

COMMENTS ON CENTRAL BANK OF NIGERIA DATA LOCALIZATION DIRECTIVE

October 2026

The Global Data Alliance (GDA)¹ is pleased to provide comments on the Central Bank of Nigeria's (CBN) Circular, entitled, "Introduction of Market Structure Requirements, Data Localisation, Ultimate Beneficial Ownership Disclosure, and Systemic Oversight Measures in the Nigeria Payments System," reference PSS/DIR/PUB/CIR/001/004 (Circular). Our comments focus on the data localization requirement in paragraph 2.

The GDA is a cross-industry coalition of companies committed to high standards of data responsibility, safety, and security. Our members are active in finance, insurance, technology, manufacturing, and other sectors, and rely on the ability to access and transfer information across borders to innovate and create jobs.

We support CBN's objectives of improving ownership transparency, addressing concentration risk, promoting a fair, competitive, and resilient payments ecosystem, and safeguarding the integrity of Nigeria's payments system (Circular, page 1). Cross-border access to information and digital tools can help advance these objectives while supporting data protection, cybersecurity, financial inclusion, and economic opportunity.

Financial institutions depend on international data access for everyday operational and regulatory functions. Fraud detection, sanctions screening, and anti-money laundering compliance benefit from comparison of transactions against global reference information. Group risk management depends on information from different jurisdictions, and payments rely on interconnected processing infrastructure. Businesses throughout Nigeria's economy also depend on these services to reach customers, pay suppliers, and participate in international trade.

The GDA encourages CBN to preserve access to the global capabilities that support trusted payments. Secure international services can help smaller providers obtain advanced tools without building every system themselves. A location requirement that narrows those options could raise costs and concentrate operational dependencies, working against the Circular's competition and resilience objectives.

Accountability and supervisory access

Paragraph 2 provides: "All Financial Institutions and participants facilitating payments within Nigeria shall ensure that payments transaction data generated within Nigeria are stored and managed in Nigeria in accordance with data protection laws and regulations applicable in Nigeria. Accordingly, all affected Financial Institutions shall fully comply with this requirement effective January 1, 2027." (Circular, page 2).

CBN has a legitimate interest in obtaining complete, usable payment records and holding regulated institutions accountable. Retention requirements and enforceable audit and access rights can support that oversight, including where institutions use outsourced services. The GDA therefore recommends replacing the blanket localization requirement with safeguards that allow institutions to select domestic or international infrastructure based on security, operational performance, and legal accountability.

¹ The Global Data Alliance (GDA) is a cross-industry coalition of companies committed to high standards of data responsibility that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA members operate in healthcare, biopharmaceuticals, medical devices, insurance, technology, and other sectors. For more information, see www.globaldataalliance.org.

Institutions would remain responsible for their providers and for ensuring timely CBN access to records. Encryption and secure key management can protect confidentiality, while access controls and audit logs support oversight of data use. Incident reporting and tested recovery arrangements address operational disruptions. These measures give CBN a basis for evaluating protection and access that physical location alone cannot establish.

To reflect this approach, we recommend that paragraph 2 could instead provide: “Institutions shall protect payment transaction data in accordance with applicable Nigerian law, retain records required for supervision, and ensure timely and effective CBN access to those records. Subject to applicable data protection and prudential safeguards, institutions may use any domestic or international infrastructure and services for storage, processing, support, and recovery. Institutions remain accountable for their service providers and for compliance with these obligations.”

Nigeria's cross-border data framework

Nigeria already has a framework for protected international transfers of personal data. Sections 41–43 of the Nigeria Data Protection Act 2023 (NDPA) provide routes based on adequate protection or specified statutory conditions. Section 41 identifies laws, binding corporate rules, contractual clauses, codes of conduct, and certification mechanisms that afford adequate protection, with the basis for transfer and adequacy documented. The Nigeria Data Protection Commission's (NDPC) General Application and Implementation Directive 2025 (GAID), Article 45 and Schedule 5, provides further guidance, including NDPC approval where required.

The GDA encourages CBN and NDPC to coordinate a formal revision of paragraph 2 that accommodates transfers meeting this framework alongside appropriate financial-sector safeguards. Joint guidance could explain how institutions can demonstrate compliance through recognized transfer instruments and reuse relevant assessments and assurance evidence. This would give institutions a clear path to meet both privacy and prudential obligations, while retaining accountability for the data they process.

Cybersecurity and Operational Resilience

The cross-border nature of fraud and cyber threats makes international cooperation particularly important to payment system integrity. Global cybersecurity services can combine threat information from different markets and give Nigerian institutions access to specialist incident-response teams. Restrictions that reduce the information available to analysts or prevent teams from supporting Nigerian systems could weaken detection and response.

The GDA therefore recommends that the revised Circular expressly accommodate secure international processing and access for transaction screening, fraud prevention, anti-money-laundering compliance, group risk management, and incident response, subject to applicable law. Institutions should also be able to use international cloud services and geographically distributed backups. These capabilities can help maintain payments when a disruption affects an entire region.

CBN's concerns about operational dependence can be addressed through provider due diligence, ongoing monitoring, tested exit plans, portability, and recovery requirements. Allowing institutions to draw on a wider range of secure providers and recovery locations would support this effort. Any restrictions should respond to identified risks and the effectiveness of available safeguards.

Scope of the Localization Requirement

The Circular does not define “payments transaction data” or “managed,” or expressly address foreign processing, additional copies, and remote access. If interpreted to require exclusive domestic storage or management, paragraph 2 could restrict global cloud services, transaction monitoring, specialist support, and disaster recovery. Even a requirement to duplicate infrastructure locally can impose substantial costs.

The GDA recommends clear guidance on covered payment records and when information is considered generated within Nigeria, including transactions involving participants in more than one country. Further guidance should distinguish storage, processing, management, and remote access, and explain the treatment of logs, metadata, support records, analytics, and genuinely anonymized information. Pseudonymized personal data should continue to receive the protections required under Nigerian law.

If CBN retains a domestic record requirement, it should be limited to a copy of specified records necessary for an identified supervisory purpose. The location of those records should not determine the location of all related software, personnel, or infrastructure. The GDA recommends expressly preserving lawful international copies, processing, remote support, and recovery capabilities under this fallback.

Consultation and Implementation

The Circular states that “The CBN shall monitor compliance with the provisions of this Circular and may, where necessary, impose supervisory sanctions in accordance with applicable laws, regulations, and guidelines.” (Compliance and Enforcement, page 2). Clear revisions and guidance will therefore be important before institutions are expected to comply with paragraph 2.

The GDA recommends deferring the January 1, 2027 localization deadline while CBN revises the requirement and develops coordinated guidance with NDPC. A focused consultation with banks, payment providers, technology suppliers, businesses that depend on payments, and consumer representatives would help identify operational effects and workable alternatives. That process should consider privacy and security outcomes alongside competition, costs, financial inclusion, and continuity of service.

Once the revised approach is settled, institutions should have sufficient time to assess contracts, validate controls, and test any necessary changes. We encourage proportionate supervisory treatment of institutions implementing agreed transition plans, so that the process supports reliable payments and effective compliance.

Conclusion

The GDA appreciates CBN's consideration of these comments and welcomes further engagement with CBN and NDPC on rules that protect customers and payment system integrity while preserving secure international data access. Should you have any questions, please feel free to contact Joseph Whitlock, Executive Director, Global Data Alliance, at jwhitlock@bsa.org.