Key contacts

Ijeoma Uju
Partner,
Corporate & Commercial
ijeoma.uju@templars-law.com

Oghomwen Akpaibor
Managing Counsel,
Corporate & Commercial
oghomwen.akpaibor@templars-law.com

Abdulsamad Lawal
Associate,
Corporate & Commercial
abdulsamad.lawal@templars-law.com

Client Alert

Nigeria's National Digital Cloud Policy:
Key Provisions and Implications for Business

Introduction

On 17 August 2026, the Federal Government released the National Digital Cloud Policy ("Policy").[1] The Policy supersedes the Nigeria Cloud Computing Policy 2019 and takes immediate effect, except for the sovereignty provisions in Part III of the Policy, which require Presidential approval.[2] The Policy marks a shift from the 2019 general cloud adoption to the deliberate development of a domestic cloud and data infrastructure ecosystem in Nigeria. Its objectives are to attract infrastructure investment, promote regional competitiveness and establish protocols necessary to secure national control over government and regulated data.

This Client Alert highlights the implications for cloud service providers, data centre operators, regulated entities and businesses that use cloud services in Nigeria.

Scope of Application

The Policy operates at three levels:

- **General Market Framework**: Parts I and IV apply to all market participants and establish the framework for investment, trade, market development, and implementation.
- **Public Sector Mandate:** Part II applies to Federal Ministries, Departments or Agencies of the Federal Government (MDAs). It mandates a cloud-first adoption, aggregated government demand procurement through Galaxy Backbone Limited ("GBB") and a National Digital Marketplace. State Governments may opt in voluntarily.[3]
- **Sovereign Data**: Part III applies only to "sovereign data" which is defined as: (a) data generated by the Federal Government and its MDAs or entities exercising public functions on its behalf; (b) data generated under Federal regulation, licence or directive that has

[1] National Digital Cloud Policy, Federal Republic of Nigeria, August 2026. (the "Policy")
[2] Part 14.5; Part 11.7. of the Policy
[3] Part 1.6; Part 10.5. of the Policy

been specifically designated as sovereign.[4] All other data outside the definition of sovereign data is expressly excluded and remains governed by the Nigeria Data Protection Act, 2023, other sectoral regulation, and ordinary commercial law.

Key Policy Mechanisms

i. Investment Incentives for Cloud and Data Centre Operators

Under the Policy, qualifying investments in cloud and data centre infrastructure will be eligible for:[5]

- **Fiscal incentives**: import duty exemptions on core data centre equipment such as servers, storage, networking, racks, cabling; power and cooling infrastructure, equipment required for qualifying deployments; appropriate capital allowances; value added tax treatment for exported cloud services; and potential preferred status and tax incentives for qualifying strategic digital infrastructure projects.[6]
- **Regulatory Facilitation and Investment Certainty:** streamlined regulatory approvals and licencing processes to reduce administrative barriers to market entry and infrastructure deployment.
- **Capital Mobility and Foreign Exchange Treatment**: seamless capital repatriation while qualifying exported cloud and data service revenues for potential foreign exchange and trade incentives.
- **Energy Access as an Investment Incentive:** support in accessing reliable electricity, including opportunities to utilise renewable and alternative energy solutions for cloud infrastructure. Importantly, the beneficiaries of these incentives are required to commit to capability development programmes, including knowledge transfer and skills development.[7]

ii. Eligibility and qualification for incentives under the Policy[8]

The eligibility and qualification criteria under the Policy focus on transforming domestic capacity into a regional export hub while ensuring domestic skills transfer. The core qualification criteria for stakeholders include:

- **Infrastructure Deployment**: demonstration of present or committed deployment of qualifying infrastructure within Nigeria.
- **Registration & Compliance:** mandatory registration under the Digital Infrastructure Assurance Registration scheme with strict adherence to data protection, cybersecurity, and consumer protection laws.
- **National Framework Integration**: participation in the National Digital Marketplace (for government contracts) and alignment with national interoperability standards is necessary.
- **Local Capability Commitments**: proportional investment in skill-building and local technology transfer.

iii. Government as Anchor Customer

The Federal Government (FG) proposes to use its own aggregated purchasing as a commercial incentive for infrastructure investment. To this end, the Policy creates a structured demand signal for providers as follows:

[4] Part 11.2. of the Policy
[5] Part 3.2. of the Policy
[6] Part 3.2. of the Policy
[7] Part 3.7. of the Policy
[8] Part 3.8. of the Policy

- All new MDA systems must be cloud first.[9]
- Government procurement will now be centralized through GBB, creating volume-based purchasing power.
- A National Digital Marketplace will serve as the procurement channel with listing requiring a valid Certificate of Registration under the Digital Infrastructure Assurance Registration scheme.[10]
- A ringfenced Anchor Capacity Fund aimed at de-risking private infrastructure investment will underwrite baseline government demand for cloud services.[11]

These proposed measures undoubtedly create material commercial opportunities for registered providers, including international operators with local infrastructure.

iv. The Sovereign Data Treatment

Importantly, rather than forcing broad data localization requirements, the Policy targets specific risks by applying data residency and control requirements strictly to defined Sovereign data.

It classifies Sovereign data into four distinct tiers:[12]

- **Level 4 (Classified):** covering national security and critical infrastructure, requires exclusive in-country hosting, local processing, and government-controlled encryption keys.
- **Level 3 (Highly Sensitive)**: covering regulated personal, financial, biometric, and health data, mandates storage in Nigeria, with continuous sovereign recovery capabilities, while allowing processing in approved environments;
- **Level 2 (Sensitive)**: covering routine administrative records, permits hybrid deployments subject to National Information Technology Development Agency ("NITDA") authorization; and[13]
- **Level 1 (Open)**: covering public information, carries no residency restrictions.

Crucially, the designation of data as sovereign is not automatic and requires formal justification under the Policy. Consequently, MDAs seeking sovereign classification must demonstrate to the Sovereign Government Cloud Governance Committee that the restriction sought represents the least restrictive means to protect national interests with Level 3 and Level 4 designations further contingent on Presidential approval. Furthermore, it is important to note that these residency controls attach to the data classification rather than the provider's corporate origin, thereby potentially allowing a qualified international or domestic entity to host sovereign workloads.[14]

Cross-Border Data Flows

The Policy affirms an open approach to cross-border transfers:[15]

- commercial data may move freely as no localization requirement applies;
- cross-border processing of sovereign data is permitted where authorized by the NITDA, subject to safeguards under the Nigeria Data Protection Act 2023;
- the NDPC[16] will publish a whitelist of jurisdictions with adequate protection; and
- the Federal Government will also ensure that all measures are properly aligned with Nigeria's commitments under the African Continental Free Trade Area.

[9] Part 7.1. of the Policy
[10] Part 9.1. of the Policy
[11] Part 10.2. of the Policy
[12] Part 11.3. of the Policy
[13] Part 11.4. of the Policy
[14] Part 11.6; Part 11.7. of the Policy
[15] Part 4.3; Part 4.6. of the Policy
[16] Nigeria Data Protection Commission

Implementation Timeline & Targets

Phase 1 – Activation and Baseline (0–6 months): Publication of directives and incentive criteria; establishment of Governance Committee and Anchor Capacity Fund.

Phase 2 – Deployment and Market Activation (6–12 months): National Digital Marketplace goes live; priority MDA migrations begin; recognised jurisdictions whitelist published; capacity development programmes launched.

Phase 3 – Scale and Export Development (12–24 months): Scaled migration; regional interconnection; mutual recognition arrangements pursued; first review of sovereignty requirements.

Key targets include USD 250 million private investment committed to cloud and data infrastructure in Nigeria within 12 months, 70% of new government systems designed cloud-first, and 10 registered providers on the Marketplace within 12 months[17] alongside progressive increases in compliant hosting capacity and the development of Nigeria's regional cloud export market.

Recommended Actions:

- **Cloud providers and data centre operators**: should begin to assess eligibility for incentives and the process for registration under the Digital Infrastructure Assurance Registration scheme to access government business. The Government's US$250m (12-month) / US$750m (24-month) investment targets suggest a live courtship of investment capital; operators with capacity to deploy could seek early anchor-investor positioning.
- **Regulated entities**: the Policy does not impose general data localisation on commercial data as sovereignty requirements are narrowly confined to defined categories of government and regulated data. However, "regulated data" categories should be watched closely as they are defined.
- **Businesses using cloud services**: take note that your commercial data is unaffected by the sovereignty provisions. The Policy provides regulatory certainty for continued use of international cloud services.
- **All stakeholders**: actively track the publication of incentive qualification criteria and the operationalisation of the National Digital Marketplace, both expected within 6–12 months.

If you require any further clarification, do not hesitate to contact us.

[17] Part 14.4. of the Policy