ACHPR/Res.620 (LXXXI) 2024

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

DRAFT GUIDELINES

Table of Contents

Section A: Preamble

The African Commission on Human and Peoples' Rights (the African Commission) meeting at its [...] Ordinary Private Session, held [...] :

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. The Resolution recognised the rapid advancement of technology and increasing reliance on data across governance, economic development, and social interaction throughout the African continent;

The Resolution 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; 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;

The Resolution mandates the Special Rapporteur on Freedom of Expression and Access to Information in Africa 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;

Recalling 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;

Cognisant of the African Union Convention on Cyber Security and Personal Data Protection and the African Union's Data Policy Framework;

Reaffirming that access to data for a public good can foster innovation, encourage collaboration, and empower the public to engage actively in governance and decision-making. These can also support the achievement and evaluation of progress toward achieving the Sustainable Development Goals;

Concerned that there is no guidance 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 when promoting and harnessing data access as a tool for advancing human rights and sustainable development in the digital age.

Section B: Preface

1. The African Commission on Human and Peoples' Rights (the Commission), in its Resolution from the 81st Ordinary Session, has established a clear mandate for its Member States to advance equitable data access and governance. This Resolution ACHPR/Res.620 (LXXXI) 2024, formally titled Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age (Resolution 620).
2. Resolution ACHPR/Res.620 (LXXXI) 2024, formally titled Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age (Resolution 620) was adopted by the African Commission on Human and Peoples' Rights (ACHPR) during its 81st Ordinary Session in October-November 2024 in Banjul, The Gambia.
3. Resolution 620 emerged from growing recognition of data's transformative potential in Africa's digital transformation. It was inspired by the 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. The Commission acknowledged the rapid advancement of technology and increasing reliance on data across governance, economic development, and social interaction throughout the African continent.
4. Resolution 620 aims to inform evidence-based policies, enhance public participation, and promote innovation, contributing to the Sustainable Development Goals and Africa's Agenda 2063.
5. The Resolution seeks to empower journalists and media organisations by ensuring access to data critical for investigative reporting and public-interest journalism, thereby strengthening the media's role as a watchdog in a democratic society.
6. Resolution 620 acknowledges significant risks, including 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.
7. The Resolution is essential for preserving the transparency and credibility of elections, allowing citizens to participate fully in those processes and make choices based on facts rather than falsehoods. The absence of information integrity measures to counteract misinformation and disinformation renders the information ecosystem vulnerable to manipulation and interference, undermining the foundations of democracy.
8. Resolution 620 mandates the Special Rapporteur on Freedom of Expression and Access to Information to develop normative standards for data collection, deployment, and access across Africa, establishing a framework for continent-wide consultation and implementation.
9. Resolution 620 recognises that equitable access to data (encompassing statistics, datasets, and research findings) is essential for creating a just, informed, and inclusive society in the digital era.
10. The primary objectives of the the Resolution are to:
    a. harnessing data's power to promote democracy,
    b. facilitate human rights exercise, and
    c. ensure transparency and accountability in governance.
11. 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. While existing instruments primarily address information held by public bodies, these guidelines recognize that digitalisation requires specific governance of data as raw digital signals, records, and datasets that underpin decision-making, innovation, and accountability across both public and private sectors.

12. The Guidelines are grounded in human rights primacy, ensuring that all data collection, sharing, and use must serve to advance, not undermine, the dignity and rights of individuals and communities.

13. The Guidelines prioritise uplifting marginalized communities, including women, persons with disabilities, rural populations, and children - through access to data that is inclusive, affordable, available in multiple languages and accessible formats.

14. The Guidelines serve as a principle based framework for States to implement Resolution 620 through aligning their national data strategies, policies and regulation with regional and international human rights standards in the digital era.

Section C: Key Principles

These Guidelines represent normative standards and draw on the following principles, informed directly from the Commission's resolution:

15. **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.
16. **Maximum Disclosure:** The principle of maximum disclosure should be the default for all public data and for relevant private data. Disclosure should be presumed unless demonstrably harmful. Restrictions on access must be a narrow exception, strictly justified by international human rights standards.
17. **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, governance, and the benefits derived from its use.
18. **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.
19. **Data for Public Accountability and Journalism:** Data is an indispensable tool for public accountability. Governments and private entities must ensure that data is accessible to journalists for the purpose of investigating matters of public interest, holding power to account, and fostering a well-informed public discourse.
20. **Data Access by Design:** Systems for data collection, storage and dissemination must be built with proactive disclosure features, accessibility standards and interoperability by default.

Section D: Definitions

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

Dynamic data means documents 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 documents 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 documents 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 of the number of potential beneficiaries of the value-added services and applications based on those datasets.

Data designates signals and records in structured or unstructured formats, including text, images, sound and video. AI model parameters, weights and algorithms may all be considered as data. Much "raw" data can be processed to produce meaningful results, including becoming an 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 (ML), 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 information can be organised and utilised.

Data sharing means the act of providing data access 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.

Data access means the institutional, regulatory, policy, legal, and contractual frameworks established to determine the conditions of data access.

Data access or access to data means the practical availability of data for retrieval and/or processing, usually subject to various conditionalities.

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

Data holders means entities or individuals who, according to applicable laws or regulations, 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 intermediaries means entities appointed in data access and sharing arrangements to facilitate data access and/or data sharing between data holders and data processors. Their role must be balanced with state capacity building to ensure sovereignty is not outsourced.

Data literacy means the ability of the public to recognise and act on the opportunities and risks at stake in data sharing, based on their knowledge and skills as well as on their understanding of applicable legal, ethical and institutional parameters.

Information means any original or copy of documentary material irrespective of its physical characteristics, such as records, correspondence, fact, opinion, advice, memorandum, data, statistic, book, drawing, plan, map, diagram, photograph, audio or visual record, 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 to whom a request has been made.

Information integrity means the accuracy, consistency and reliability of information content, processes and systems to maintain a healthy information ecosystem.

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.

Metadata means recorded structural or descriptive information about the primary data. Metadata can include personal data.

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.

Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

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, the Guidelines include specific measures for 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 considering trade-offs over time.

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 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.

Pseudonymisation means to the processing of personal data in such a manner that the personal 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.

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.

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

Section E: Scope and Application

21. The Guidelines include specific provisions for natural or legal persons insofar as they perform public functions or operate with public funds, according to national law. In this context, the application of these Guidelines to natural or legal persons will differ from State to State and legislative or administrative conceptions of a public function.

22. States remain responsible for ensuring that the provisions of the African Charter, these Guidelines, other relevant instruments developed by the African Commission 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.

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:

23. Harmonise and domesticate the African Union Convention on Cyber Security and Personal Data Protection and the African Union's Data Policy Framework into national law to ensure consistency and facilitate regional interoperability.
24. 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.
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. Establish a clear and legitimate legal framework that narrowly defines the circumstances under which public sector bodies may request and access data held by private bodies, limited 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 authorisation and robust data security protocols and accountability safeguards to prevent misuse or overreach
27. Create or formally designate a state institution such as a Data Protection Authorities or Information Commission and provide it with sufficient legal powers, technical capacity, and financial resources to oversee data governance, ensure compliance with the law, and offer effective redress for violations of the right to information.
28. Create or strengthen the National Integrated Data Management Framework 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 center and promoting the use and reuse of data by all participants while safeguarding for information integrity and against data misuse.
29. 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 access.

F2: Legal Measures

Reform existing legislation:

30. Reform existing access to information legislation to explicitly define "data" and "datasets" as forms of information subject to the right of access. These reforms should recognise access to data as an indispensable tool for public participation and evidence-informed policy-making.
31. These reforms need to integrate the recommendations established by these guidelines in order to reflect access to data as an integral form of information subject to the right to access.

Encoding the right of access to data:

32. States shall ensure that the right of access to information, guaranteed by law, shall be in accordance with the following principles:
33. 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.
34. Every person has the right to access data held by public bodies and private bodies expeditiously and inexpensively.
35. Every person has the right to access data of private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.
36. 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.
37. States shall ensure that freedom of information/ access to information laws shall take precedence over any other laws that prohibit or restrict the disclosure of information.
38. States shall adopt national policies that make publicly funded data, including research data, openly available by default. This is a core principle designed to stimulate a wider uptake of public data.
39. The right of access to information 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.
40. Where data serves an overriding public interest (e.g., health, environment, elections, disaster response), disclosure obligations should be absolute.

Protected disclosures in the public interest:

41. No person shall be subject to civil, criminal, administrative or employment-related or other sanctions or harm, for releasing information 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.
42. States shall ensure legal measures to establish and implement protected disclosure regimes and independent institutions to oversee the protected disclosure of information in the public interest.

Duty to create, keep, organise and maintain information:

43. States shall ensure legal measures that require public bodies, 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.
44. Data retention should align with proportionality principles. Long-term datasets critical to rights and development (e.g population, environment, archives) must be preserved beyond routine administrative timelines.
45. Public and 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:

46. 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.

47. 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.

48. 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.

49. 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.

50. States shall encourage and facilitate innovative data sharing models, including but not limited to data donations and data pools, in order to promote equitable access, public value creation, and responsible data use.

Competitive data markets:

51. 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.

52. States shall foster competitive markets for data through sound competition policy and regulation that addresses possible exploitation of market dominance and other appropriate measures, including enforcement and redress mechanisms that increase stakeholders' agency and control over data and ensure an adequate level of consumer, intellectual property, cyber security and privacy and personal data protection

Enabling Reuse:

53. 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.

54. States should develop and implement public programmes to increase awareness about the benefits of these specifications for open, interoperable data access.

Procedure for accessing information:

55. Access to data requests for reuse shall be granted as expeditiously and inexpensively as possible, and in accessible formats and technologies.

56. No requester shall be required to demonstrate a specific legal or personal interest in the data requested or to provide justification for a request.

57. 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.

58. Any refusal to disclose information shall be provided timeously and in writing, and it shall be well-reasoned and premised on international law and standards.

F3: Measures for Specific Data

Research Data:

59. 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 information on data-producing organisations, documentation on the data they produce and specifications of conditions attached to the use of these data, available and accessible internationally.
    c. Legal conformity: paying due attention, in the design of access regimes for digital research data, to national legal requirements concerning national security, privacy and trade secrets.
    d. 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.
    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: describing 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.
    h. Efficiency: promoting further cost effectiveness within the global science system by describing good practices in data management 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.

60. 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.

61. 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:

62. To create an interoperable digital health ecosystem that facilitates secure data exchange while safeguarding patient privacy, States require clear review and approval procedures; a risk-based approach to access to health and streamlined approval processes that involve multiple organisations.
63. States shall implement the following to ensure access to health data for reuse for secondary purposes:
    a. Concrete improvements to privacy and transparency, rather than relying on communication efforts, as 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:

64. States shall establish clear obligations for the proactive disclosure of environmental data, consistent with continental and regional frameworks and natural resource governance instruments.
65. 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 mitigation measures, ensuring that communities and stakeholders have timely access to information that affects their rights, livelihoods, and environments.

Private Data in the Public Interest:

66. 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.
67. 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.
68. 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.

69. 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.
70. State measures should promote transparency in all data-sharing collaborations, including the data used and the impact of the collaboration.
71. 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:

72. 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.

Elections Data:

73. Elections bodies shall establish and enforce an agreed set of principles to promote integrity in public information, which can set clear standards and expectations for the behaviour of political parties, candidates and even media outlets, in the creation, dissemination and management of information.
74. Elections bodies shall develop and implement measures to elevate accurate information and official information sources on digital platforms, as well as countering disinformation and other content that violates platform policy and threatens the electoral process or the reputation of the election bodies and their officials.
75. Election bodies shall establish standardised frameworks for safeguarding information integrity, including developing joint public campaigns and shaping policies for responsible information dissemination, including the establishment of efficient channels for information exchange among stakeholders, allowing for the sharing of disinformation trends, effective countermeasures and public sentiment insights - for a timely and cohesive response to disinformation campaigns.
76. 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 information on the content regulation processes.
77. Elections bodies shall facilitate effective relationships between the election body, elections monitoring organisations, civil society, other electoral stakeholders and digital platforms and adequate policies and processes to enable rapid access to elections data during the electoral period and timely responses to threats to information integrity or disinformation.
78. States need to promulgate stronger national legislative obligations on data controller monopolies such that they are obliged by law to provide:
    a. Access to election data
    b. Human rights impact assessments
    c. Election plans
    d. Cooperation agreements between election bodies, civil society and fact checkers .

F4: Institutional Measures for Public Bodies

Proactive disclosure

79. Public bodies shall be required, even in the absence of a specific request, to proactively publish data of public interest, including information about their functions, powers, structure, officials, decisions, budgets, expenditure and other information relating to their activities.
80. Where private bodies conduct activities on behalf of public bodies, and for which public funds are utilised or public functions or services are performed, public bodies shall require such private bodies to proactively publish data emanating from such activities in the public interest; or facilitate publication of such data in the public interest.
81. Data proactively published (disclosed) shall be accessible and reusable across media, including digital media in accordance with internationally accepted open data standards.

Prioritisation Releasing High-Value Datasets

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

Standardised and Open Formats

84. 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

85. Public bodies must be transparent about the conditions for data reuse. This includes publishing the standard licence or other open licence and making information about available data, including metadata, easily discoverable online.

Fair and Non-Discriminatory Access

86. Public sector bodies 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.

Marginal Cost Charging

87. Public sector data should be available free of charge. In cases where charges are applied, they are generally limited to the marginal costs incurred for reproduction and dissemination.

National Statistical Offices

88. The role of National Statistical Offices (NSO's) of States shall advance from a data collector to a central data steward and coordinator in an Integrated National Data Management Framework.
89. The NSO shall work with Data Intermediaries 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.
90. The NSO shall set and maintain standards for data collection, processing, and dissemination and take responsibility for skills development in public bodies for implementing data standards, to ensure data from different sources are consistent, coherent, and can be integrated effectively.
91. The NSO 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.
92. 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.

93. 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.
94. The NSO as a 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.
95. For the purposes of implementing the National Integrated Data Management Framework, the NSO shall ensure:
    a. adequate human capital, meaning people with the right skills to use data, safeguard them, design policies, and hold power to account in the NSO and in public bodies.
    b. trust across stakeholders to uphold the social contract for data to maximise value and prevent misuse.
    c. funding for data production, exchange, and use, including funding for the data infrastructure.
    d. adequate incentives for public bodies to produce, protect, and share data, valuing data transparency.
    e. adequate measures to ensure data demand and a culture of data reuse.

National Data Advisory Council

96. 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, the National Statistics Offices and oversee the implementation of legislative and institutional measures for access to data.
97. The Council could consult experts and develop research and guidance on data ethics, balancing data availability with privacy, ensuring trust and transparency, promoting technical best practices, international and regional developments and public-private partnerships to facilitate access to data.
98. The composition of the Council shall be defined in these Guidelines. In addition to its advisory role to national government, the Information Commission, and the National Statistics Offices, membership shall include representatives from these organs of state, as well as from relevant private sector actors. 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 within its jurisdiction.
99. The Council shall ensure multistakeholder participation in all data policy, technical, institutional, and legal measures.

Judiciary

100. Recognising that the public availability of judicial decisions is an important element of open justice and helps foster transparency of the judicial process while ensuring the need for public scrutiny in a democratic society, the State Justice authorities shall promote data sharing and access to data through timeous publication of judicial decisions in open formats.
101. In judicial decisions, to balance the right to personal data protection and the right to access to data on judicial decisions, the justice authorities shall apply the proportionality test 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 interference 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).

Information Commission

102. An independent and impartial oversight mechanism such as an Information Commission shall be established by law to monitor, promote and protect the right of access to information and resolve disputes on access to information.
103. The independence of the Information Commission shall 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.
104. 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.
105. The Information 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 willfully refuse to comply.
106. The Information 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 confidentiality, integrity, and availability of data (data security).
    a. To this effect, the Information Commission should promote the adoption of impact assessments and audits as well as responsible stewardship for data sharing within organisations, and appropriate human resource policies that clearly assign roles and data governance responsibilities, install consultation mechanisms, promote awareness and a culture of confidence, and avoid undue risk aversion.

F5: Exemptions and Safeguards

Exemptions

107. 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.
108. 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.
109. Laws governing classification of information shall stipulate the maximum period of the classification and restrict classification only to the extent necessary, never indefinitely.
110. 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.

111. These Guidelines acknowledge that personal information protected under personal data legislation are not open by default and the right to access data must be balanced with fundamental rights to privacy.
112. These Guidelines acknowledge intellectual property rights of third parties but prohibits public sector bodies from using the sui generis database right to prevent or restrict the reuse of documents beyond the limits set out in national laws.

Safeguards

113. Public bodies shall, in accordance with national law, ensure the following safeguards for access or reuse of public data:
114. 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 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;
115. Public bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure 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.

F6: Enforcement

Compliance and Audits

116. Both public and private bodies should be encouraged to undergo regular information audits tied to reporting and governance processes to strengthen proactive disclosure practices. As part of this process, institutions can be encouraged 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.

Sanctions and Appeals

117. States shall adopt policy, regulatory, or administrative measures to address failures to comply with proactive disclosure obligations or with requests for information. Such measures shall provide for:
    a. The wilful or negligent destruction, damage, alteration, concealment or falsification of information and the obstruction or interference with the performance of the duties of an information holder or of an oversight mechanism, should be recognised as a serious infraction subject to appropriate remedial action 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 disclosure may be sanctioned in accordance with institutional, regulatory frameworks, administrative or governance frameworks.

c. Any refusal to disclose information 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. An independent oversight mechanism may be established to review appeals where necessary, within a maximum of 90 days.

e. Appeal and review decisions should be communicated in clear and accessible formats, without administrative fees, and applicants should retain the right to seek recourse through judicial or other independent bodies in line with national procedures.

F7: Ethical Data Governance and AI

118. States shall mandate the use of ethical principles in data collection and usage by all public institutions. These principles must be aligned with international human rights standards, promoting fairness, non-discrimination, and public good.
119. States shall implement a requirement for human rights impact assessments and fairness audits for all AI systems used in public service delivery or governance. This is essential to identify and mitigate biases that could exacerbate structural inequalities and discrimination.
120. States shall mandate all public bodies to provide clear and understandable explanations for decisions made by AI or automated systems, especially when those decisions affect a citizen's rights or welfare.

Section G: Implementation

121. States shall adopt legislative, administrative, judicial and other measures to give effect to this Guideline and facilitate its dissemination.
122. 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 this Resolution 620.
123. 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. 4. 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 this Declaration
124. These Guidelines are designed to be implemented through a multi-stakeholder approach, ensuring the meaningful participation of government private sector, civil society,academia, the technical community and affected communities in the design, implementation and oversight of policies and practices.
125. States should collaborate with civil society, 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 with their mandate to develop normative standards, providing invaluable national insights to inform this critical pan-African work to ensure that data serves as a powerful force for justice, inclusion, and transparency across the African continent.
126. States shall develop and implement national data literacy and digital skills programs for the public to empower them to understand their data rights, navigate online information, and critically evaluate data-driven narratives.
127. 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.
128. 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.
129. 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.
130. The Special Rapporteur shall endeavour reviews of data access frameworks and encourage 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.

Appendix A: Acknowledgements

[.....]

Appendix B: Drafting Process

Resolution 620 explicitly mandates 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."

Resolution 620 calls for the Special Rapporteur to consult broadly, actively seeking input from a wide range of parties, including civil society organisations, regulatory bodies, technology companies, media organisations and journalists, and academics. This ensures that the final guidelines are grounded in diverse perspectives and are relevant to the varied contexts across Africa.

The consultation process allows for direct input from organisations and individuals to provide their views and experiences on data access and governance.

The drafting and consultation process included:

[...]

The outcome is these Guidelines that will be a valuable tool for a range of diverse access to data stakeholders, including particularly African Union Member States.