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

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

Contents

FOREWORD

These Guidelines are issued by the African Commission on Human and Peoples' Rights (the African Commission) pursuant to Resolution 620 on "Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age," adopted by the African Commission during its 81st Ordinary Session.

Resolution 620 recognises that in the digital age, data is not merely a resource to be managed but a precondition for the realisation of human rights and the achievement of sustainable development. The Resolution calls on state parties to adopt measures that ensure access to data held by both public and relevant private actors to the end of advancing human rights and sustainable development. The Resolution mandates the Special Rapporteur on Freedom of Expression and Access to Information in Africa to consult broadly across the continent and to develop appropriate normative standards to guide data collection, deployment, and access. These Guidelines are issued in fulfilment of that mandate.

The Guidelines are the product of extensive consultations with stakeholders including public and private sector actors, civil society organisations, digital rights advocates and researchers across the continent. The Guidelines reflect the

diversity of African experiences and the shared commitment to ensuring that the digital transformation serves the enjoyment of human rights and development.

The purpose of the Guidelines is to elaborate policy, legal and institutional measures, responding to a context in which:

- Existing access to information frameworks, while essential, do not adequately address the distinct implementational challenges posed by the volume, complexity, and proprietary nature of data, as well as the private sector's predominance in control and access to data;
- Without adequate transparency, oversight, or avenues for redress, data-driven Artificial intelligence, algorithmic systems, and automated decision-making can significantly harm human rights;
- Cross-border data flows, including the dominance of trans-national technology companies in data processing and storage, raise particular challenges for enforcement of domestic legal frameworks;
- Unequal access to digital infrastructure, connectivity, and digital literacy - across and within African states - exacerbates existing inequalities and excludes marginalized communities from the benefits of data-driven governance and development;
- Women and girls, persons with disabilities, youth, indigenous peoples, rural communities, and other marginalised groups face heightened risks of data-related harms and encounter unique barriers to accessing data essential for the realisation of their rights;
- Data protection and privacy laws, while essential, have at times been used to block legitimate access to data of public interest, thereby obstructing transparency, accountability, and the right to information;
- Many African states could benefit from having effective and independent oversight institutions with the authority to adjudicate data access, order remedies, and ensure compliance with access obligations.

In this context, the Guidelines provide measures that together will serve to promote and harness data access as a tool for advancing human rights and sustainable development in the digital age. They constitute a soft law instrument that offers an authoritative interpretation of the obligations of state parties under the African Charter, particularly for Articles 9 (right to receive information), and 22 (right to development). They are informed by the Commission's existing jurisprudence on access to information, privacy, democracy, development and digital rights. The Guidelines are intended to support:

- State parties: as a blueprint for legislative, policy and institutional reform, as well as a benchmark for compliance with African Charter obligations;
- The judiciary and quasi-judicial bodies: as an interpretive aid in adjudicating disputes involving access to data;
- For national human rights institutions and civil society: as a framework for monitoring, advocacy, and accountability;
- For private sector actors: as guidance on best practices for transparency, accountability, and responsible data governance;
- For regional and subregional institutions: as a reference for aligning digital governance instruments with human rights standards, and developing cross-country African approaches.

The right to access data is not a luxury to be deferred. It is fundamental for human dignity, democratic governance, and the collective pursuit of a just and prosperous Africa. Let us ensure that data access is fashioned to ensure that digital transformation leaves no one behind.

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

PREAMBLE

Affirming its mandate pursuant to Article 45 of the African Charter on Human and Peoples' Rights (the African Charter), including the authority to formulate and lay down principles and rules upon which African States may base their legislation;
Recalling Resolution 620, "Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age" which recognises the importance of data in advancing human rights and sustainable development and which mandates the Special Rapporteur on Freedom of Expression and Access to Information in Africa to develop appropriate normative standards accordingly;
Recalling Article 9 of the African Charter, which guarantees every individual the right of access to information, and additionally recognising that, in the digital age, this right incorporates access to data;
Recalling Article 22 of the African Charter, which affirms the right to development, and additionally recognising that access to data is essential to the realisation of this right, including through enabling informed participation in development planning, decision-making and economic opportunity;
Further recalling that the rights enshrined in the African Charter are indivisible, interdependent, and interrelated, and that access to data is needed for the effective enjoyment of civil, political, economic, social, and cultural rights;
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;
Recalling the Declaration of Principles on Freedom of Expression and Access to Information in Africa, the Model Law on Access to Information for Africa, and the Guidelines on Access to Information and Elections in Africa, as well as various other resolutions, which together establish the normative framework that underpins rights enjoyed through information ecosystems on the continent, including the rights to access to information, privacy and data protection, political participation and freedom of expression;
Recognising the African Union Convention on Cyber Security and Personal Data Protection and the African Union Data Policy Framework which provide important regional frameworks for data governance;
Affirming that access to data and the protection of personal data are complementary obligations, and that any limitation on access must be prescribed by law, pursue a legitimate aim, and be strictly necessary and proportionate in a democratic society;
Recalling further Resolution 473 on the need to undertake a study on human and peoples' rights and Artificial Intelligence (AI), robotics and other new and emerging technologies in Africa, which underscores the Commission's engagement with emerging technologies affecting access to data;
Noting the African Union's Digital Transformation Strategy for Africa (2020–2030) and Agenda 2063, for which access to data is foundational for inclusive development, innovation, and continental integration;
Recognising that human rights enshrined in the African Charter increasingly depend on access to data in the digital age;
Reaffirming that access to data for a public good can foster human rights and societal innovation, as well as help support progress towards achieving the right to development and the Sustainable Development Goals and *Agenda 2063: The Africa We Want*;
Concerned that despite the proliferation of data-driven technologies, there is no tailored guidance for African governments and private actors on promoting and harnessing data access as set out in Resolution 620

The African Commission on Human and Peoples' Rights meeting at its [...] Ordinary Session, held [...]
Adopts the African Guidelines on Access to Data, an instrument for promoting and harnessing data access as a tool for advancing human rights and sustainable development in the digital age.

DEFINITIONS

African Charter refers to the African Charter on Human and Peoples' Rights.

African Commission refers to the African Commission on Human and Peoples' Rights.

Anonymisation means a process of changing records so that they do not relate to an identified or identifiable natural person, or to a process of rendering personal data anonymous so that the data subject is not or no longer identifiable.

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 their training models and subsequent applications such as real-time inferences and generative outputs.

Data encompasses the representation in electronic form of information at a granular level, with potential for conversion into higher-level meaning. It typically comprises 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). Information itself may be treated as data for further knowledge conversion operations.

Dataset means a collection of data, and is typically organised as tables, arrays or specific formats, such as CSV or JSON for easy retrieval and analysis. Datasets are essential for data analysis, machine learning, AI and other applications that require reliable, accessible data. With generative AI, datasets can also be constituted from unstructured data, thereby expanding how data can be organised and utilised as a resource.

Data access refers to the legal right or technical ability to retrieve, view, use, move, or manipulate data as part of the wider right to information, including from public body and private body data holders, and is enabled by availability, integrity and usability of such data. Access may be achieved by downloads of data or by processing data elsewhere, including on site, with the option of saving the results of such processing.

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, data access and sharing arrangements according to their different roles, responsibilities and rights, technologies, and business models. State capacity and engagement is needed in order to promote access to this ecosystem and ensure that human rights and national sovereignty are not eroded.

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

Data intermediaries means entities active in data access and sharing arrangements which facilitate data access and/or data sharing or the commercial exchange of data.

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

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 a data intermediary and may take place under diverse licence conditions.

Data subject means an identifiable natural person or identifiable group to whom data relates, including communities under customary or national law, and who have the right of consent to collection, processing and distribution of their data.

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

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 because of the number of potential beneficiaries of the value-added services and applications based on those datasets.

Information includes any original or copy of documentary material irrespective of its physical characteristics, such as records, correspondence, fact, opinion, advice, advertisement, 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.

Information integrity means the accuracy, consistency and reliability of information content, processes and systems to maintain a trustworthy information ecosystem, and is fundamentally enabled by the underlying integrity of data.

Interoperability means the ease of technical possibility for 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 descriptive information about 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 re-use.

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.

Personal data means information relating to an identified or identifiable a 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 factors specific to an individual's physical, legal, physiological, mental, economic, cultural or social identity.

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.

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 juristic person or any successor in title; but excludes public bodies and relevant private bodies.

Proactive disclosure refers to a regular flow of information by routinely providing information to the public without the need for people to make a request.

Public authorities mean juristic persons, legislative bodies and judicial authorities, insofar as they perform administrative functions, as defined by national law.

Public body means 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. Such benefits are 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 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.

Publish means to make available in a form and manner that is easily accessible to the public and includes providing copies or making information available through broadcast and electronic means of communication.

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.

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.

Sui generis rights in intellectual property terms means the application in specific jurisdictions of unique rights for specific categories of intellectual property, such as database protection where the database does not give rise to rights under traditional intellectual property laws such as patent or copyright law.

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.

KEY PRINCIPLES

These Guidelines are directly informed by Resolution 620 which recognises that data access forms an essential part of the right to information and is vital as a tool for human rights, democracy and sustainable development. The measures set out below draw on the following principles, informed directly by the Commission's resolution:

Data as a Strategic Asset: Data is a strategic public asset with the transformative potential to be used in the public interest, for public value, to promote democracy, good governance, and in furtherance of internationally and African agreed development goals. Data should therefore serve to support policies, services, or interventions that improve societal well-being, transparency, and accountability.

Data Access by Design: Systems for data collection, storage, and dissemination must be built with proactive disclosure features, accessibility standards, interoperability and security provisions by default.

Proactive Disclosure: Access without the need for active requests should apply, at a minimum, to key datasets of public interest such as budgets, procurement, health, education, and environmental data, and be made available in open, reusable formats.

Maximum Disclosure: The principle of maximum disclosure should be the default for all public data and for relevant private bodies' data. Disclosure should be presumed unless demonstrably harmful. Restrictions on access must be a narrow exception, strictly justified by international human rights standards.

Data Justice and Equity: Individuals have the right to meaningful information about the provenance, logic, significance, consequences, and categories of data involved in automated decision-making that affects their rights, and they have the right to challenge decisions based solely on automated processing and call for a human review. Furthermore, data initiatives must be designed to address structural inequalities and ensure that marginalised and vulnerable communities have equitable access to data, its governance, and the benefits derived from its use.

Data Integrity and Information Integrity: To be meaningful, the right of access to data requires that the data exhibits integrity in regard to accuracy, consistency and reliability of processes and systems, and this further underpins Information Integrity and a trustworthy information ecosystem.

Data Access and Protection Complementarity: Access to data and the protection of personal data are complementary obligations. Neither should be pursued to the exclusion of the other. Data protection frameworks must include exceptions for legitimate access to data of public interest, and access frameworks must incorporate safeguards to protect personal data from misuse, discrimination, and unlawful surveillance.

Transparency, Accountability, and Ethics: Data collection, processing, and use must be transparent and accountable. Ethical principles must be embedded in all data initiatives, with mechanisms to address biases in data and automated decision-making. Further, data is an indispensable tool for accountability and must therefore be accessible to journalists and researchers for matters of public interest, holding power to account, and fostering a well-informed public discourse.

Private Sector Accountability: State parties have a positive duty to regulate private actors whose data practices impact upon the enjoyment of human rights. These Guidelines extend to data held by private entities where such data is necessary for the exercise of human rights, is of significant public interest, in addition to the case of relevant private entities defined above. Legal frameworks imposing transparency, accountability, and access obligations need to encompass private sector actors where data is implicated in harms and benefits to human rights.

Effective Remedies: Any person who's right to access data is denied should have the right to an effective remedy before an independent body that has the power to order disclosure, impose sanctions, and award appropriate redress.

MEASURES

General Measures

To ensure a robust, coherent framework for data governance that gives adequate attention to access issues and aligns with regional and international standards, the following guidance sets out 12 steps to would need to be taken:

1. 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.
2. Combine a whole-of-government approach to data frameworks to enable effective policy coordination and comprehensive multi-stakeholder participation.
3. Create or strengthen a National Integrated Data Management Framework (elaborated below) that fosters the production of, and access to, data that is relevant to human rights and development, and which fosters the equitable and safe flow of data between government, individuals, civil society, academia, and the private sector, while safeguarding against data security breaches as well as forms of extraction and processing that violate human rights.
4. Develop and implement a national Open Data Policy that mandates public institutions, and bodies receiving public funds, to proactively make data publicly available.
5. Standardise access processes for public and private data requests including consistent justification requirements for cases of non-disclosure.
6. Ensure that data holders and data processors must obtain informed consent where required, limit data use to defined purposes, and respect data subjects' rights to access, correction, and deletion.
7. Establish a clear legal framework that narrowly defines the circumstances under which public sector bodies and other stakeholders may gain access to data held by private bodies in situations of genuine and demonstrable overriding public interest (such as 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.
8. 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 related rights.
9. Prioritise storage of open government data within national or regional data centres to promote sovereignty.
10. Promote access to data about the extent of environmentally sustainable data practices such as energy sources for data centres and the management, recycling, and disposal of electronic waste.
11. Take actions to ensure data access for the purpose of assessing whether datasets used for AI and algorithmic decision-making are representative, validated for accuracy, and monitored for bias, and assess data provenance and usage constraints.
12. Co-operate on an African regional and sub-regional basis to develop common cross-country approaches to securing access to data collected and held by transnational private sector actors.

Legal, Policy and Programmatic Measures

To align with a human rights-compliant legal framework on data access, corresponding measures will ensure that:

13. Existing legislation and regulation are interpreted to encompass data:

a. Access to information dispensations be expressly understood to encompass "data" and "datasets" as forms of information subject to the right of access, with applicable provisions on proactive disclosure, formats, denial of access, oversight and enforcement.
b. Any conflicting provisions in existing legal rules (e.g., Official Secrets Acts, cybersecurity laws) which may unnecessarily impact on access to data can be identified and addressed.

14. The right of access to data is encoded:

As a component of the right of access to information that is guaranteed by law, access to data should be covered by the following principles in current or new legal provisions:

a. Every person shall have the right to access data held by public bodies and relevant private bodies expeditiously and inexpensively.
b. Every person shall have the right to access data of other private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.
c. The right of access to data shall be guided by the principles of proactive disclosure and maximum disclosure, limited by narrowly defined exemptions, which shall be provided by law and shall comply strictly with international human rights law and standards.
d. Legal measures governing consent shall include clear opt-in and opt-out rights that cover collection, processing and access, such that that individuals maintain meaningful control over their personal data.
e. Data should be openly available, easily discoverable, accessible, used, shared and disseminated by anyone for any purpose that is not circumscribed by narrow exemptions.
f. Cross-border transfers of data need to comply with national data protection laws and international agreements to ensure equivalent protection.
g. Where access to data serves an overriding public interest (e.g., health, environment, elections, disaster response, countering gender-based violence), disclosure obligations should be absolute.
h. Legal provisions are needed to provide for remedy in the face of refusal to provide access to data, such as through specifying administrative review by an oversight body or ombudsperson, as well as through the option of judicial appeal.

15. Disclosures in the public interest are protected:

a. 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.

16. There is a duty to create, keep, organise and maintain data:

a. Legal prescriptions are needed in order to require that public bodies and relevant private bodies create, keep, organise and maintain data in a manner that facilitates data integrity and supports the exercise of the right of access.
b. Data retention should align with proportionality principles, and long-term datasets critical to rights and development (e.g. population, environment, public archives) kept beyond routine administrative timelines.
c. Public and relevant private bodies need to be required to maintain and publish catalogues of the datasets they hold, with metadata and use conditions clearly indicated.

17. Public value is at the core of data access:

a. To materialise public value, there is need for inclusive involvement of relevant stakeholders in the data ecosystem – including vulnerable, underrepresented, or marginalised groups – during the design, implementation, and monitoring of data governance frameworks including around data access provisions.
b. Transparency of data access and sharing arrangements is necessary to encourage the adoption of responsible data governance practices throughout the data value cycle, including in regard to compliance with codes of conduct, ethical principles and privacy and data protection regulations.
c. Where personal data is involved, there is a need for compliance 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.
d. There is value in encouraging and facilitating innovative data sharing models, including but not limited to data donations and data pools, including involving researchers, data scientists and journalists.

18. Data markets are competitive and operate for all:

a. Competitive markets for data require sound competition policy and regulation that addresses possible exploitation of market dominance, and provides for enforcement and redress mechanisms that increase stakeholders' agency and control so as to ensure adequate protection of consumers, intellectual property claims, legitimate security interests, privacy and personal data protection.
b. Governance needs to 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.
c. In facilitating data sharing between public and private sectors, necessary steps need to be taken in order to avoid conflicts of interest, including ensuring that:
    i. Public bodies do not grant exclusive data access that undermines fair competition, but treat all market participants on fair, reasonable, and non-discriminatory terms, balanced with consideration of tiered access and partnership regimes in order to spread value beyond the most well-resourced entities and bring about inclusive benefit;
    ii. Public-private, and private-private, partnerships do not result in the capture of public data for private commercial advantage at the expense of broad-based public access.
d. States may develop sector-specific competition guidance for distinctive data markets, particularly in areas such as digital platforms and online intermediaries; advertising; telecommunications and connectivity services; financial services and fintech; health data and digital health services; and agricultural data and agritech.

19. Data use is enabled:

a. There is a need to foster the findability, accessibility, interoperability and reusability of data across organisations, including within and across the public and private sectors. In particular, this calls for efforts to ensure that:
    i. Data is provided together with any required meta-data, documentation, data models and algorithms, offered in a transparent and timely manner, and supported by appropriate data access control mechanisms, including application programming interfaces (APIs);
    ii. 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 and open formats.
b. Data governance frameworks provide for include public programmes to increase awareness about the benefits of open and interoperable data access.

20. Procedures are in place for requests to access data:

a. Where access to data is subject to a request:

i. Access should be granted as expeditiously as possible, and within timelines established by national law (not exceeding 30 days for standard requests, subject to limited extension in justified circumstances).
ii. Access should be provided inexpensively, with fees limited to marginal costs of reproduction and dissemination where applicable. Access to user-generated data and data of significant public interest should be free of charge.
iii. Data should be provided in open, interoperable, machine-readable formats including, where appropriate, formats accessible to persons with disabilities.
iv. No requester should be required to demonstrate a specific legal or personal interest in the data requested or to provide justification for a request, unless otherwise provided by law for specific categories of sensitive data.
v. Requesters are entitled to help in making requests orally or in writing, with appropriate support provided to non-literate persons and persons with disabilities to make requests on an equal basis with others.
vi. Any refusal to disclose data should be provided timeously and in writing, should be well-reasoned, and should be premised on international law and standards. The refusal should specify the applicable exemption, the harm that disclosure would cause, and the public interest considerations weighed.

b. For data made available through automated means, including application programming interfaces (APIs), portals, or real-time feeds, the following guidance applies:
i. Access mechanisms should be clearly documented, publicly available, and supported by technical assistance where appropriate.
ii. Access should not be subject to unreasonable technical barriers, proprietary lock-in, or unfair discriminatory terms.
iii. Users should have the right to access data through APIs without being required to provide justification for the purpose of access, except where necessary to prevent violations of rights or protect security.

c. Where data is dynamic or subject to frequent updates (including sensor data, real-time monitoring data, or streaming data), access mechanisms should enable timely retrieval. States and relevant private bodies should ensure that dynamic data of significant public interest (for instance, environmental monitoring, public health data, disaster response data) is accessible in real time or near real time where technically feasible.

d. Procedures for access should distinguish between:
i. Whole datasets, where access to entire datasets is requested, procedures should facilitate bulk download or API access.
ii. Granular or specific data, where access to only specific data records is requested or granted, procedures should enable precise retrieval without requiring access to the entire dataset.

e. States may establish standardised request procedures, including online portals and electronic forms, to streamline access. Such procedures should not create undue barriers and should provide alternatives for individuals lacking internet access or digital literacy.

f. Any denial, delay, or partial disclosure of data should be subject to appeal before an independent oversight body designated under these Guidelines (see Appendix C). The oversight body may order disclosure, impose timelines, or award remedies.

Exemptions and Safeguards

21. Exemptions

a. Data 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 data may only be withheld for the period over which the harm could occur.

b. Where a portion of a dataset containing requested data is exempted from disclosure, the exempted portion should be severed or redacted and access granted to the remainder of the dataset.
c. Laws governing classification of data should stipulate the maximum period of the classification, and restrict classification only to the extent necessary, never indefinitely.
d. In general, data may only be legitimately withheld as an exemption if its release would:
    i. Result in the unreasonable disclosure of the personal information of a third party;
    ii. Cause substantial prejudice to a legitimate commercial or financial interest of relevant stakeholders or other third party;
    iii. Endanger the life, health or safety of an individual;
    iv. Cause substantial prejudice to the national security and defence of the State;
    v. Cause substantial prejudice to international relations where the data 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;
    vi. Cause prejudice to law enforcement, in particular, the prevention and detection of crime, apprehension or prosecution of offenders and the administration of justice;
    vii. 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
    viii. Jeopardise the integrity of a professional examination or recruitment process.
e. Data-specific exemptions: In addition to the exemptions above, data may be withheld where:
    i. Disclosure of anonymised data would create a significant risk of re-identification of individuals or groups, and such risk cannot be adequately mitigated through technical or organisational measures.
    ii. Disclosure of algorithms, source code, or proprietary models would substantially compromise the integrity, security, or functioning of algorithmic systems, provided that such withholding does not prevent meaningful accountability for decisions affecting individual rights.
    iii. Disclosure of technical specifications, access protocols, or security measures would create a substantial risk of unauthorised access, manipulation, or harm to data processing systems.
    iv. Disclosure would violate intellectual property rights protected under national law, provided that such rights are not used to prevent legitimate access to data of public interest or to frustrate the right to access user-generated data.
f. The exemptions set out in the sections above should be interpreted narrowly. Where the public interest in disclosure outweighs the harm to the protected interest, the data should be disclosed.

22. Safeguards

Public bodies are expected to operate safeguards for access or reuse of public data, according to which:

a. Access is granted only where the public sector body or the competent body, following the request, has ensured that data has been anonymised in the case of personal data.
b. For cases of commercially confidential information, including trade secrets or content protected by intellectual property, access may depend upon the data being modified, aggregated or treated by other methods of disclosure control.
c. Public bodies should impose conditions that preserve data integrity, retaining a right to verify the process, the means and results of processing of data undertaken by the re-user, and also retaining the right to limit the use of results of processing that prejudice the rights and interests of the public body or third parties without overriding public interest.

d. In alignment with the African Union Convention on Preventing and Combating Corruption, there should be protections against retaliation, as well as guarantees of anonymity and legal immunity in respect of good-faith disclosures by whistleblowers alerting about data management practices that arbitrarily restrict data access rights.

Safeguards for Private Actors:

a. Private actors subject to access obligations under these Guidelines shall, in accordance with national law, ensure the following safeguards:
    i. Access for re-use of data shall be granted only where the private actor has ensured that personal data has been anonymised, unless access is for a public interest purpose that requires personal data;
    ii. Commercially confidential information, including trade secrets or intellectual property, shall be modified, aggregated, or treated by any other method of disclosure control, unless disclosure is required by overriding public interest;
    iii. Where access is provided through a secure processing environment, the private actor shall maintain the integrity and security of the environment and retain the right to verify the process, means, and results of processing undertaken by the re-user;
    iv. Any conditions imposed on access or re-use shall be publicly available, clearly stated, and applied in a non-discriminatory manner.

b. Private actors shall include contractual or other legally binding conditions prohibiting re-users from using accessed data for:
    i. Unlawful surveillance or discrimination;
    ii. Violation of privacy or data protection rights;
    iii. Harassment;
    iv. Any purpose that would violate international human rights law.

Enforcement

23. Responsibility:

The designated oversight body, preferably the Information Commission or equivalent (see Appendix C), shall be responsible for enforcing these Guidelines, thus monitoring compliance, investigating violations, and issuing directives.

24. Compliance and Audits

a. Oversight should promote, and may require, public and private bodies to conduct regular audits to strengthen proactive data 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.
b. The oversight authority shall conduct regular audits and inspections to ensure adherence to data management, disclosure, and ethical standards.

25. Sanctions and Appeals

26. States should adopt policy, regulatory, or administrative measures to address failures to comply with proactive disclosure obligations or with requests for data. Such measures should respond to:

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, recognising these acts as infractions 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 have systematically obstructed disclosure may be sanctioned in accordance with regulatory frameworks. An independent oversight body shall be entitled to publish reports on patterns of failure to meet proactive disclosure duties or systematic obstructed disclosures and the sanctions applicable.

27. Measures shall be proportionate and subject to the following tiered framework:
    a. Tier 1: Transparency – The independent oversight body shall issue a public report identifying the nature and extent of the non-compliance and recommending corrective actions.
    b. Tier 2: Corrective action – The entity shall be given a reasonable period, not less than 90 days, to remedy the non-compliance. The oversight body may provide technical assistance to facilitate compliance.
    c. Tier 3: Civil remedies – Affected individuals, civil society organizations, and national human rights institutions shall have standing to seek injunctive relief, damages, or declaratory relief before an independent court or tribunal for harms arising from non-compliance.
    d. Tier 4: Judicial sanctions – Where non-compliance is persistent, egregious, and unremedied after the exhaustion of Tiers 1–3, proportionate sanctions may be imposed, but only:
        i. By order of an independent and impartial court or tribunal;
        ii. Following a finding of persistent, egregious, and unremedied non-compliance;
        iii. With the sanction proportionate to the nature and gravity of the violation.
    e. Conditions:
        i. Administrative authorities shall not have the power to impose financial sanctions, license revocations, operational restrictions, or platform bans without prior independent judicial authorization.
    f. Accountability measures under this section shall not be used for:
        i. Political victimisation;
        ii. Arbitrary censorship of freedom of expression;
        iii. Economic coercion;
        iv. Surveillance or harassment of users, journalists, or human rights defenders.

28. Refusals:
    a. Applicants experiencing a refusal to disclose data should receive written reasons and be able to initiate an internal review, at no cost, within a reasonable period, for example within 30 to 45 days.
    b. Review of such appeals should occur within a maximum of 90 days and be communicated in clear and accessible formats. Applicants retain the right to seek additional recourse through judicial or other independent bodies in line with national procedures.
    c. Appeal and review decisions should be communicated in accessible formats, without administrative fees,
    d. Affected individuals, civil society organizations, and national human rights institutions shall have standing to seek recourse through judicial or other independent bodies such as injunctive relief, damages, or declaratory relief before an independent court or tribunal for harms arising from non-compliance.

ACCESS, ETHICS AND AI

Datasets used for AI must be accurate, representative, and securely managed, with safeguards to prevent unauthorized access, manipulation, or breaches. The public should have access to data on compliance with such ethical standards.

29. Recommended steps:

    a. AI systems used in public service delivery or governance should be required to exhibit human rights impact assessments which encompasses the data involved. This is essential to identify and mitigate data-related biases that could exacerbate structural inequalities and discrimination, and the public is entitled to access data about such assessments.
    b. AI service providers can be required to report 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. The public is entitled to access data in such reports.
    c. Data access rights can be extended to private actors, including digital platforms, whose use of artificial intelligence and automated decision-making systems has the potential to affect fundamental rights. For

digital platforms, required human rights impact assessments can include assessments of data and data access in regard to how content moderation, ranking, and recommendation systems impact on the rights access to information, privacy, freedom of expression, and non-discrimination. The public is entitled to access such assessments.

d. 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 access as well as data provenance, quality, representativeness and security.
e. Africa regional and sub-regional co-operation will support effective application of these standards at country-level.

IMPLEMENTATION

30. Operationalisation of these Guidelines will encompass several steps:

a. Legislative, administrative, judicial, budgeting and other measures need to be taken in order to give effect to these Guidelines and facilitate their dissemination.
b. This guidance is 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.
c. States can collaborate with civil society, media, academia, the private sector, and communities to design, implement, and monitor policies and practices on data, including in respect of data access. Furthermore, States can 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.
d. There is a need for national data literacy and digital skills programmes to empower the public to understand their data rights, and for regulators to assess data-driven online recommendation and content moderation systems as well as platform business models.
e. Continuous professional development is essential for civil servants in data governance, access, quality management, and ethical use to inform evidence-based decisions making.
f. Continued dedicated resources are needed to improve the quality, integrity, and completeness of public data across all sectors, since that poor data is a significant barrier to the value that is unlocked by public access to data.
g. States may adopt, and periodically apply, measurable performance indicators for the implementation of data access within data governance frameworks, developed through public consultation.
h. There should be periodic reviews of data access frameworks and enforcement, at least every three to five years, to adapt to technological changes and implementation experiences. The findings of such reviews should be made public and formally reported to parliament or an equivalent oversight body to ensure transparency and accountability.
i. In accordance with Article 62 of the African Charter, each Periodic Report submitted to the ACHPR, can provide detailed information on the measures taken to facilitate compliance with the provisions of these Guidelines.
j. The Special Rapporteur will encourage national reviews of data access frameworks and may engage in the development of further guidance and voluntary submissions of reports by States or institutions on implementation progress of Resolution 620.

APPENDIX A: MEASURES FOR SPECIFIC DATA

1. Selected Categories of Data:

a. Sensitive data needs to be encrypted, access-limited, and processed only for explicitly authorized purposes.
b. 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.
c. 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.
d. Sex-disaggregated data is essential to support gender equality, as per UN Women's Minimum Set of Gender Indicators.

2. Budget and Fiscal Data:

a. Requirements can provide for publication of machine-readable datasets on procurement, tax expenditures, and debt, in line with Open Budget Index and International Budget Partnership standards.

3. Research Data from Public Funding:

a. National policies and institutional measures can specify access regimes for research data from public funding in accordance with the following objectives and principles:
    i. 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
    ii. 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.
    iii. 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.
    iv. Legal conformity: paying due attention, in the design of access regimes for digital research data, to national legal requirements concerning national security and privacy.
    v. 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.
    vi. Interoperability: paying due attention to the relevant international standard requirements for use in multiple ways, in co-operation with international organisations.
    vii. 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.
    viii. Efficiency: advancing further cost effectiveness within the African and global science system by promoting good practices in data management, access and specialised support services.
    ix. Accountability: evaluating the performance of data access regimes to maximise the support for open access among the scientific community and society at large.
b. 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.

c. 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:

a. To create an interoperable digital health ecosystem that facilitates secure data exchange while safeguarding patient privacy. An opportunity and risk-based approach can inform clear review and approval procedures and streamlined approval processes that involve multiple organisations.
b. There is need to 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.
c. The following measures will ensure access to health data for reuse:
    i. Making concrete improvements to privacy and transparency, because public trust is crucial to obtaining patient data.
    ii. Establishing 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.
    iii. Creating an online library to provide data curation code, tests, and documentation to ensure access to well-curated data.
    iv. Developing 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 access decisions.
    v. Creating a common application for ethics, information guidance, and access permissions.

Environmental Data:

a. There should be 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.
b. Requirements are needed for 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.
c. It is essential to have provisions for real-time or near-real-time access to data concerning environmental hazards (e.g., pollution, deforestation).
d. Access to data is needed about data centres use of energy for storage and processing, as well as on the management, recycling and exposure of electronic waste.

Private Data in the Public Interest:

a. To unlock the value of data across the economy, there is a need for measures to ensure private sector data is appropriately available, accessible and usable for public interest purposes and across the economy, while protecting data rights and private sector's intellectual property.
b. Governance should ensure the availability of open and interoperable data standards for proactive disclosures by the private sector to enable data use in the public interest.
c. There is a need to foster awareness amongst private sector organisations of the societal benefits of proactive data disclosures and data sharing through regular engagements with the private sector.

d. States can explore incentives, such as public recognition programmes, to increase proactive disclosures of private sector data and sharing of data by the private sector on a voluntary basis.
e. Measures are needed to promote transparency in all data-sharing collaborations, including the data used and the impact of the collaboration.

Sector Guidance:

It is valuable to have self- or co-regulation mechanisms – including voluntary guidance, standards, codes of conduct and templates at the sector level for data access and sharing agreements.

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

a. Platforms shall commit to greater transparency regarding their data collection practices, algorithmic decision-making, and terms of service as related to data access.
b. African states can overcome disadvantages in power in relation to digital platforms by ensuring a pan-African approach to the governance of multi-national enterprises that are significant data holders, including co-operation to develop a continental Code of Conduct regarding stakeholder access to data in the public interest.
c. This Code of Conduct, adapted and regularly updated at the national level by the Information Commission (or equivalent), may include, but not be limited to, the following provisions:
    i. Such platforms shall commit to refraining from initiating, pursuing, or threatening legal action, 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 alternative access mechanisms are provided by the platform.
    ii. The platforms be mandated to actively develop and provide robust, secure, auditable, and non-discriminatory access mechanisms (e.g., APIs, data sharing agreements, sandboxed environments) for stakeholders seeking non-publicly accessible data or structured access to public-facing data. Such mechanisms should be reasonably priced (if applicable) for non-profit uses, and should offer timely access to real-time data.
    iii. Clear criteria are set out 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 aspects, and wider scientific understanding.
    iv. Such research must adhere to ethical guidelines, data protection laws, and standards of academic, journalistic or other professional integrity.
    v. Mechanisms exist 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 operated either the Information Regulator (or equivalent), National Statistical Office, or national research facility (or equivalent).

APPENDIX B: INSTITUTIONAL MEASURES

Proactive disclosure

1. Public bodies should 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.
2. 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 should 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.

Prioritisation Releasing High-Value Datasets

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

Open, Interoperable, Machine-Readable Formats

5. Public sector bodies should 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

6. 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

7. 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.

Data Access Policies

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

Marginal Cost Charging

9. 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.

APPENDIX C: INSTITUTIONAL ARCHITECTURE FOR DATA ACCESS

Independent oversight body:

An independent and impartial oversight mechanism, ideally an Information Commission (or hybrid or equivalent) established by law, has the mandate to monitor, promote and protect the right of access to information and data and to resolve disputes. This implies that:

a. 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 Information Commission requires adequate human capital, meaning people with up-to-date skills to use data, design policies and regulations.
b. Public bodies and relevant private bodies shall be required to recognise decisions of the Information Commission as legally binding in all matters relating to access to data, including resolving disputes.
c. The Information Commission's powers shall include the power to issue orders to public bodies, compelling them to release information, and options for punitive action against officials who refuse to comply.
d. The Information Commission shall accredit Data Intermediaries to facilitate compliance with data governance and access standards and a competitive market in data brokerage.
e. The Information Commission ensures that stakeholders are held accountable in taking responsibility, according to their roles, for the integrity of the data they make available and for the systematic implementation of risk management measures throughout the data value cycle, including measures to protect the security, confidentiality, quality, and availability of data. To this effect, the Information Commission will:

i. Promote the adoption of impact assessments and audits as well as responsible stewardship for data access.
ii. Oversee the adoption of public service standards (e.g., response times, appeals processes), install consultation mechanisms, create a culture of confidence in the civil service and discourage undue risk aversion on data disclosure.
iii. Clarify roles and responsibilities amongst data-holding agencies within public institutions, support related capacity building, resourcing and skills development, and promote partnerships to support these.
iv. Include within its functions the promotion of data literacy within the wider public as well as in the civil service curriculum.
v. Operate a mechanism for regular public reporting on the state of data openness and access requests, and provide transparency reports on its own functioning in adjudicating and promoting data access.

National Statistical Offices:

a. 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.
b. 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.
c. 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 interoperable.
d. 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.
e. For the purposes of implementing the National Integrated Data Management Framework, the NSO shall ensure:
    i. trust across stakeholders to uphold data to maximise public value while preventing misuse.
    ii. funding initiatives for data access and use, including funding for infrastructure and skills.
    iii. adequate incentives for public bodies to produce, protect, and share data.
    iv. adequate measures to ensure data demand capacity and a culture of data use.

National Data Advisory Council:

a. States may consider establishing a National Data Advisory Council or such other similar body, falling within the purview of the existing Information Commission or national data/information regulators. The Council shall help develop the National Integrated Data Management Framework, advise the national government, the Information Commission (or equivalent), the National Statistics Office and the national research institution/s. It should conduct monitoring and make recommendations.
b. 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 in the private sector, academia, the media and civil society.

Judiciary:

a. Judicial authorities promote open justice through enabling data sharing and access to data through timeous publication of judicial decisions in open formats, as well as proactive publishing of how persons are able to gain access to justice.
b. To balance the right of access to data with other rights and obligations, judicial decisions concerning access will align 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 excessive in relation to the objective).

Elections Management Bodies and Data:

a. Elections management bodies (EMBs) are urged to establish and enforce an agreed set of data principles that can help to promote electoral transparency, and set clear standards and expectations for political parties, candidates and media outlets, in regard to applicable data creation, management and access.
b. EMBs can develop and implement measures in order to elevate accurate data and official data sources on digital platforms.
c. These bodies can operate standardised frameworks for safeguarding electoral data integrity, responsible data dissemination and sharing of data about disinformation trends, effective countermeasures and public sentiment.
d. There should be ensure effective communication channels between online platforms and election stakeholders, and there should be algorithmic measures to prioritise access to accurate data about elections.
e. EMBs facilitate effective relationships with elections monitoring organisations, civil society, researchers, journalists and other electoral stakeholders and digital platforms to enable rapid access to elections data and timely responses to threats to data integrity and data-driven disinformation.
f. There is need for stronger national legislative obligations on platforms, including advertising platforms, which are major data holders, such that they are obliged by law to provide data on:
    i. Their human rights impact assessments in regard to elections
    ii. Their election risk-mitigation plans
    iii. Their cooperation agreements such as with election bodies, media, civil society and fact checkers.