BANWO & IGHODALO

How Nigeria's data localization regime shapes fintechs' handling of financial, identity, and transaction data

DECEMBER 18, 2025

Introduction

As Nigeria's digital financial ecosystem grows, regulators, including the Central Bank of Nigeria (**"CBN"**), National Information Technology Development Agency (**"NITDA"**), Securities and Exchange Commission, and the National Insurance Commission, have increasingly adopted a data localization policy stance. Although this policy stance is ostensibly aimed at safeguarding critical national infrastructure and protecting personal and financial data, it has resulted in fintechs and other financial services platforms facing an increasingly complex regulatory landscape that mandates local storage of sensitive data and imposes restrictions on international data transfers. This article seeks to discuss a few of the regulations that created the landscape and their implication on transfer of data within the ecosystem.

Regulatory context

Data localization is a specific policy or law that mandates that any data created within a country's borders must remain stored and processed within that country. This is often done for national security, to ensure local law enforcement agencies can access the data, or to boost the local technology economy (forcing technology giants to invest in local infrastructure). For instance, the CBN's *Guidelines on Point of Sale (POS) Card Acceptance Services 2011* require domestic Point of Sale (POS) and Automated Teller Machine (ATM) transactions to be routed exclusively through local network switches. These rules apply to a wide range of entities, including merchant acquirers, card issuers, merchants, payment terminal service providers, processors, and cardholders. Routing domestic transactions abroad is expressly prohibited, ensuring that sensitive financial data remains within the Nigerian jurisdiction.

Beyond payments, NITDA's *Guidelines for Nigerian Content Development*[1] also impose obligations on entities handling sovereign data to store such data exclusively within Nigeria. Sovereign data, in line with Nigeria's content development and cloud computing frameworks, refers to data generated, owned, or controlled by the Nigerian government exclusively within Nigeria. Cross-border transfers or hosting of sovereign data are permitted only with NITDA's express approval, following local storage. For the required approval to be granted, NITDA will consider an entity's level of compliance with the *Nigeria Data Protection Act*

[1]NITDA's Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2019.

2023 (**"NDPA"**), adherence to the *Nigeria Cloud Computing Policy (2019)*, assurance of government access, non-disclosure commitments, robust data security measures, and periodic audits.

The *Designation and Protection of Critical National Information Infrastructure Order, 2024* designates systems such as the Bank Verification Number (BVN), National Identification Number (NIN), and the Nigerian Interbank Settlement System (NIBSS) as Critical National Information Infrastructure (CNII). While such designation is primarily aimed at safeguarding and preserving these systems, it arguably reinforces broader data localisation imperative and cybersecurity objectives. A good example of this is the CBN's *Regulatory Framework for BVN Operations*[2] which mandates that all BVN data should be stored within Nigeria and limits its use to licensed financial institutions for purposes such as customer onboarding, account maintenance, and identity verification.

As indicated above, cross-border transfer of sensitive data falling under the data localization mandate requires regulatory consent and adherence to strict NDPA safeguards. The NDPA establishes the legal framework for personal data protection in Nigeria. The law permits cross-border data transfers only when the destination country provides an adequate level of protection or when certain statutory conditions are met by the transferor, including obtaining the data subject's consent, or where there is no consent, transfer is necessary for performing a contract, protecting vital interests, or fulfilling important public interests. Organizations are required to document the legal basis for transfers, assess the adequacy of protections, and conduct a Transfer Impact Assessment (TIA) to identify potential risks and mitigation measures prior to executing international data transfers.

The immediate concern flowing from data localization mandates would be availability of infrastructure and processes to ensure the security and integrity of data stored locally. This is addressed through the integration of localisation and cybersecurity requirements, as exemplified by the CBN's cybersecurity regime which focuses on how the data is protected once it resides within approved infrastructure. Under the *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs) 2024*, financial institutions must ensure that their technical infrastructure providers and digital service vendors implement and maintain appropriate security controls consistent with standards such as Payment Card Industry Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS) and PIN Transaction Security (PTS).

[2]CBN's Regulatory Framework for BVN Operations and Watch-List for the Nigerian Banking Industry (2021)

Operational implications for fintechs and recommended steps towards building a compliance-ready data strategy

Fintechs and financial service platforms should take a proactive and structured approach to data management in Nigeria. This begins with mapping and classifying data flows, particularly those involving financial, identity, and transactional data, to identify which datasets are subject to localization requirements or special protection under the regulatory oversight of the CBN, NITDA, or the Nigeria Data Protection Commission (**"NDPA"**). In this regard, fintechs and financial services platforms dealing with federal ministries, departments and agencies will have to comply with or adopt the data classification under Schedule A of the National Cloud Policy 2019. Companies should ensure that sensitive or regulated data is stored domestically, and that any cross-border data transfers comply with the adequacy and safeguard requirements provided in the NDPA.

Early engagement with regulators such as the CBN, NITDA, and NDPC can help clarify grey areas, secure necessary approvals for cross-border arrangements, and demonstrate a culture of compliance. Fintechs should also adopt strong contractual and technical safeguards when working with cloud providers, payment processors, or third-party vendors, ensuring that all partners meet Nigeria's data protection and cybersecurity standards.

Cyber resilience is equally critical. Firms should implement and routinely test incident response plans, maintain PCI DSS and related security certifications, and ensure continuous monitoring and audit of systems that process sensitive data. Conducting Transfer Impact Assessments (TIAs) before any international data movement and Data Protection Impact Assessments (DPIAs) for high-risk processing, can further help identify vulnerabilities and demonstrate accountability under the NDPA.

In the medium term, fintechs should establish a holistic data governance framework that integrates privacy, cybersecurity, and operational risk management. This includes appointing a Data Protection Officer (DPO) (guided by a seasoned Data Pro-

tection Compliance Organisation (DPCO)), developing internal data handling policies, and embedding compliance into product design ("**privacy by design**") and ensuring that privacy and security of data is the default.

By embedding these practices, fintechs will not only achieve compliance but also strengthen consumer trust, improve operational resilience, and position themselves competitively within Nigeria's rapidly evolving and increasingly regulated digital financial ecosystem.

DISCLAIMER: This article is only intended to provide general information on the subject matter and does not by itself create a client/attorney relationship between readers and our Law Firm or serve as legal advice. We are available to provide specialist legal advice on the readers' specific circumstances when they arise.

CONTACT PERSONS

Olumide Osundolire

Partner

E: Oosundolire@banwoighodalo.com

Vanessa Obi

Associate

E: VObi@banwo-ighodalo.com

Oluwatoba Oguntuase

Senior Practice Support Lawyer

E: Ooguntuase@banwo-ighodalo.com