Data at home: the new battleground for African MNOs

As African regulators enforce stricter data residency rules and digital economies mature, mobile network operators are being pushed to rethink the physical, legal and architectural foundations of their networks. The outcome is a shift from centralised data flows to distributed, sovereign infrastructure designed for performance, trust and long-term strategic resilience.

For the past two decades, the defining challenge for African mobile network operators was coverage. The goal was to get signal to rural areas, to expand the radio network footprint, to scale backhaul capacity, and later to support the dramatic rise of mobile data. But as connectivity has become more pervasive, the competitive battleground has shifted. Today, the strategic question is not simply whether networks can reach people, but where the data those networks generate is stored, processed and governed. Data sovereignty has moved from the margins of legal compliance to the centre of infrastructure strategy.

Christian Tshishiku, Senior Analyst, DC Byte

"Data sovereignty is now a core part of how MNOs think about network design," explains Nitesh Singh, Managing Director and Communications, Media & Technology Lead for Africa at Accenture. "Many African countries have enacted laws that require sensitive or regulated data to be stored and processed locally. That changes how you architect your platforms. If your analytics, billing or security functions are running in another region, you cannot comply. The design shifts from global to local by necessity."

The impact is particularly pronounced in markets like Nigeria, Ghana, Kenya and South Africa, where data protection frameworks are established and actively enforced. Nigeria's NDPR and various sector-specific regulations impose residency requirements on telecom and financial services data. Ghana's Data Protection Act introduces stringent conditions on how data may be collected, moved, and stored. Kenya's Data Protection Act applies similar conditions, while South Africa's POPIA embeds privacy obligations into corporate operations. What all of these frameworks share is a common principle: data produced within national borders falls under national legal jurisdiction, and operators must ensure that data is physically and operationally accessible to authorities within the state.

The shift from centralised processing to localised compute

For years, many MNO groups and service providers depended on regional data hubs to serve multiple markets. Johannesburg, Lagos and Nairobi acted as processing and interconnect centres, just as Marseille, Lisbon and Dubai acted as offshore gateways for international transit. That model offered scale efficiencies. But data sovereignty introduces friction into that architecture.

"As soon as data must remain within the country where it is generated, the very idea of a multi-country processing hub becomes problematic," says Stefano M. Resi, Head of Data Centre Sales for Middle East and Africa at

Nokia. "If you run shared billing, shared analytics or shared customer experience platforms, you now need to redesign those systems to operate in each sovereign territory. It is not simply a compliance obligation. It changes the topology of the network and the operating model of the business."

Resi emphasises that the implications go far beyond hosting decisions: "data sovereignty touches every internal function," he says. "Budgeting changes because new infrastructure is required. Procurement changes because only certain vendors meet compliance standards. Governance changes because financial structures, shareholder eligibility and partner qualification can be regulated. You cannot isolate the impact. It becomes systemic."

The result is a shift toward distributed architectures composed of in-country data centres linked through secure, policy-aligned interconnection. Operators are no longer designing networks around pure efficiency or cost. They are designing for jurisdictional alignment, latency optimisation and resilience.

Infrastructure disparities are creating divergent MNO strategies

Not every African country is positioned equally for this transition. Markets such as South Africa, Nigeria and Kenya have mature data centre ecosystems with Tier III and Tier IV facilities, carrier-neutral interconnection hubs and hyperscaler nodes. Operators in these markets, including MTN, Vodacom, Airtel Africa and Safaricom, are already shifting workloads into sovereign environments to reduce latency and meet regulatory obligations.

In contrast, countries such as Zambia, Malawi and Sierra Leone lack large-scale certified facilities, forcing operators to continue hosting workloads offshore. The immediate benefit is reduced capital expenditure, but the trade-offs are clear: increased latency, dependency on international transit links, exposure to geopolitical risk, and vulnerability when submarine cables are disrupted.

"This is where the divide becomes visible," notes Christian Tshishiku, Senior Analyst at DC Byte. "Operators in countries with strong data sovereignty regulations are building partnerships with domestic data centre providers. Meanwhile, in markets with weaker frameworks, data continues to flow out of the country. That may reduce cost, but it diminishes national resilience and slows the development of local digital ecosystems."

Tshishiku adds that sovereign hosting is increasingly seen as a competitive differentiator, especially among enterprise and public sector clients: "government institutions, financial service providers and large corporates are explicitly asking where data resides. The ability to guarantee in-country storage is becoming a procurement advantage."

Local hosting is no longer only about compliance

Latency may be the most compelling operational argument in favour of sovereign data processing. African digital services are increasingly real-time in nature: mobile banking, payment authentication, cloud collaboration applications, streaming media, and low-latency enterprise services all perform significantly better when data does not need to traverse multiple international links.

"When data is processed close to the customer, the service experience improves measurably," says Singh. "We are talking about improved load times, smoother video delivery, more stable calls and better real-time analytics. These benefits matter in markets where mobile is the primary access point to the internet."

Resi draws an analogy to automotive engineering. "In the 1980s, cars were powerful but not particularly safe. When the industry invested in safety — airbags, crash-resistant frames, electronic braking — the result was not slower cars, but safer and faster ones. Data sovereignty has a similar dynamic. By strengthening national data control and security, you lay the foundation for better performance, greater trust and ultimately faster digital economic development."

Hyperscalers are entering African markets because of sovereignty, not despite it

Several years ago, cloud hyperscalers preferred to serve Africa through remote regions in Europe or the Middle East. That model is now increasingly untenable. Corporate clients and governments are insisting on domestic control of sensitive data, and MNOs are seeking architectures that place compute closer to users. Cloud providers have responded by deploying local zones, edge nodes and full regions in South Africa, Kenya, Nigeria and soon Egypt and Morocco.

"The direction is unmistakable," Tshishiku notes. "Hyperscalers are adapting to sovereign requirements because the market demands it. Local presence is becoming mandatory for capturing enterprise workloads in Africa."

Singh adds that AI use cases are accelerating this trend. "AI workloads are inherently data-intensive. Their accuracy and usefulness depend on locally relevant datasets. That means keeping data local to train and operate the models. Sovereignty and AI are deeply interlinked."

Regulatory fragmentation remains the largest structural barrier

While sovereign frameworks are stimulating investment and infrastructure development, the lack of harmonisation across African regions increases cost and complexity. Fifty-four countries now have over fifty interpretations of data residency and data protection. Some are precise and enforceable. Others remain broad or ambiguously worded.

"One of the biggest challenges is consistency," Resi explains. "Regulations evolve faster than infrastructure can be deployed. Interpretations vary across ministries and agencies. Operators need clarity and predictability to justify capital investment. A regional or continental framework, similar to the European GDPR alignment model, would unlock greater efficiency and scalability. But we are not there yet."

Despite the fragmentation, Resi remains optimistic: "in almost every market where data sovereignty frameworks have been introduced, infrastructure investment followed. Data frameworks stimulate data infrastructure, and infrastructure stimulates digital services and economic growth. This is a long-term trajectory, not a short-term phase."

The competitive frontier is now trust

Perhaps the most significant shift is not technical, but strategic. Data sovereignty has elevated trust to a market differentiator. In a mobile-first continent where personal and financial services are mediated through handheld devices, trust is an operational currency.

"When customers understand that their data is stored and protected under local law, confidence increases," says Singh. "This matters not only for consumers, but for governments and enterprises. Trust is becoming a structural component of competitive strategy for MNOs."

The question is no longer whether data sovereignty will shape the future of African telecommunications. It already is. The real question is which operators will build the technical, legal and organisational foundations early enough to convert compliance into advantage.

The answer is beginning to show in latency curves, network stability metrics, enterprise contract wins and hyperscaler partnerships. The next decade will belong to operators who build networks not only for speed and coverage, but for proximity, resilience, authentication integrity and sovereign alignment. Those who continue to rely on offshore processing will eventually find cost efficiencies outweighed by regulatory pressure, customer expectations and digital sovereignty priorities.

Africa's data economy is no longer weightless. It has a home. And where that home is located is now a defining strategic choice. ■

Stefano M. Resi, Nokia

Nitesh Singh, Accenture