Memorandum:

Summary of Windhoek Meeting and Submissions Received Post-Version 2 of the ACHPR Resolution 620 Guidelines

Purpose

This Memorandum summarises written submission received post version 2 of the Guidelines and the discussions held during the Windhoek consultation on the draft *Guidelines on Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age* (Resolution 620). It highlights key inputs, consensus areas, and how these have informed Version 3 of the Guidelines.

Submission 1: Information Regulator

The Information Regulator (South Africa) submitted a legal and institutional analysis on *the Resolution on Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age: Draft Guidelines* (September 2025). The submission drew from its mandate under the *Protection of Personal Information Act* (POPIA) and the *Promotion of Access to Information Act* (PAIA).

Definitions

- The Regulator recommended that terms such as *Anonymisation*, *Dynamic Data*, *Research Data*, and *High-value datasets* not be limited to "documents", but instead cover all data formats. The Regulator suggested deleting narrow examples in the *Public Interest* definition to better capture societal benefits like democracy, rule of law, and accountability.

Scope and Application

- The Regulator expressed concern that the Guidelines apply only to public bodies or private entities performing public functions or funded by public resources. It recommended extending the scope to all *natural and legal persons*, including the private sector and Big Tech, in line with the *horizontal application of rights*.

Measures

- General Measures (F1): Recommended allowing both *public and private bodies* to request access to data, subject to genuine public-interest tests, and replacing "judicial authorisation" with "judicial review."
- Legal Measures (F2): Suggested re-numbering for accuracy, ensuring consistency in the use of "data" rather than "information", and inserting a clause that personal data must be processed lawfully. It further proposed distinguishing between public and private data requests, requiring justification only where data is privately held.
- Specific Data (F3): Proposed adding *personal data protection* responsibilities for research institutions, removing restrictions that limit private data access to emergencies, and using *Election Management Bodies (EMBs)* instead of "Elections bodies."
- Institutional Measures (F4): Supported integrating the *National Data Advisory Council (NDAC)* within existing oversight institutions such as the Information Commission or Data Protection Authority. Recommended relocating the NDAC

section to follow that of the Information Commission and clarifying that the NDAC should operate at a *policy level* rather than as an operational data access point.

- Exemptions and Safeguards (F5): Called for consistent terminology ("data" vs "information"), clear legal bases for classification decisions, and correction of paragraph numbering.

Implementation

- The Regulator proposed pluralising "Guideline(s)" for consistency and adding a new clause requiring States to *resource access to information oversight authorities* adequately to fulfil their functions under these Guidelines.
- Overall, the submission reinforces the legal soundness and institutional coherence of the Guidelines. It also deepens their human-rights grounding and calls for clearer accountability obligations for private-sector actors in data governance.

Submission 2: SA Comm Conference

- Proposed *data-sharing models* such as *data donations* and *data pools.*
- Recommended *codes of conduct* for platforms to protect researchers engaging in public-interest data use.
- Requested clarification on *ownership of public archives* and differentiated access tiers. This has been integrated in *F3 (Research Data)* and *F4 (Institutional Measures).*

Submission 3: FIFAfrica,Windhoek

The Windhoek consultation convened around 20 participants with expertise in data governance, access to information, and digital rights. Participants were familiar with Version 2 and engaged in detailed discussions followed by presentation by members of the African Alliance for Access to Data (AAAD).

Main discussion points:

- *Transparency and Data Handling*: Participants proposed stronger transparency obligations. Version 3 introduces requirements for *transparent documentation of data processing and publication workflows* (F1).
- *Cybersecurity Safeguards*: Stakeholders called for clearer safeguards against data misuse. A new clause under *Ethical Data Governance and AI* (F7) now mandates *proportionate cybersecurity measures.*
- *Consent and User Rights*: Participants recommended explicit opt-in and opt-out mechanisms for individuals. Section F2 now provides *accessible and transparent opt-out rights.*
- *Data Localisation and Sovereignty*: Stakeholders supported *domestic or regional hosting of open government data* to advance African data sovereignty.
- *Cultural and Linguistic Data*: Cultural and linguistic data were recognised as *high-value datasets* (Definitions and F4).
- *Platform Accountability*: Section F7 now calls for *platform accountability mechanisms to prevent online gender-based violence.*
- *Environmental Sustainability*: F1 introduces *green data principles* and responsible e-waste management.
- *Performance and Consultation:* Section G requires *measurable indicators* and *public participation* in data-governance frameworks.

Participants reaffirmed that the Guidelines must remain strongly normative, rights-based, and framed in mandatory language ("shall"). They supported empowering existing national authorities rather than creating new oversight bodies

Additional Areas To Be Expanded at Implementation

- **Cybersecurity Standards for Data Access & Sharing**
  - Cybersecurity varies widely across states and is governed by separate national legislation; ACHPR cannot prescribe technical controls.
  - States should develop or update national cybersecurity frameworks governing secure data storage, transmission, encryption, incident response, and cross-border data exchange.

- **Sector-Specific Codes of Practice**
  - Feedback asked for individual sector annexes to the guidelines. Not added, because the Guidelines must remain cross-cutting.
  - Sector regulators should produce tailored codes, operating procedures, and technical standards aligned with the Guidelines.

- **Deepened GBV/Online Harms Provisions for Platform Accountability**
  - The Guidelines include general provisions on platform transparency. The feedback sought expanded gender-based violence online sections and detailed platform accountability frameworks.
  - This was not added to keep the Guidelines level-neutral. States may adopt more detailed policies through national digital rights frameworks.

- **Blockchain for Elections**
  - Some participants wanted blockchain for electoral data integrity. This was not included because of strong technical and human rights concerns and the technology may not be appropriate in high-risk centralised election systems.
  - States may explore appropriate technologies for election integrity.