

Written Submission on the Human Rights Implications of Data Centre and Digital Infrastructure Expansion in South Africa

The Association for Computing Machinery (ACM) welcomes the initiative of the South African Human Rights Commission (“the Commission”) in calling for public submissions on the human rights implications of the rapid expansion of data centres and digital infrastructure in South Africa. ACM is the world’s largest educational and scientific computing society, and its Technology Policy Council provides non-partisan, evidence-based technical expertise to policymakers worldwide. This submission is offered through this lens to assist the Commission in aligning data-centre governance with constitutional obligations, international human-rights standards and recognised best practice.

The growth of data centres in South Africa can advance the progressive realisation of socio-economic rights and support the country’s Artificial Intelligence (AI) ambition as it develops an AI national strategy and national AI policy to maximise the benefits of the AI economy. However, this infrastructure also utilises significant energy and water, as well as data-processing capacity, which are concentrated in the hands of a few largely foreign-owned operators. These features raise distinct human-rights questions that are worthy of further inquiry.

This submission is made by the ACM Africa Technology Policy Committee on behalf of the Technology Policy Council of ACM. It reflects ACM’s institutional expertise and published positions and does not purport to represent the views of any individual member.^{1,2,3}

The South African Context

South Africa is the most developed data-centre market in Africa, anchored in Johannesburg and Cape Town and driven by the arrival of global hyperscale cloud providers and large carrier-neutral operators and Africa Data Centres.⁴ Industry analysts project the need for an additional 700 data centres across Africa in addition to the already existing 150 centres concentrated in

¹ Bran Knowles. 2021. ACM TechBrief: Computing and Climate Change. Association for Computing Machinery, New York, NY, USA. Retrieved July 27, 2026 from <https://dl.acm.org/doi/book/10.1145/3483410>

² Philipp Hacker, Kai Ebert, Nicolas Alder, Vlad C. Coroamă, Ralf Herbrich, Bran Knowles, Lynn Kaack, and Alejandro Saucedo. 2025. Policy Brief on Powering Europe's Digital Transformation: A Roadmap to Greener Data Centers. Policy Brief. ACM Europe Technology Policy Committee. Retrieved from https://www.acm.org/binaries/content/assets/public-policy/europe-tpc/acm_data_center_final.pdf

³ Micah Altman, Aloni Cohen, and Kobbi Nissim. 2024. ACM TechBrief: Data Privacy Protection. Association for Computing Machinery, New York, NY, USA. Retrieved from <https://dl.acm.org/doi/book/10.1145/3679004>

⁴ Mordor Intelligence. [n.d.]. *South Africa Hyperscale Data Center Market*. Retrieved July 23, 2026 from <https://www.mordorintelligence.com/industry-reports/south-africa-hyperscale-data-center-market>

South Africa, Kenya and Nigeria to meet Africa's connectivity and data storage requirements.⁵ This growth raises real public-interest tensions.

Investments in data infrastructure will be judged against their potential socio-economic benefits, and thus must be contextually responsive. South Africa's 2024 National Data and Cloud policy (Policy) makes important policy interventions around digital infrastructure on a universal access basis and the availability of government data in data centres that enable data sharing and interoperability.⁶ The Policy recognises that the "absence of a regulatory environment might deter increased investment in digital technologies as investors largely seek regulatory certainty to ensure adequate protection of their investments. Connectivity and utilisation of technologies should be supported by a reliable energy supply."⁷ In addition, the Policy recognises that "data centres also rely significantly on cooling systems that require vast volumes of water. In addition to energy supply challenges, issues of sustainability are beginning to take centre stage. The implication for South Africa is that in its pursuit of reliable energy supply solutions, consideration should be given to ensuring that data centre providers ensure that they make self-provisioning for water and electricity while addressing carbon emission reductions to mitigate against environmental degradation."⁸

Equitable Access to Digital Infrastructure

Digital Infrastructure in the policy refers to the technological foundation that supports digital services, processes, and applications. It can include hardware, software, networks, and communication systems. Digital infrastructure is a strategic priority necessary to bridge the digital divide and to ensure universal and equitable access for all South Africans. According to the African Union (AU) Data Policy Framework, "data infrastructure that enables an integrated data system is a key strategic asset for countries, but the scale, extent and speed of change brought about by data-driven digital technologies make regulation complex and resource intensive."⁹

The core equity concern in the construction of data centres that can consume nationally scarce resources in energy and water while producing benefits in terms of compute capacity, jobs, connectivity, and taxes is whether publicly shared resources should subsidise private and often offshore value creation, which can widen rather than narrow existing inequalities. A rights-based

⁵Chido Muniyati. 2025. *Accelerating Digital Inclusion in Africa*. Brookings Institution. Retrieved July 23, 2026 from <https://www.brookings.edu/articles/accelerating-digital-inclusion-in-africa/>

⁶ Department of Communications and Digital Technologies, Republic of South Africa. 2024. *National Data and Cloud Policy*. Government Gazette No. 50741. Retrieved July 23, 2026 from https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf

⁷ National Data and Cloud Policy (see note 3), 8.

⁸ National Data and Cloud Policy (see note 3).

⁹ African Union. 2022. *AU Data Policy Framework*. Retrieved July 23, 2026 from <https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf>

framework should therefore ask whether data centres can measurably advance domestic digital inclusion, and how that benefit is secured and verified.

South Africa is fortunate, given that its policy ecosystem for AI is still developing. The South African Human Rights Commission can lead conversations with the state as an independent stakeholder on behalf of non-state actors to influence the design of the future AI policy and strategy for the government to:

1. Adopt a “digital-inclusion dividend” expectation by requiring large data centre approvals be accompanied by verifiable commitments to domestic digital inclusion through, for example, contributions to community networks, public interest connectivity, affordable access programmes, local skills development, or reserved capacity for South African public institutions, SMEs and researchers.
2. Introduce a monitoring and evaluation framework where operators and relevant state bodies can assess whether standardised indicators in the forthcoming AI policy or strategy (local jobs, local compute served to South African users, procurement, energy source, and community-access contributions) are being met.
3. Recommend early, accessible and well-documented community consultation for major data centre construction projects, consistent with the principles of administrative justice, and ensure energy and environmental impact assessments are part of the approval process.

Privacy and Data Protection

The concentration of personal information in domestic data centres is, in principle, favourable to privacy. It can support data localisation, lawful oversight and faster breach response. However, there can be unintended consequences of data localisation.

Data localisation refers to policies that require personal or non-personal data to be stored or processed within the borders of a specific country.¹⁰ Data residency, a related but narrower concept, simply dictates the geographical location where data is stored. While the Protection of Personal Information Act (POPIA) does not contain a general mandatory data localisation requirement, other South African laws and policies impose specific localisation or residency obligations, particularly for sensitive government data and certain sectors. For example, the Data and Cloud Policy mandates that “government data that incorporates content about the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa”.¹¹ This differs from

¹⁰ Global Center on AI Governance. 2025. *Training Playbook for Data Protection Authorities: A Pilot for the Information Regulator of South Africa*. Retrieved July 23, 2026 from <https://www.globalcenter.ai/research/training-playbook-for-data-protection-authorities-a-pilot-for-the-information-regulator-of-south>

¹¹ National Data and Cloud Policy (see note 3), sec. 15.4.2.

POPIA's cross-border transfer rules, adding layers of complexity, particularly for technologies that inherently rely on fluid, global data flows.

Local storage and processing can be significantly more expensive and less scalable than leveraging hyperscale global cloud infrastructure. Further, data localisation is often an expression of national data sovereignty. However, overly restrictive measures can conflict with the economic benefits of free data flows and international trade, impacting multinational companies and digital services. International best practices for data localisation and residency lean towards a nuanced, risk-based approach rather than blanket restrictions, acknowledging the needs of a global digital economy.¹²

While the mandate for the operationalisation of POPIA falls with the Information Regulator (IR) of South Africa, the South African Human Rights Commission can work with the IR with the objective of protecting the right to privacy by jointly publishing guidance on conducting human rights due diligence on cloud providers and contractual guarantees regarding data residency. Data residency in South Africa does not by itself guarantee South African legal control. Where a domestically hosted facility is operated by, or its parent is subject to, a foreign jurisdiction, personal information may be exposed to extraterritorial access demands. International practice reflected in the EU's treatment of international transfers under the GDPR is to require that transfers and remote access preserve an essentially equivalent level of protection, backed by transparency about lawful-access requests.

The Commission may wish to examine whether POPIA's section 72¹³ regime, and operators' contractual arrangements, adequately address government-access and onward-transfer risks for data physically located in South Africa.

Regional approaches

Africa's regional digital technology landscape is governed by AU frameworks. Over the past decade, the AU has published several regional frameworks on data and digital technologies and the Malabo Convention on Cybersecurity 2014 and the AU Data Policy Framework 2022 contain important provisions and recommendations that South Africa should consider.

The Malabo Convention on Cybersecurity 2014

Comprehensive cybersecurity guidelines and readiness assessments are critical for cloud adoption. On a fundamental level, the multi-tenant architecture of cloud services expands the number of persons with access to critical data, increasing entry points for cyberattacks. Strict data security and access protocols are therefore crucial for cloud systems used to manage public services housing citizens' sensitive data.

¹² Global Center on AI Governance (see note 7).

¹³ Republic of South Africa. 2013. Protection of Personal Information Act (POPIA), sec. 72. Retrieved July 23, 2026 from <https://popia.co.za/section-72-transfers-of-personal-information-outside-republic/>

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014¹⁴ was adopted by the African Union (AU) in June 2014. Besides the EU's GDPR, the Convention is regarded as the only legally binding regional data protection framework. However, only 15 member states have ratified the protocol, and South Africa is yet to adopt the framework.

We recommend that the South African government should consider the Malabo Convention as an effective way to reinforce continental data-protection interoperability.

The AU Data Policy Framework 2022

The AU Data Policy Framework¹⁵ emphasises the need for member states to build comprehensive data infrastructure, including the cloud, to harness value from public data. The framework specifically recognises the cloud as one of the three foundational data infrastructures (the others being big data and digital platforms) needed to harness value from public data. It makes human rights-related recommendations to member states, including establishing data portability rights that facilitate switching between cloud suppliers, ensuring that data can flow across borders as freely as possible while promoting an equitable distribution of benefits and addressing risks related to human rights violations and other legitimate interests of states such as the fight against money laundering, tax evasion, online gambling, and national security.

Further, the Protocol recommends the African Court on Human and People's Rights, the East African Court of Justice, and the Economic Community of West African States (ECOWAS) Community Court of Justice as potential avenues to adjudicate complex disputes on privacy and equality, which are relevant to personal data protection and the use of data to unfairly discriminate.¹⁶ Such a role can potentially be replicated at a national level for South Africa, but there are risks of significant overlap with the mandate of the Information Regulator.

Conclusion

Data centres will underpin South Africa's digital and AI future. Whether that future is rights-respecting depends on governance choices made now. ACM's Africa Technology Policy Committee commends the Commission for framing this as a human-rights inquiry and stands ready to provide further technical assistance, including on standards, privacy engineering, cybersecurity and equitable access measurement as the stakeholder engagement process advances. We would welcome the opportunity to participate in that process and to contribute to any resulting policy guidance.

¹⁴ African Union. 2014. *African Union Convention on Cyber Security and Personal Data Protection*. Adopted June 27, 2014. Retrieved July 23, 2026 from <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

¹⁵ African Union (see note 6).

¹⁶ African Union (see note 6), 60.