt-out rights, ensuring that individuals maintain meaningful control over how their personal data. Opt-out mechanisms should be feasible, transparent, and non-discriminatory, balancing the protection of individual rights with the promotion of public value.
43. As part of the right to information, access to data entails that data should be openly available, easily discoverable, accessible, used, shared and disseminated by anyone for any purpose that is not circumscribed by narrow exemptions.
44. States shall ensure that freedom of information/ access to information laws, and correspondingly of data, shall take precedence over any other laws that prohibit or restrict the disclosure of information.
45. Cross-border transfers of data must comply with national data protection laws and international agreements to ensure equivalent protection.
46. States shall adopt national policies that make publicly funded data, including research data, openly available by default (see below).

47. Where data serves an overriding public interest (e.g., health, environment, elections, disaster response, countering gender-based violence), disclosure obligations should be absolute.
48. Legal provisions should provide for remedy in the face of refusal to provide access to data, such as through administrative review by an oversight body or ombudsperson, as well as through, judicial appeal. (see below)

**Procedure for accessing information:**

49. Access to data requests, including for reuse, shall be granted as expeditiously and inexpensively as possible, and in accessible formats and technologies.
50. No requester shall be required to demonstrate a specific legal or personal interest in the data requested or to provide justification for a request.
51. Requesters shall be assisted in making requests for data orally or in writing and in conformity with processing requirements. Appropriate support shall be provided to non-literate persons and persons with disabilities to make requests for information on an equal basis with others.
52. Any refusal to disclose data shall be provided timeously and in writing, and it shall be well-reasoned and premised on international law and standards.

**Protected disclosures in the public interest:**

53. Protection should be specified in law to apply to whistleblowers sounding public interest alarms about data management practices that adversely affect data access rights.
54. No person shall be subject to civil, criminal, administrative or employment-related or other sanctions or harm, for releasing data on wrongdoing or which discloses a serious threat to health, safety or the environment, or whose disclosure is in the public interest, in the honest belief that such information is substantially true.
55. States shall ensure legal measures to establish and implement protected disclosure regimes and independent institutions to oversee the protected disclosure of data in the public interest.

**Duty to create, keep, organise and maintain information:**

56. States shall ensure legal measures that require public bodies and relevant private bodies, shall create, keep, organise and maintain data in a manner that facilitates the exercise of the right of access to information and enables data access and data sharing for the reuse of data as a public good.
57. Data retention should align with proportionality principles, and long-term datasets critical to rights and development (e.g population, environment, public archives) must be preserved beyond routine administrative timelines.
58. Public and relevant private bodies should be required to maintain and publish catalogues of the datasets they hold, with metadata and reuse conditions clearly indicated.

**Data access for public value:**

59. States shall promote inclusive representation of and engage relevant stakeholders in the data ecosystem – including vulnerable, underrepresented, or marginalised groups – in open and inclusive consultation processes during the design, implementation, and monitoring of data governance frameworks related to data access and sharing to reinforce trust.
60. States shall enhance transparency of data access and sharing arrangements to encourage the adoption of responsible data governance practices throughout the data value cycle that meet applicable, recognised, and widely accepted technical, organisational, and legal standards and obligations, including codes of conduct, ethical principles and privacy and data protection regulations.

61. Where personal data is involved, States should ensure transparency in line with privacy and data protection frameworks with respect to what personal data is accessed and shared, including with whom it is shared, for what purpose, and under what conditions access may be granted to third parties.
62. States shall empower individuals, social groups, and organisations through appropriate mechanisms and institutions such as trusted third parties that increase people's agency and control over data they have contributed or that relate to them, and enable them to recognise and generate value from data responsibly and effectively.
63. States shall encourage and facilitate innovative data sharing models, including but not limited to data donations and data pools, including involving researchers, data scientists and journalists in order to promote equitable access, public value creation, and responsible data use. States shall incentivise and encourage knowledge partnerships.

#### **Competitive data markets:**

64. States shall encourage competition-neutral data-sharing partnerships, including Public-Private Partnerships (PPPs), where data sharing across and between public and private sectors can create additional value for society. In so doing, States should take all necessary steps to avoid conflicts of interest or undermining government open data arrangements or public interests.
65. States shall foster competitive markets for data through sound competition policy and regulation that addresses possible exploitation of market dominance, including enforcement and redress mechanisms that increase stakeholders' agency and control over data and ensure an adequate level of consumer, intellectual property, security and privacy and personal data protection.

#### **Enabling Reuse:**

66. States shall foster, where appropriate, the findability, accessibility, interoperability and reusability of data across organisations, including within and across the public and private sectors. In particular:
  - a. strive to ensure that data is provided together with any required meta-data, documentation, data models and algorithms in a transparent and timely manner, supported by appropriate data access control mechanisms, including application programming interfaces (APIs);
  - b. assess and, whenever possible, promote the development and adoption of interoperable specifications for effective data access, sharing, and use, including common standards for data formats and models as well as open source implementations - promoting open formats.
67. States should develop and implement public programmes to increase awareness about the benefits of these specifications for open, interoperable data access.

### **F3: Measures for Specific Data**

#### **Selected Categories of Data**

Sensitive data must be encrypted, access-limited, and processed only for explicitly authorized purposes, with additional safeguards against unauthorized disclosure.

Access to children's data must align with the UN Convention on the Rights of the Child and the need for child-sensitive data governance, including consent and protection mechanisms.

There must be safeguards against stigmatization or misuse of data in relation to marginalised groups, as per the UN Guidelines on Disaggregation of Data for the SDGs as well as the CARE Indigenous Data Sovereignty principles.

Sex-disaggregated data is essential to support gender equality, as per UN Women's Minimum Set of Gender Indicators

## **Budget and Fiscal Data**

States should require publication of machine-readable datasets on procurement, tax expenditures, and debt, in line with Open Budget Index and International Budget Partnership standards.

### **Research Data from Public Funding:**

68. States shall establish in national policies and institutional measures access regimes for research data from public funding in accordance with the following objectives and principles:
  - a. Openness: balancing the interests of open access to data to increase the quality and efficiency of research and innovation with the need for justifiable restrictions recognising intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests
  - b. Transparency: making available and accessible clear information on data-producing organisations, documentation on the data they produce, and specifications of conditions attached to the use of these data.
  - c. Formal responsibility: promoting explicit, formal institutional rules on the responsibilities of the various parties involved in data-related activities pertaining to authorship, producer credits, ownership, usage restrictions, financial arrangements, ethical rules, licensing terms, and liability.
  - d. Legal conformity: paying due attention, in the design of access regimes for digital research data, to national legal requirements concerning national security and privacy.
  - e. Protection of intellectual property: describing ways to obtain open access under the different legal regimes of copyright or other intellectual property law applicable to databases as well as trade secrets.
  - f. Interoperability: paying due attention to the relevant international standard requirements for use in multiple ways, in co-operation with other international organisations.
  - g. Quality and security: fostering good practices for methods, techniques and instruments employed in the collection, dissemination and accessible archiving of data to enable quality control by peer review and other means of safeguarding authenticity, originality, integrity, security and establishing liability. This includes the need for data to be accurate, complete, timely, and protected against unauthorized access or misuse.
  - h. Efficiency: advancing further cost effectiveness within the African and global science system by promoting good practices in data management, access and specialised support services.
  - i. Accountability: evaluating the performance of data access regimes to maximise the support for open access among the scientific community and society at large.
69. Research institutions shall develop Research Data Management Policies. These policies shall establish rules and guidelines for how research data is to be collected, stored, and shared, in alignment with national and international best practices for reuse for commercial or non-commercial purposes insofar as they are publicly funded and make it publicly available through an institutional or subject-based repository that enables data access and data sharing.
70. All academic and research institutions, and any entities handling academic data, shall establish, implement, and publicly disclose clear protocols for the retention, anonymisation, and destruction of such data. These protocols shall include specific safeguards to prevent the unlawful repurposing of student-submitted work and other research outputs.

### **Health Data:**

71. To create an interoperable digital health ecosystem that facilitates secure data exchange while safeguarding patient privacy, States require an opportunity and risk-based approach. This can inform clear review and approval procedures and streamlined approval processes that involve multiple organisations.
72. States should distinguish between aggregated public health data (which should be open) and personal health data (which must be protected), guided by the WHO Health Data Governance Principles.
73. States shall implement the following to ensure access to health data for reuse for secondary purposes:
  - a. Concrete improvements to privacy and transparency, because public trust is crucial to obtaining patient data. This entails implementing scalable security measures beyond pseudonymisation.
  - b. Establish a centralised and secure data environment to standardise patient data handling, enforce standardised storage and curation of a catalogue of commonly used datasets with clear guidelines on which entities are eligible for access.
  - c. Create an online library to provide data curation code, tests, and documentation to ensure that analysts can access well-curated data.
  - d. Develop a single map detailing all approval procedures with all relevant organisations ensuring transparency of approval criteria, regulatory agencies for approval and clear and transparent timeframes for approvals.
  - e. Create a common application for ethics, information guidance, and access permissions.

### **Environmental Data:**

74. States shall establish clear obligations for the proactive disclosure of environmental data, consistent with continental and regional frameworks such as Principle 10 of the Rio Declaration and the UNECE Aarhus Convention, aligned with national governance instruments concerning natural resources.
75. States shall require public authorities and private companies, particularly those operating in extractive and high-impact industries, to publish environmental and social impact data openly and comprehensively. This disclosure shall include baseline assessments, monitoring reports, and risk mitigation measures, ensuring that communities and stakeholders have timely access to information that affects their rights, livelihoods, and environments. As per the Extractive Industries Transparency Initiative (EITI) disaggregated data should be required in terms of company, project, and community impact.
76. States should ensure they have provisions for real-time or near-real-time access to data concerning environmental hazards (e.g., pollution, deforestation).

### **Private Data in the Public Interest:**

77. To unlock the value of data across the economy, States shall develop measures to ensure private sector data is appropriately available, accessible and usable during state emergencies, for public interest purposes and across the economy, while protecting data rights and private sector's intellectual property and measures to observe ethical data disclosure, access, and reuse.
78. States should foster awareness amongst private sector organisations of the societal benefits of proactive data disclosures and data sharing through engagements with the private sector, private sector regulatory bodies, Chambers and sector councils.

79. States should explore incentivising mechanisms, such as public recognition programmes, to increase proactive disclosures of private sector data and private sector data sharing on a voluntary basis.
80. States should ensure the availability of open and interoperable data standards for proactive disclosures by the private sector to enable data reuse in the public interest.
81. State measures should promote transparency in all data-sharing collaborations, including the data used and the impact of the collaboration.
82. States should engage in periodic research on the macroeconomic and social benefits of proactive data disclosures and data sharing by the private sector for the public interest.

**Sector Guidance:**

83. States shall promote, where appropriate, self- or co-regulation mechanisms – including voluntary guidance, standards, codes of conduct and templates at the sector level for data access and sharing agreements – that provide legal flexibility while ensuring that all relevant stakeholders have access to implementation guidance for implementing access to data measures.

**Access to Digital Platforms' Data Holdings in the Public Interest:**

84. Private sector digital platforms falling within the scope of these Guidelines, operating within Member States and/or processing the data of African users, shall be required to sign and adhere to a binding Code of Conduct regarding stakeholder access to data in the public interest.
85. This Code of Conduct, which shall be developed and regularly updated by the Information Commission (or equivalent) with oversight of access to information or data in the public interest shall include, but not be limited to, the following provisions concerning stakeholder access, drawing upon international best practices and adapting them to African contexts:
  - (a) Such platforms shall commit to refraining from initiating, pursuing, or threatening legal action, including but not limited to actions alleging breach of contract, intellectual property infringement, or unauthorised access, against African researchers, journalists and civil society actors who engage in the automated collection (scraping) of publicly accessible data from their services for legitimate public interest purposes, particularly in cases where no reasonable and equivalent alternative access mechanisms are provided by the platform. This protection shall extend to actions taken against the various actors' affiliated institutions.
  - (b) Such platforms shall be mandated to actively develop and provide robust, secure, auditable, and non-discriminatory alternative access mechanisms (e.g., APIs, data sharing agreements, sandboxed environments) for stakeholders seeking non-publicly accessible data or more structured access to public data, ensuring such mechanisms are technically feasible, reasonably priced (if applicable), and timely.
  - (c) The Code of Conduct shall establish clear criteria for what constitutes "legitimate public interest research," encompassing areas such as, but not limited to, studies on algorithmic bias, online harms to human rights, disinformation and/or hate speech, market competition, socio-economic and psychological impact, , and contributions to scientific understanding. Such research must adhere to ethical guidelines, data protection laws, and standards of academic, journalistic or other professional integrity.

(d) Platforms shall commit to greater transparency regarding their data collection practices, algorithmic decision-making, and terms of service related to data access, enabling stakeholders to better understand the data environment.

(e) Platforms shall commit to engaging in good faith with African stakeholders to address data access challenges, provide clarifications on data structures, and explore collaborative research opportunities.

86. The provisions of this clause are designed to foster an environment conducive to independent, critical research necessary for robust digital governance and public accountability across Africa. They aim to redress power imbalances between large digital platforms and African stakeholders in data access, ensuring that the absence of structured access mechanisms does not become a de facto barrier to essential data-driven insights.

87. Mechanisms for vetting bona fide data requests as being based on public interest criteria and ethical standards, and for enforcement of decisions, dispute resolution, and periodic review of adherence to this Code of Conduct shall be established by the Information Regulator (or equivalent), National Statistical Office, national research facility (or equivalent).

#### **Access to Public Archives Data and Classified Information:**

88. Access to public archives data shall be governed by the principles of maximum disclosure, timely availability, and ease of use, subject to the classifications and limitations in relevant national legislation.

89. National legislation shall define clear, auditable processes for the classification, declassification, and secure management of public archives data, ensuring accountability and preventing arbitrary withholding of information.

90. States shall invest in digital archival infrastructure and capacity building to ensure the long-term preservation, accessibility, and discoverability of public archives data, leveraging digital technologies to that end.

#### **Elections Data:**

91. Elections management bodies shall establish and enforce an agreed set of data principles that can help to promote integrity in public information, and also set clear standards and expectations for the behaviour of political parties, candidates and media outlets, in the creation, dissemination and management of electoral data.

92. Elections management bodies shall develop and implement measures to elevate accurate data and official data sources on digital platforms, as well as countering data-based disinformation.

93. Election management bodies shall standardise frameworks for safeguarding data integrity, responsible data dissemination and sharing of data about disinformation trends, effective countermeasures and public sentiment insights.

94. To ensure enforcement of online platforms' own content regulation during elections, elections bodies shall ensure effective communication between online platforms and election stakeholders, and have measures to prioritise access to accurate, reliable data about the content regulation processes.

95. Elections bodies shall facilitate effective relationships between the election body, elections monitoring organisations, civil society, researchers, journalists and other electoral stakeholders and digital platforms and put in place adequate policies and processes to enable rapid access to elections data during the electoral period and timely responses to threats to data integrity or data-driven disinformation.
96. States need to promulgate stronger national legislative obligations on platforms, including advertising platforms, that are major data holders, such that they are obliged by law to provide data on:
  - a. Their human rights impact assessments in regard to elections
  - b. Their election risk-mitigation plans
  - c. Their cooperation agreements such as with election bodies, media, civil society and fact checkers.

## F4: Institutional Measures for Public Bodies

### **Data Access Policies**

Public body policies on data access should cover collection, storage, sharing, quality, retention, disposal and security, as part of wider comprehensive data management provisions. There needs to be robust technical and organizational measures to protect data against unauthorized access, breaches, or loss, including secure storage, encryption, and access control.

### **Proactive disclosure**

97. Public bodies shall be required, even in the absence of a specific request, to proactively and timeously publish data of public interest, including data about their functions, powers, structure, officials, decisions, budgets, procurement data, environmental impact assessments, fiscal expenditure and related information.
98. Relevant private bodies shall be required to proactively publish data emanating from such activities in the public interest; and to facilitate publication of other data in the public interest.
99. Data proactively published or otherwise disclosed under legal requirements shall be accessible and reusable in accordance with internationally accepted open data standards.

### **Prioritisation Releasing High-Value Datasets**

100. Public bodies shall proactively disclose "high-value datasets" free of charge, in machine-readable formats, and accessible via Application Programming Interfaces (APIs).
101. Thematic categories for HVDs include geospatial, environmental, official statistics, company ownership, cultural, linguistic and meteorological data, among others.

### **Standardised and Open Formats**

102. Public sector bodies shall make documents and data available for reuse in open, machine-readable formats. This measure is intended to facilitate seamless reusability and interoperability across the AU.

### **Transparency on Reuse Conditions**

103. Public bodies must be transparent about the conditions for data reuse. This includes publishing the standard licence or other open licence, such as Creative Commons or an equivalent open licence and making easily discoverable online their available information about datasets, including metadata.

### **Fair and Non-Discriminatory Access**

104. Public sector bodies must protect against vendor lock-in and are prohibited from making exclusive arrangements for the reuse of public data, except in very limited, exceptional circumstances, to ensure fair competition in the market for data-driven services.
105. States shall actively promote and facilitate the adoption of innovative, voluntary, and rights-respecting data sharing models to maximize data access for the public good and public value.
106. In this regard, data sharing models, including but not limited to data donations (where individuals consent to the use of their data for specific public interest purposes) and the establishment of data pools (collaborative mechanisms for collecting, managing, and sharing data from multiple sources), shall be actively encouraged.
107. Such models must be underpinned by transparent governance frameworks, robust safeguards for privacy and personal data protection, and mechanisms to ensure data justice and equitable benefit-sharing.

### **Marginal Cost Charging**

108. Public sector data should generally be available free of charge. In cases where charges are applied, they are generally limited to the marginal costs incurred for reproduction and dissemination.
109. While public sector bodies' data-access standards must be non-discriminatory, this does not exclude the possibility of tiered access where charges are levied on powerful entities in order cross-subsidise and support less well-resourced entities such as academic researchers and marginalised communities in data access and use.

## **F5: Institutional architecture**

### **Independent oversight body**

110. Specific institutional arrangements, resourcing models and capacity-building measures required to meet data expectations will necessarily vary across contexts and will need to be addressed through careful planning that addresses low-capacity and resource-constrained administrations.
111. An independent and impartial oversight mechanism, ideally an Information Commission (or hybrid or equivalent – hereafter “Commission”), shall be established by law to monitor, promote and protect the right of access to information and resolve disputes on access to information.
112. The independence of such a body should be guaranteed in law, which shall stipulate a transparent and participatory appointment process, a clear and specific term of office, adequate remuneration and resourcing, and ultimate accountability to the legislature. The Commission requires adequate human capital, meaning people with up-to-date skills to use data, design policies and regulations, and hold power to account as regards data access.
113. Public bodies and relevant private bodies shall be required to recognise decisions of the Information Commission as formally and legally binding in all matters relating to access to information, including resolving access to information disputes.
114. The Commission's powers shall include the power to issue orders to public bodies, compelling them to release information, and can take punitive action against officials who wilfully refuse to comply.
115. The Commission shall ensure that data is safeguarded and accredit Data Intermediaries to facilitate access to de-identified data to foster public trust, a prerequisite for a robust data ecosystem.
116. The Commission shall ensure that stakeholders are held accountable in taking responsibility, according to their roles, for the quality of the data they share and for the systematic implementation of risk management measures throughout the data value cycle, including measures necessary to protect the security, confidentiality, integrity, and availability of data.
  - a. To this effect, the Commission should promote the adoption of impact assessments and audits as well as responsible stewardship for data sharing within organisations.
  - b. It should oversee the adoption of service standards (e.g., response times, appeals processes). install consultation mechanism, create a culture of confidence and discourage undue risk aversion.

- c. The Commission should clarify roles and responsibilities amongst data-holding agencies, and support related capacity building, resourcing and skills development within public institutions. It should promote partnerships with civil society, academia, and international organizations to support such training programs.
- d. The Commission's functions should include promotion of data literacy within the wider public as well as in the civil service curriculum.
- e. The Commission should operate a mechanism for regular public reporting on the state of data openness and access requests, and provide transparency reports on its own functioning as regards adjudicating and promoting data access.

### **National Statistical Offices**

- 117. The role of National Statistical Offices (NSO's) of States as a data collector should be enhanced to play the part of a central data steward and coordinator in an Integrated National Data Management Framework.
- 118. The NSO shall work with data holders and data intermediaries and public bodies to support data access and data sharing, ensuring that a country's data assets are used effectively and ethically for the public good.
- 119. The NSO shall set and maintain standards for data collection, processing, and dissemination and work with the Information Commission (or equivalent) to foster skills development in public bodies for implementing data standards, and help ensure that data from different sources are consistent, coherent, and can be integrated effectively.
- 120. To improve data interoperability, the NSO shall build cross-government consensus on defining and agreeing on standards. This improves collaboration, encouraging experts across sectors to consider problems and risks in detail.
- 121. To incentivise and promote the adoption of standards across the wider public sector, the NSO shall assess and articulate the benefits of adopting data standards, formulate and implement processes to help identify and showcase implementation of standards, or pilots of new standards to demonstrate the value of adopting them.
- 122. The NSO as a national data steward shall support data quality processes to safeguard the integrity of the data and the capability of the data for reuse beyond their original purpose by different stakeholders.
- 123. For the purposes of implementing the National Integrated Data Management Framework, the NSO shall ensure:
  - a. trust across stakeholders to uphold the social contract for data to maximise value and prevent misuse.
  - b. funding for data production, exchange, and use, including funding for the data infrastructure.
  - c. adequate incentives for public bodies to produce, protect, and share data, valuing data transparency.
  - d. adequate measures to ensure data demand and a culture of data reuse.

### **National Data Advisory Council**

- 124. States can consider establishing a National Data Advisory Council, falling within the purview of the existing Information Commission or national data/information regulators, so as to incorporate their influence and powers in line with existing and reformed legislation on access to information. The Council shall develop, implement and monitor the Data Policy, serve as the central data access point, advise the national

government, the Information Commission (or equivalent), the National Statistics Office and national research facility. It should conduct monitoring and make recommendations.

125. The Council could consult experts and develop guidance on data ethics, and foster public-private partnerships to facilitate access to data.
126. The composition of the Council shall include representatives from government, the Information Commission (or equivalent), the National Statistics Office and national research facility, as well as from non-State stakeholders. This multistakeholder composition shall ensure that the Council is best placed to advise and oversee the country in relation to data access laws and best practices.
127. The Council shall ensure multistakeholder participation in developing and reviewing data policy, technical, institutional, and legal measures.

## **Judiciary**

128. Justice authorities shall promote open justice through enabling data sharing and access to data through timeous publication of judicial decisions in open formats.
129. In judicial decisions, to balance the right to access to data on judicial decisions with other rights and obligations, the justice authorities shall apply the international standards of: (i) Suitability (the measure should be suitable for achieving the desired objective); (ii) Necessity (a less restrictive means should be used if it is equally effective); and (iii) Proportionality in the strict sense (the measure should not be disproportionate to the objective). Proportionality shall precede tests of legality (whether the possible interference with the right is based on national law) and legitimate aim (whether the interference pursues one of the aims dictated by any limitation clauses present, respectively, in the frameworks on Civil and Political Rights).

## **F6: Exemptions and Safeguards**

### **Exemptions**

130. Information may only be legitimately withheld where the harm to the interest protected under the relevant exemption demonstrably outweighs the public interest in disclosure of the information. Such information may only be withheld for the period over which the harm could occur.
131. Exemptions are subject to oversight, transparency, and periodic review.
132. Where a portion of a document containing requested information is exempted from disclosure, the exempted portion shall be severed or redacted and access granted to the remainder of the document that is not exempted from disclosure.
133. Laws governing classification of information shall stipulate the maximum period of the classification and restrict classification only to the extent necessary, never indefinitely.
134. All classification decisions strictly abide by lawful exemptions.
135. Information may only be legitimately withheld as an exemption if its release would:
  - a. Result in the unreasonable disclosure of the personal information of a third party;
  - b. Cause substantial prejudice to a legitimate commercial or financial interest of relevant stakeholders or other third party;
  - c. Endanger the life, health or safety of an individual;

- d. Cause substantial prejudice to the national security and defence of the State;
- e. Cause substantial prejudice to international relations where the information relates to information required to be held in confidence under international law, the position of the State with respect to international negotiations, and diplomatic or official correspondence with States or international organisations and diplomatic or consular missions;
- f. Cause prejudice to law enforcement, in particular, the prevention and detection of crime, apprehension or prosecution of offenders and the administration of justice;
- g. Result in the disclosure of confidential communication between medical practitioner and patient, lawyer and client, journalist and sources, or is otherwise privileged from disclosure in legal proceedings; or
- h. Jeopardise the integrity of a professional examination or recruitment process.

136. These Guidelines acknowledge that personal information protected under personal data legislation is not open by default and the right to access data must be balanced with fundamental rights to privacy.

137. These Guidelines acknowledge intellectual property rights of third parties but prohibits public sector bodies from claiming a sui generis database to prevent or restrict the reuse of documents beyond the limits set out in national laws.

### **Safeguards**

Public bodies shall, in accordance with national law, ensure the following safeguards for access or reuse of public data:

- 138. Access is granted for the re-use of data only where the public sector body or the competent body, following the request for re-use, has ensured that data has been anonymised (in preference to pseudonymisation), in the case of personal data; and modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights;
- 139. Public bodies shall impose conditions that preserve the integrity of the data processing environment used, retaining a right to verify the process, the means and any results of processing of data undertaken by the re-user to preserve the integrity of the protection of the data, and retaining the right to prohibit the use of results of processing that prejudice the rights and interests of the public body or third parties.
- 140. In alignment with the African Union Convention on Preventing and Combating Corruption, there should be protections against retaliation, anonymity guarantees, and legal immunity for good-faith disclosures by whistleblowers.

## **F7: Enforcement**

### **Responsibility**

141. The designated oversight body, preferably the Information Commission (or equivalent), shall be responsible for enforcing these Guidelines, in accordance with national laws and international standards, which involves monitoring compliance, investigating violations, and issuing directives.

### **Compliance and Audits**

142. Both public and private bodies should be encouraged to undergo regular audits tied to reporting and governance processes to strengthen proactive disclosure practices. As part of this process, institutions can be required by law to publish, at least annually, a list of datasets in their custody, including information on their accessibility status (open, restricted, or confidential), together with justifications for any restrictions.

143. The oversight authority shall conduct regular audits, inspections, and reporting to ensure adherence to data management, disclosure, and ethical standards.

### **Sanctions and Appeals**

144. States shall adopt policy, regulatory, or administrative measures to address failures to comply with proactive disclosure obligations or with requests for data. Entities that fail to comply with these guidelines may face administrative sanctions, fines, suspension of data handling privileges, or legal proceedings as provided by law. Measures shall provide that:
- a. The wilful or negligent destruction, damage, alteration, concealment or falsification of data and the obstruction or interference with the performance of the duties of a data holder or of an oversight mechanism, be recognised as a serious infraction subject to appropriate remedial action and be established as offences punishable by law.
  - b. Institutions, officers, and executives of institutions that have a pattern of failure to meet proactive disclosure duties or systematically obstructed disclosures should be sanctioned in accordance with institutional, regulatory frameworks, administrative or governance frameworks, including criminal liability in cases of willful obstruction or destruction of data. These sanctions should be proportionate and dissuasive, and explicitly apply to both public servants and entities that fail to comply. On the other hand, there should also be incentives for compliance (e.g., performance-based rewards).
  - c. Any refusal to disclose data should be subject to an expeditious internal appeal process at no cost to the applicant. Applicants should receive written reasons for refusal and be able to access an internal review within a reasonable period, for example within 30 to 45 days.
  - d. Review appeals should occur within a maximum of 90 days and be affordable, and be accessible to marginalized groups. Appeal and review decisions should be communicated in clear and accessible formats, without administrative fees, Digital platforms can provide access to filing complaints, tracking cases, and accessing decisions. Applicants should retain the right to seek recourse through judicial or other independent bodies in line with national procedures.
  - e. States shall establish clear liability mechanisms for the legal misuse or unauthorised use of public data by third parties, ensuring accountability, remedies, and deterrence against practices that undermine transparency, privacy, or public trust.
  - f. Enforcement policies and procedures shall be periodically reviewed and updated to reflect emerging risks, technological changes, and evolving legal standards.

### **F8: Ethical Data Governance and AI**

145. States shall mandate the use of ethical principles in data collection and usage by all public institutions and ensure such in AI adoption. These principles must be aligned with international human rights standards, promoting fairness, non-discrimination, transparency, accountability, equity, protection of individual privacy and the public interest.
146. States shall implement a requirement for human rights impact assessments and fairness audits for all AI systems and related data as used in public service delivery or governance. This is essential to identify and mitigate biases that could exacerbate structural inequalities and discrimination.

147. States can call for AI service providers to explain how they are identifying and mitigating ethical and rights risks before deployment, including how data quality and access issues may be implicated in data bias, algorithmic bias, explainability, and accountability.
148. They should be able to specify that datasets used for AI must be accurate, representative, and securely managed, with safeguards to prevent unauthorized access, manipulation, or breaches.
149. States shall mandate all public bodies to provide clear and understandable explanations for the decisions and underlying data used in AI or automated systems, especially when those affect a citizen's rights or welfare.
150. States shall implement proportionate cybersecurity safeguards to protect data integrity in AI systems without unduly restricting access.
151. Stakeholders, including affected communities, should be engaged in the design, deployment, and evaluation of AI systems to ensure alignment with societal values and expectations, including in relation to data provenance, quality, representativeness and security.

## Section G: Implementation

152. States shall adopt legislative, administrative, judicial, budgeting and other measures to give effect to these Guidelines and facilitate its dissemination.
153. When States review or adopt legislation on access to information, they shall be further guided by the African Commission's Model Law on Access to Information for Africa and the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 and ACHPR Resolution 620.
154. When States adopt measures related to elections, they shall be further guided by the African Commission's Guidelines on 28 Access to Information and Elections in Africa.
155. In accordance with Article 62 of the African Charter, States shall, in each Periodic Report submitted to the African Commission, provide detailed information on the measures taken to facilitate compliance with the provisions of these Guidelines.
156. These Guidelines are designed to be implemented through a multi-stakeholder approach, ensuring the meaningful participation of government, private sector, civil society, media, academia, the technical community and affected communities in the design, implementation and oversight of policies and practices.
157. States should collaborate with civil society, media, academia, the private sector, and communities to design, implement, and monitor their data policies. Furthermore, States shall engage actively with the Special Rapporteur on Freedom of Expression and Access to Information in Africa as they proceed, providing national insights to inform how data serves as a powerful force for human rights, transparency, inclusion and development across Africa.
158. States shall develop and implement national data literacy and digital skills programs for the public to empower them to understand their data rights, navigate the online information environment, and critically evaluate data-driven narratives and platform business models.
159. States shall develop and implement continuous professional development for civil servants in data governance, data quality management, and the ethical use of data to inform evidence-based policy-making.
160. States shall ensure continued dedicated resources to improving the quality, integrity, and completeness of public data across all sectors, recognising that poor data is a significant barrier to effective governance.
161. States shall conduct periodic reviews of data access frameworks, at least every three to five years, to adapt to technological changes and implementation experiences. The findings of such reviews shall be made public and formally reported to parliament or an equivalent oversight body to ensure transparency and accountability.
162. The Special Rapporteur shall encourage reviews of data access frameworks and for States to adopt regular reporting and monitoring practices to assess implementation and effectiveness. The Rapporteur may also engage in the development of further guidance, voluntary submissions of reports by States or institutions implementing Resolution 620, and regional analysis on implementation progress of Resolution 620.
163. States shall adopt, and periodically apply, measurable performance indicators for the implementation of data access within data governance frameworks, developed through public consultation.

## Appendix A: Acknowledgements

The Rapporteur wishes to thank the African Alliance for Access to Data for its support in organising consultations towards the Guidelines, as well as Research ICT Africa for leading the drafting process and integrating stakeholder comments. Acknowledgements are due to APC, Cipesa, and Luminare who helped to make a number of consultations possible. Finally, gratitude is extended to the many organisations and individuals who took time to engage with the process, illustrating that this initiative has strong resonance with African interests in data, human rights and sustainable development.

## Appendix B: Drafting Process

Resolution 620 mandated the Special Rapporteur on Freedom of Expression and Access to Information in Africa to lead the drafting process and develop "appropriate normative standards to guide data collection, deployment and access issues concerning data." It called for the Rapporteur to consult broadly to this end. Under the leadership of the Rapporteur, the consultation process achieved input from a wide range of parties, including civil society organisations, regulatory bodies, technology actors, media organisations and journalists, and academics. This helps to ensure that the Guidelines are grounded in diverse perspectives and are relevant to the varied contexts across Africa.

The process included:

Phase 1: 2024-2025 discussions with the African Alliance for Access to Data decide what kind of instrument to aim for - concluding with recommendation to the Rapporteur to develop Guidelines as the optimum instrument.

Phase 2: Broad consultations and awareness raising under auspices of the Rapporteur:

Virtual events - 11[1]

In person events - 14 (Lusaka, Kampala, Manila, Addis, Dakar, Windhoek, Johannesburg, Nairobi)[2]

Responses to an online form: 226 responses in English and 20 in French

Phase 3: Focused consultations specifically on Resolution 620 draft Guidelines:

In person events on Version 1 and 2 - Johannesburg (sidelines of M20 summit), Windhoek (sidelines of FIFAfrica)

Online consultation on Version 3 - Nov/Dec 2025 (eight detailed responses)

---

[1]

1. 22 August: Legal Resources Centre (LRC), International Network of Civil Liberties Organizations (INCLIO), African Internet Rights Alliance (AIRA)
2. 30 May General Assembly of African Network of Information Commissions
3. 9 July: African Network of Human Rights Institutes
4. 18 July African Open Science Platform
5. 19 July West African Youth IGF (WayIGF)
6. 19 June African Fact Checkers Network
7. 9 July Disinformation summit in (South Africa) (South African Human Rights Commission - SAHRC)
8. 25 August West African Digital Rights Network
9. 29 August Africiviste (and Article19)
10. Misa Mozambique

[2]

11. AI LABS (Data Science for Social Impact Research Group)
  1. April 29-1 May: Paradigm Initiative Digital Rights and Inclusion Forum (Lusaka)
  2. May 7-8: UNESCO Southern African World Press Freedom Day (Johannesburg)
  3. July 14 -17 Network of Independent Media Councils in Africa (NIMCA) (Arusha)
  4. July 4: Thomson Reuters Foundation, East Africa Advocates Training and AI Forum (Kampala)
  5. July 23-24: University of Stellenbosch Disinformation conference (Centre for Information Integrity in Africa)
  6. August 27: East Africa Communication Association
  7. September 30 - 1 October: AU-UNESCO-SA, G20 AI for Africa
  8. September 1-2: M20 (Johannesburg)
  9. September 3-5: Ctrl+J (Johannesburg)
  10. September 24-26: FIFAfrica (Windhoek)
  11. September 9: SA Communications Association (Gqeberha)
  12. October 1-2: African Fact Check Summit (Dakar)
  13. October 29-30, Datafest (Kampala)
  14. November 5-7: African Investigative Journalism Conference (Johannesburg)