Data Localisation in Nigeria:

Separating Myth from Reality

ÆLEX

LEGAL PRACTITIONERS & ARBITRATORS

aelex.com @aelexpartners

Introduction

Artificial intelligence, cloud computing, cybersecurity and digital sovereignty have fundamentally changed the way governments think about data.

Around the world, policymakers are increasingly asking where data should be stored, who should have access to it and under what circumstances it should leave national borders. These questions are no longer confined to technology policy, they have become matters of economic policy, national security, industrial development and international trade.

Nigeria is no exception. As businesses increasingly migrate to cloud infrastructure and digital platforms become central to commercial activity, questions surrounding data localisation have become more prominent. Financial institutions, telecommunications operators, healthcare providers, public institutions and multinational companies are all grappling with how best to manage data within an increasingly complex regulatory environment.

Yet, despite the growing attention the topic has received, one misconception persists: that Nigeria has a single data localisation law requiring all data generated within Nigeria to remain in Nigeria.

It does not.

Rather than imposing a single comprehensive data localisation law, Nigeria's approach is evolving through legislation, sector-specific regulation, technical standards and government policy, each addressing different categories of data and different regulatory objectives.

Recent initiatives by the Central Bank of Nigeria (CBN) and the National Information Technology Development Agency (NITDA) demonstrate that this framework continues to develop as policymakers seek to balance digital sovereignty, cybersecurity, innovation and cross-border digital commerce.

Understanding that framework, and, perhaps more importantly, recognising the direction in which it continues to evolve, is becoming increasingly important for businesses operating in Nigeria.

Why is Data Localisation Receiving Increased Attention?

Data has become one of the most valuable commercial assets in the modern economy. At the same time, governments increasingly view certain categories of data as strategic national assets. Several factors have contributed to this shift.

First, concerns around cybersecurity have heightened the importance of maintaining control over sensitive data and critical digital infrastructure.

Secondly, rapid advances in artificial intelligence have increased the strategic value of access to large datasets, prompting governments to reconsider how national data resources should be managed.

Thirdly, geopolitical developments have highlighted the risks associated with over-reliance on foreign digital infrastructure, encouraging many countries to strengthen domestic digital capabilities.

Finally, the continued expansion of cloud computing has made it easier than ever for data to move across multiple jurisdictions, raising new questions regarding regulatory oversight, accountability and jurisdiction.
Against this backdrop, the conversation has evolved beyond privacy. Increasingly, it concerns digital sovereignty, economic resilience and national competitiveness.

Does Nigeria Have a Data Localisation Law?

The short answer is no. However, the position is more nuanced than that simple answer suggests. Nigeria has not adopted a single, comprehensive data localisation law requiring all data generated within the country to be stored exclusively in Nigeria. Instead, the legal framework consists of multiple legislative instruments, sector-specific regulations, technical standards and government policies addressing different aspects of data governance.

These include:

- The Nigeria Data Protection Act 2023;
- The General Application and Implementation Directive (GAID) 2025;
- The National Cloud Computing Policy (2019);
- Sector-specific requirements issued by regulators such as the Central Bank of Nigeria, the Nigerian Communications Commission, the National Health Insurance Authority and other public institutions; and
- Procurement and public sector policies relating to government information systems.

Viewed collectively, these instruments demonstrate that Nigeria has adopted a layered regulatory approach rather than a single comprehensive localisation statute. In practice, localisation obligations depend on the nature of the data, the sector involved, the applicable regulator and, increasingly, broader policy objectives relating to national digital infrastructure and sovereign cloud capabilities.

Data Localisation and Data Residency Are Not the Same Thing

One of the most common sources of confusion is the tendency to use the terms data localisation and data residency interchangeably. Although closely related, they describe different concepts.

Data residency simply refers to the jurisdiction in which data is stored. Data localisation goes further by requiring certain categories of data to be stored, or in some cases processed, within a specified jurisdiction, often accompanied by restrictions on transfers outside that jurisdiction.

A company may, for example, choose to host customer data within Nigeria for commercial reasons while maintaining encrypted backup copies overseas. Depending on the applicable legal and regulatory framework, that arrangement may satisfy residency objectives without constituting strict localisation.

Understanding this distinction is important because many organisations assume that local hosting automatically satisfies localisation requirements. In reality, the legal analysis often depends on whether cross-border transfers occur, the safeguards applied and the nature of the data involved.

The NDPA and Cross-Border Transfers

Contrary to popular perception, the Nigeria Data Protection Act does not impose a general prohibition on transferring personal data outside Nigeria. Instead, it regulates such transfers through a framework based on adequacy, appropriate safeguards and accountability.

Organisations remain responsible for ensuring that personal data transferred outside Nigeria continues to receive an appropriate level of protection, whether through adequacy decisions, contractual safeguards or other recognised transfer mechanisms.

The GAID provides additional guidance regarding the implementation of these obligations and clarifies the expectations placed on data controllers and processors. For many organisations, therefore, compliance with the NDPA is less about determining whether data may leave Nigeria and more about ensuring that appropriate governance and transfer mechanisms are in place before it does.

Beyond the NDPA: A Sectoral and Policy-Driven Approach

Although the NDPA provides the principal framework governing personal data and cross-border transfers, it represents only one component of Nigeria's broader approach to data localisation.

Increasingly, sector regulators are introducing targeted localisation requirements where they consider local storage necessary to support operational resilience, regulatory oversight or the protection of critical national infrastructure.

One recent example is the CBN's June 2026 Circular introducing market structure requirements, ultimate beneficial ownership disclosure obligations and data localisation measures within Nigeria's payments ecosystem.

The Circular requires financial institutions and other participants facilitating payments within Nigeria to ensure that payment transaction data generated within Nigeria is stored and managed within Nigeria, with full compliance required from 1 January 2027.

Unlike the NDPA, which focuses primarily on protecting personal data through regulated transfer mechanisms, the CBN's approach reflects broader policy objectives relating to the resilience, integrity and operational oversight of Nigeria's payment systems.

The financial services sector therefore illustrates an important point. Data localisation in Nigeria is no longer driven solely by privacy considerations. Increasingly, it is being used as a regulatory tool to support financial stability, operational resilience and systemic supervision.

Towards Sovereign Cloud Infrastructure

Data localisation is also increasingly reflected in Nigeria's broader digital economy policies. NITDA's National Cloud Computing Policy, first issued in 2019, established a "Cloud First" approach for government institutions while encouraging the development of indigenous cloud service providers and local cloud infrastructure.

Rather than simply promoting cloud adoption, the Policy recognises cloud computing as an important enabler of digital government, economic development and local technology capacity. It also introduces important policy considerations relating to cloud procurement, vendor lock-in, data classification and the need for cloud solutions that support national digital objectives.

More recently, NITDA has begun translating these policy objectives into more detailed technical guidance. The National Cloud Technical Document proposes comprehensive standards governing sovereign cloud deployments for public institutions, including technical requirements relating to cloud procurement, recognised deployment models, cybersecurity controls, data classification, disaster recovery, localisation, service levels and infrastructure standards.

Particularly noteworthy is its emphasis on hosting higher-sensitivity government data within Nigeria while recognising that certain cross-border transfers may remain appropriate where adequate legal and technical safeguards exist.

Closely linked to these developments is NITDA's recently issued National Data Classification Framework, which seeks to establish a structured methodology for classifying data according to its sensitivity, criticality and the potential impact of its compromise.

Rather than treating all information alike, the Framework recognises that different categories of data require different levels of protection and, consequently, different governance, security and hosting arrangements.

This represents an important policy development. It suggests that future discussions around data localisation in Nigeria are likely to become increasingly risk-based rather than driven by blanket localisation requirements.

Highly sensitive government information and critical national data may warrant stricter localisation and sovereign cloud requirements, while less sensitive information may continue to be hosted or transferred across jurisdictions, subject to appropriate legal, contractual and technical safeguards.

For businesses, the practical implication is that data classification is becoming an increasingly important component of data governance. Decisions regarding where data should be stored, processed and transferred are likely to depend not only on the applicable legal framework, but also on the nature and sensitivity of the data itself.

Organisations that maintain robust data inventories and classification frameworks will therefore be better positioned to respond as Nigeria's localisation requirements continue to evolve.

Taken together, these developments suggest that Nigeria's policy direction extends beyond protecting personal data. Increasingly, it seeks to establish a broader governance framework for data, cloud infrastructure and digital sovereignty, one that combines legislative requirements, sector-specific regulation, technical standards and government policy to support public sector digital transformation, strengthen national digital resilience and build trusted domestic digital infrastructure.

Is Nigeria's Digital Infrastructure Ready?

Legal obligations are only one part of the discussion. Effective data localisation depends not only on regulatory requirements but also on the availability of reliable digital infrastructure capable of supporting local storage, processing and cloud-based services.

Nigeria has witnessed significant investment in carrier-neutral data centres, cloud infrastructure and fibre connectivity over recent years. International cloud providers, together with local cloud operators and data centre operators such as Rack Centre, Open Access Data Centres (OADC) and Equinix (through MainOne), have expanded local infrastructure, increasing the capacity available to organisations seeking in-country hosting solutions.

Importantly, recent government initiatives also recognise that localisation requirements cannot exist in isolation. The National Cloud Computing Policy and the National Cloud Technical Document reflect a broader policy objective of strengthening Nigeria's indigenous cloud ecosystem and digital infrastructure, recognising that any meaningful localisation strategy must be supported by commercially viable local hosting capacity, resilient cloud services and appropriate cybersecurity capabilities.

While challenges remain, including energy reliability, nationwide infrastructure resilience and the continued expansion of hyperscale cloud capacity, Nigeria's digital infrastructure has developed considerably over recent years and is increasingly capable of supporting localisation requirements across a growing range of sectors.

The focus is therefore shifting beyond whether localisation is technically feasible to how Nigeria can continue expanding the infrastructure needed to support its broader digital economy ambitions.

Data Localisation and Regional Digital Trade

Nigeria's evolving approach must also be considered within the broader context of the African Continental Free Trade Area (AfCFTA), which seeks to facilitate digital trade and cross-border services across the continent. As African economies become increasingly interconnected, policymakers will continue to balance legitimate objectives relating to digital sovereignty, cybersecurity and national resilience against the economic benefits of cross-border data flows and regional digital integration.

How that balance ultimately develops is likely to become one of the defining regulatory questions for Africa's digital economy over the coming decade.

Conclusion

Perhaps the most important point is that Nigeria's data localisation framework should not be viewed as settled. The direction of travel is becoming clearer than the final destination.

Recent initiatives by the CBN and NITDA demonstrate that policymakers are moving beyond broad policy statements towards increasingly specific localisation, sovereign cloud and digital infrastructure requirements. At the same time, the rapid development of artificial intelligence, cloud computing and shifting geopolitical dynamics will continue to influence how governments think about data governance.

More fundamentally, data localisation should not be viewed as an end in itself. Rather, it forms part of a broader strategy aimed at strengthening digital sovereignty, cybersecurity, regulatory oversight and the resilience of Nigeria's digital economy. Businesses should therefore resist treating today's localisation requirements as the final position. Instead, they should monitor legislative, regulatory, technical and policy developments closely and periodically reassess their data governance strategies to ensure they remain aligned with evolving legal obligations and commercial realities.

For boards, general counsel and technology leaders, the question is no longer simply where data is stored. Increasingly, it is whether their organisations have the governance, infrastructure and strategic flexibility to operate confidently in a regulatory environment that is still taking shape.

Authors

Tiwalola Osazuwa

Peretimi Akinmodun

Lazarus Kalu