Central Bank of Nigeria

FREQUENTLY ASKED QUESTIONS AND ANSWERS ON THE DATA LOCALISATION CIRCULAR ISSUED ON JUNE 15, 2026

1. What is meant by “payment transaction data”?

Answer

Payment transaction data refers to information generated, collected, processed, or stored in connection with the initiation, authorisation, processing, clearing, settlement, or reconciliation of a payment transaction.

This includes but not limited to transaction amounts, dates and times, transaction references, payer and beneficiary details, account or wallet identifiers, payment channels, transaction status, and associated records used for verification, dispute resolution, or audit purposes.

2. What exactly constitutes compliance with the requirement that payment transaction data be "stored and managed in Nigeria"?

Answer

The supervisory directive is that the complete lifecycle of a regulated institution’s payment transaction data (from [Creation] ➔ [Storage] ➔ [Usage] ➔ [Sharing] ➔ [Archiving] ➔ [Destruction]) should reside in Nigeria and remain subject to Nigerian governance, operational control, administration, security management, monitoring, and regulatory oversight.

Accordingly, compliance encompasses the localisation of production environments, databases, storage infrastructure, governance arrangements, database administration, access administration, information security management, backup and recovery processes, incident management, audit monitoring, change management, configuration management, business continuity arrangements, and all other operational activities necessary for the management of regulated payment transaction data. Institutions should be able to demonstrate that payment transaction data is stored in Nigeria and accessible for supervisory review and subject to Nigerian legal and regulatory control throughout its lifecycle.

3. What datasets fall within the scope of the Data Localisation requirements?

Answer

The Data Localisation requirements apply to payment transaction data generated within Nigeria and all related or supporting datasets necessary for the processing,

settlement, reconciliation, monitoring, supervision, reporting, auditing, investigation, dispute resolution, business continuity, and reconstruction of payment activities.

This includes, but is not limited to, production databases, settlement records, transaction logs, payment records, audit trails, reporting databases, backup repositories, replicated datasets, disaster recovery environments, archives, data warehouses, operational telemetry, monitoring information, diagnostic data, fraud monitoring information, security logs, and any other datasets capable of storing, reconstructing, supporting, or reproducing regulated payment transactions.

4. What evidence will be required to demonstrate compliance with the data localisation requirements?

Answer

Institutions should maintain adequate documentary, operational, technical, governance, and audit evidence capable of demonstrating ongoing compliance with the Circular.

Examples of such evidence may include architecture diagrams, data-flow maps, asset inventories, system configurations, cloud deployment records, governance frameworks, internal policies, risk assessments, audit reports, vendor agreements, service level agreements, access control records, monitoring logs, cybersecurity records, incident reports, compliance attestations, business continuity documentation, disaster recovery arrangements, and other documentation necessary to substantiate compliance. Institutions should be capable of demonstrating compliance on a continuous basis and not solely for periodic examinations.

5. Can third-party providers host regulated payment transaction data?

Answer: YES

Regulated institutions may engage cloud service providers, infrastructure service providers, outsourced technology providers, processing companies, switching companies, and other third-party service providers to support their operations.

However, such arrangements do not transfer regulatory responsibility. The regulated institution remains fully accountable for ensuring compliance with applicable laws, regulations, circulars, guidelines, and supervisory requirements. Institutions are expected to maintain robust vendor governance frameworks, conduct comprehensive due diligence, establish contractual safeguards, maintain audit and inspection rights, and ensure that third-party arrangements support data localisation, cybersecurity, business continuity, operational resilience, and regulatory access requirements.

6. Can payment transaction data be processed outside Nigeria?

Answer: NO

The directive is that payment transaction data must remains subject to Nigerian governance, operational control, security protections, accessibility requirements, and regulatory oversight throughout its lifecycle, including collection, processing, storage, retention, archiving, retrieval, and destruction.

7. Can backup and disaster recovery environments be located outside Nigeria?

Answer: NO

Backup environments, disaster recovery sites, archives, business continuity repositories, and replicated databases should all be located within Nigeria.

Data localisation objectives cannot be fully achieved if regulated payment transaction data is routinely retained outside Nigeria through backup, archival, replication, or disaster recovery arrangements.

8. Can remote support arrangements compromise compliance?

Answer: YES/NO

Remote support needs CBN approval. However, institutions must ensure that such arrangements do not result in unauthorized offshore storage, replication, migration, synchronization, retention, or transmission of regulated payment transaction data.

Permissioned remote support activities such as troubleshooting, vendor-assisted maintenance, cybersecurity monitoring, incident response, and technical support may be permissible via CBN approval where appropriate governance arrangements, monitoring controls, access restrictions, audit trails, security safeguards, and accountability mechanisms are implemented and maintained. Institutions remain responsible for demonstrating that such arrangements do not undermine the objectives of the Data Localisation requirements.

9. What cloud deployment models are acceptable?

Answer: Any cloud deployment model may be used if it complies with the Circular.

The CBN adopts a technology-neutral approach and does not prescribe specific vendors, platforms, or deployment architectures. Accordingly, public cloud, private cloud, hybrid cloud, community cloud, and multi-cloud deployment models may be utilized, provided they comply with Data Localisation requirements.

Regardless of the deployment model adopted, institutions remain responsible for ensuring compliance with Data Localisation requirements, governance obligations, operational resilience expectations, cybersecurity standards, regulatory access requirements, business continuity arrangements, auditability expectations, data sovereignty objectives, and supervisory requirements.

10. What obligations apply to third-party service providers?

Answer

Third-party service providers supporting regulated payment activities are expected to operate within governance, operational, security, and compliance arrangements that support the requirements of the Circular.

Regulated institutions should conduct thorough due diligence, establish effective vendor governance programmes, maintain contractual protections, preserve regulatory access and audit rights, monitor service-provider performance, validate compliance representations, and implement appropriate risk-management measures. Regardless of outsourcing arrangements, accountability for compliance remains with

the regulated institution.

11. What role can local infrastructure providers play in supporting Data Localisation?

Answer

Local infrastructure providers play an important role in supporting the achievement of Data Localisation objectives through investments in data centres, cloud infrastructure, cybersecurity solutions, network infrastructure, hosting environments, disaster recovery facilities, managed services, and other digital infrastructure capabilities.

Such investments can contribute to data sovereignty, operational resilience, business continuity, cybersecurity preparedness, domestic capacity development, innovation, and economic growth.

The Bank recognizes the importance of private-sector participation and welcomes investments that strengthen Nigeria's digital infrastructure ecosystem. However, engagement with stakeholders should not be interpreted as regulatory approval, endorsement, accreditation, or certification of any specific provider, product, platform, or solution.

12. Which Nigerian data centres or cloud infrastructure providers is the CBN currently evaluating or considering for hosting its locally resident workloads? What minimum standards must these facilities meet before they can host critical CBN data?

Answer

Any CBN regulated entity considering sourcing a data centre or cloud infrastructure provider must ensure that it is a provider that is certified by Nigerian Communication Commission and supervised by Nigeria Information Technology Development Agency.

13. Beyond the banking sector, does the CBN intend to engage the Federal Government, ministries, departments and agencies (MDAs) to encourage or require the localisation of critical government data and workloads? If so, what role does the CBN envisage for itself in driving a broader government-wide data localisation strategy?

Answer

The Central Bank of Nigeria’s (CBN) statutory mandate is strictly confined to the financial services sector, meaning it does not have the direct authority to dictate data policies for other Federal Government Ministries, Departments, and Agencies (MDAs). However, the CBN envisages its Data Localisation Mandate (which goes into full effect on January 1, 2027) as a market-making catalyst. By forcing banks, fintechs, and payment processors to domesticate their workloads, the apex bank is intentionally creating the economies of scale needed to support a broader, government-wide data sovereignty strategy.

Rather than acting as a direct regulator of MDAs, the CBN plays a strategic, collaborative role in conjunction with Nigeria Information Technology Development Agency in driving a National Sovereign Cloud Strategy.

14. **European governments have increasingly pursued digital sovereignty by supporting local cloud infrastructure and, in some cases, providing funding or other forms of support to cloud providers to develop capabilities that meet international standards. Is the CBN considering any financing, incentives, guarantees or other support mechanisms to help qualified Nigerian cloud and data-centre operators build the capacity required to host critical financial and government workloads locally?**

Answer

The Central Bank of Nigeria (CBN) is not offering direct financing, financial guarantees, or subsidies to data center operators and cloud infrastructure providers. Instead, the CBN is using regulatory-driven demand as its primary mechanism to encourage private capital and foreign direct investment (FDI) into the sector.

15. **What does the CBN believe are the biggest barriers to achieving full data localisation in Nigeria and what specific measures is the Bank taking with other government agencies to address these gaps before the localisation deadline?**

Answer

The CBN and broader industry assessments identify key operational, regulatory, and infrastructural hurdles to full data localisation, along with coordinated inter-agency steps being deployed to eliminate these gaps.

Challenge to Full Localisation may include:

- **Downtime management during migration:** While older Tier-1 commercial banks historically localized their primary systems, newer digital banks and fintechs engineered their core software directly onto offshore hyper-scaler public clouds. Migrating complex microservices without triggering zero-downtime banking system disruptions presents execution friction. System integrator companies will help with the phased migration plan to minimise downtime.
- **Mitigating a "1% Failure Rate" During High-Volume Activity:** With Nigeria's electronic payment transactions scaling significantly, the migration cannot be treated as a routine upgrade. Dropping even 1% of transactions during live database relocations presents substantial systemic risk to national payment stability as such, migration should take place during off-peak period with substantial safeguards.

16. **How will payment data on cross-border transactions be treated, including card-scheme acquiring, remittances, correspondent banking, SWIFT and cross-border settlement and chargebacks?**

Answer

Where processing by international card schemes, correspondent banks, remittance partners, payment networks, SWIFT infrastructure, or other legitimate third parties are necessary to complete a transaction, only the data required for those purposes should

be transmitted but stored and managed within Nigeria. Also, information exchanged with international counterparties for chargeback management, fraud investigations, or dispute resolution may continue to be shared where operationally necessary and subject to applicable legal, regulatory and security controls.

17. How will institutions that are part of international groups, or that host under existing CBN no-objection approvals, transition to the requirement?

Answer

The Central Bank of Nigeria recognizes that some regulated institutions operate as part of international banking, financial technology, or payment-service groups and may currently rely on shared regional or global infrastructure. Such institutions should ensure that their arrangements ensure their data is stored, processed, managed within Nigeria and complies with other data localisation requirements.

18. How should institutions treat existing multi-year contracts with cloud and hosting providers

Answer

The Central Bank of Nigeria recognizes that some regulated institutions have existing multi-year contractual arrangements with cloud service providers, hosting providers, software-as-a-service (SaaS) vendors, and group infrastructure operators that were entered into before the issuance of the data localisation requirements. Existing contracts do not exempt institutions from compliance. Regulated institutions remain responsible for ensuring compliance with the data localisation requirements by the applicable compliance date, irrespective of the duration or commercial terms of existing contracts. Standard cloud agreements often give the provider a liability shield regarding where data sits.

19. Is there sufficient local data centre, cloud, power and connectivity capacity for the sector's demand, and how will capacity be extended beyond Lagos?

Answer: YES

Based on evidence gathered through the pre-event surveys and discussions at the CBN–NITDA Executive Regulatory Dialogue held on October 28, 2026, with the industry, there is currently sufficient local capacity to support a significant proportion of financial-sector workloads, However, capacity is unevenly distributed, concentrated largely in Lagos. While industry veterans maintain that foundational capacity exists to support the compliance shift, significant friction points remain regarding power reliability and geographical distribution.

Connectivity is Nigeria's strongest asset. With multiple subsea cables landing on the shores of Lagos, the country possesses massive international bandwidth.

Currently, over 75% of Nigeria's data centres are concentrated in Lagos due to historical proximity to subsea cable landing points. However, hosting mission-critical financial workloads locally requires geographic redundancy - a primary database in Lagos cannot use a backup system located in the same city based on international best-practice. Inland expansion is anchored heavily by the public sector providing

Abuja and Kano as government-grade colocation and cloud backup.

The national grid remains highly fragile, managing a stable output of only 4,000–6,000MW against massive nationwide demand. Consequently, local data centres cannot rely on the grid. They operate effectively as independent power plants, burning millions of standard cubic feet of gas or diesel daily to guarantee 99.99% uptime.

20. Will phased, risk-based compliance be permitted, and how will institutions unable to comply fully by 1 January 2027 be treated?

Answer: NO

The Central Bank of Nigeria recognizes that regulated institutions are at different stages of readiness and that implementation complexity varies significantly depending on an institution's size, business model, technology architecture, third-party dependencies, and the extent of existing offshore hosting arrangements.

The implementation date of 1 January 2027 remains in force. During the CBN–NITDA Executive Regulatory Dialogue held on October 28, 2026 in Lagos, the CBN reconfirmed that the deadline stands and that compliance with the Circular is a regulatory requirement.

The circular provides no automatic grace period, published transitional regime, or formal grandfathering for legacy systems past the deadline. The regulatory stance on phased implementation and the treatment of lagging institutions follows a strict enforcement framework:

This FAQ document is intended to support interpretation, enhance understanding and implementation of the Circular. It is not a replacement, neither does it override the Circular or any applicable law. In the event of any inconsistency, the Circular and applicable laws will prevail.