

THE NATIONAL DIGITAL CLOUD POLICY AND DATA PROCESSING IN NIGERIA



The implications of the new policy for businesses and organisations extend beyond the location of their data, so they need to conduct a structured review of their cloud and data-management arrangements.

Introduction

The increasing integration of technology across various sectors in Nigeria has driven demand for IT infrastructure that supports innovation, data processing and storage, digital service delivery and operational efficiency. This, in turn, has contributed to the adoption of cloud services in Nigeria. While cloud-based applications have long been embedded in the day-to-day operations of many Nigerian businesses through platforms like Microsoft 365, Google Drive, and Zoho, cloud computing adoption has now expanded to include hosting, processing, and delivering business systems and digital services.

According to Mordor Intelligence, the Nigerian cloud computing market was estimated at \$1.03 billion in 2025 and is projected to reach \$3.28 billion by 2030, representing a compound annual growth rate (CAGR) of 25.98%. This growth has been supported by the shift to remote and hybrid working, which has increased demand for systems that enable access to applications and data across locations. Changing economic conditions, including foreign exchange volatility, have also prompted businesses to move from traditional IT infrastructure to scalable infrastructure that reduces upfront investment in physical IT assets.

Nigeria's cloud regulatory framework has evolved alongside the growth in adoption to address questions about data location and control, infrastructure security, reliance on domestic and international providers, and cross-border processing, as cloud infrastructure plays an increasingly central role in storing, processing, and delivering digital services.

The Nigeria Data Protection Act 2023 (NDPA) remains the principal framework for personal data processing, including cross-border transfers, while the National Cloud Computing Policy 2019 introduced a "Cloud First" approach for Federal Public Institutions and businesses providing IT solutions to them. However, these regulatory instruments did not provide a broader framework for data sovereignty, cloud investment, or the domestic cloud ecosystem now contemplated.

Against this background, the Federal Government issued the National Digital Cloud Policy in August 2026. This article examines how the policy changes the regulatory landscape for businesses in Nigeria, particularly regarding data sovereignty, cross-border data processing and the use of cloud infrastructure.



Overview of the Policy

The policy sets out the framework for Nigeria's cloud ecosystem. It aims to promote investment in domestic cloud infrastructure, increase cloud adoption, and expand hosting capacity. As part of these objectives, the policy seeks to position Nigeria as a regional hub for data hosting and digital services, strengthen indigenous participation in the cloud value chain, and modernise government service delivery. It also aims to preserve an open and competitive market in which domestic and international cloud service providers can operate on transparent and predictable terms.

A central feature is the definition and classification of "sovereign data". The category includes data generated by the Federal Government and by entities exercising public functions, as well as data generated under government-issued licences, permits, concessions, partnerships, or regulatory obligations. Sovereign data is classified by sensitivity, with controls and hosting requirements set according to the associated risk. The policy therefore adopts a risk-based and proportionate approach, under which the most restrictive requirements apply only to the most sensitive categories, rather than treating all data held in Nigeria as equally sensitive.

The policy does not require all data generated or processed in Nigeria to be hosted domestically, as commercial data outside the sovereign-data definition remains governed by the NDPA, applicable sectoral regulation and commercial laws. Nor does it treat physical data residency as the sole means of national control; where encryption, key custody, contractual safeguards, or audits can achieve the relevant objective, a less restrictive measure should be preferred.

Businesses may therefore continue to use international cloud infrastructure, subject to assessing whether the data is sovereign and, if so, what its classification requires. Sovereignty analysis therefore turns on the data's character and classification, and on the controls available, not simply on server location or the provider's identity.

Analysis of the Policy

The policy operates alongside the requirements of the NDPA, which applies where personal data is processed in Nigeria, where the controller or processor operates in Nigeria, or where a controller or processor outside Nigeria processes the personal data of a data subject in Nigeria.

For example, a Nigerian business using an international cloud provider to store customer information would need to consider its obligations under the NDPA, including requirements to process that personal data fairly, lawfully and transparently, to implement appropriate technical and organisational measures to protect its

confidentiality, integrity and availability, and to be accountable for its processing activities. Separately, the business would also need to assess whether any of the data is sovereign data and to comply with the policy's classification-based requirements. One cloud arrangement may consequently engage both regimes for different reasons, with the NDPA governing personal-data processing and protection, and the policy addressing national control over specified data and the infrastructure used to host or process it. The regimes should therefore not be treated as alternatives, as compliance with one does not remove the need to analyse the other, and the same dataset may fall within one regime or both.

Furthermore, businesses should review existing cloud arrangements to identify where data is hosted and processed, what data is involved, the roles and locations of providers and sub-processors, and whether the arrangement provides the required level of control under the applicable framework. This is particularly important for organisations operating across jurisdictions or using platforms spanning multiple data centres. A provider's headquarters does not determine where data is stored or processed; however, businesses need visibility into the cloud architecture and the processing jurisdictions. Businesses should not assume that a standard provider configuration provides sufficient visibility; service descriptions and sub-processor disclosures may need to be examined.

The review should cover contracts and operating practices. Agreements should address data location, security, access controls, sub-processors, audit rights, incident management, data portability, and the return or deletion of data at termination.



Contractual safeguards may support control over sovereign data but may not be sufficient where infrastructure remains subject to a foreign jurisdiction capable of compelling disclosure. They should therefore be considered alongside technical and structural measures and, where necessary, domestic hosting. For cross-border processing, businesses should also document the relevant jurisdictions and confirm that provider commitments can be implemented in practice.

Financial institutions require particular attention because they process substantial volumes of personal, financial and other regulated data. They should assess the NDPA, applicable financial-sector requirements and the Policy, particularly where data is sovereign, including implications for cloud architecture, outsourcing, access, third-party providers and controls over sensitive datasets. This requires understanding not only the provider's identity but also how and where its infrastructure processes the institution's data. The assessment should also address outsourcing and concentration risk, the institution's audit rights, and the treatment of data following an incident or termination.

Businesses may also face cost implications, as compliance may require investment in additional security and key-management arrangements, migration or restructuring of workloads, and amendments to provider agreements. These implications may be particularly material where workloads must be separated, relocated, or monitored more closely. However, the cost will depend on the nature and classification of the data and should be weighed against the efficiencies of scalable cloud infrastructure, as the policy is intended to encourage investment and access to digital capacity, not simply to require businesses to maintain physical infrastructure solely to keep data in Nigeria.



Beyond compliance, the Policy may reshape Nigeria's domestic cloud ecosystem. Its emphasis on data-centre capacity, connectivity, investment, indigenous participation and regional digital services could increase local hosting options, which in turn could create opportunities for investors and technology providers across data centres, cloud services, connectivity, cybersecurity and related digital infrastructure, while giving businesses a broader range of hosting and processing choices. Successful implementation could also encourage competition between domestic and international providers and support associated services.

Recommendations

The implications for businesses and organisations extend beyond data location, so they need to conduct a structured review of their cloud and data-management arrangements. The review should map data flows and processing jurisdictions; identify providers and sub-processors; assess security, access and incident controls; review outsourcing and cloud contracts; and classify datasets to determine whether any constitute sovereign data. Organisations should test their cross-border processing arrangements against the NDPA and applicable sectoral requirements, record the basis for classification decisions, and assign responsibility for keeping the assessment current as systems, providers and data uses change.

Where data is sovereign, organisations should assess the classification-based requirements and whether contractual safeguards, encryption, key custody, audits or other controls provide sufficient national control. They should weigh those measures against domestic hosting or other changes to cloud architecture, taking into account foreign-jurisdiction disclosure risk, migration requirements and cost. Financial institutions should perform this assessment alongside their sector-specific outsourcing and technology-risk frameworks. Where domestic hosting is selected, the decision should address capacity, resilience, security and access requirements rather than location alone.

Finally, organisations should monitor the policy's implementation and the development of domestic capacity, as detailed implementation, available capacity and market practice may evolve over time. As local infrastructure, connectivity and cloud services expand, domestic hosting may become commercially attractive and support regulatory alignment. Businesses should therefore keep their provider arrangements, data classifications and security controls under review, while investors and technology providers should consider the opportunities arising from Nigeria's ambition to become a regional digital-services hub. This forward-looking approach preserves flexibility while aligning cloud adoption with Nigeria's evolving requirements for data protection, sovereignty and cross-border processing.



Detail Commercial Solicitors is distinct as Nigeria's first commercial solicitor firm to specialise exclusively in non-courtroom practice. Based in Lagos, Nigeria's business capital, DETAIL is totally committed to its clients' business objectives and reputed for dealing with the minutiae. Email: info@detailsolicitors.com

Stay updated! Follow us by clicking below:

www.detailsolicitors.com[Detail Commercial Solicitors](#)[Detail Nigeria](#)[Detail Solicitors](#)