DIGITSPOT SOLUTIONS LTD

APPROACH PAPER

The Digitspot approach to CBN payment-data localisation

Prepared for Nigerian microfinance banks · CBN data localisation · 19 November 2026

CBN circular PSS/DIR/PUB/CIR/001/004 requires payments transaction data generated in Nigeria to be stored and managed in Nigeria from 1 January 2027. This document explains how we read the requirement, what it means in practice for a bank running on AWS (or planning to), and the five-step method we use to get institutions compliant before the deadline without moving more than they need to.

> This is our technical and operational reading, not legal advice. We ask every client to have counsel confirm the interpretation before final sign-off. Where the circular is silent, we say so rather than guess.

1. The short version

- The obligation sits with the licensed institution. It cannot be passed to a cloud provider, a core banking vendor or a group IT team.
- "Stored **and managed** in Nigeria" covers more than the database. The application that processes payments, its logs, queues, caches, backups, disaster recovery copies, and the people and systems who administer it all need a Nigerian answer.
- It does not cover everything. HR, marketing, the company intranet, source code and payload-free monitoring can stay where they are. Over-localising is a cost decision, not a compliance requirement.
- On AWS, the AWS Local Zone in Lagos can host the payment path today, with nothing to order. It does not offer every AWS service, so some components are rebuilt in a self-managed form. We know exactly which ones, and how to stop the AWS plumbing quietly copying data back out of the country.
- Resilience has to be built inside Nigeria too. CBN has said localisation and resilience are not the same thing and that it expects both.
- The date is fixed. CBN has said publicly, more than once, that 1 January 2027 will not move.

2. What the circular actually says

The data-localisation measure is two sentences long:

> *"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."*

> *"All affected Financial Institutions shall fully comply with this requirement effective January 1, 2027."*

Everything else in the market is interpretation. This is ours, phrase by phrase.

PHRASE	WHAT IT MEANS	WHAT IT IMPLIES FOR YOU
All Financial Institutions and participants facilitating payments within Nigeria	Scope is set by activity, not licence class or country of incorporation	Microfinance banks are named recipients. Your payment vendors are participants too
shall ensure	The duty is the institution's	Contracts with vendors help you prove it, they do not transfer it
payments transaction data	Not defined by CBN	Anything needed to reconstruct, dispute or audit a payment (section 3)
generated within Nigeria	Where the transaction originates	A transfer started by a customer in Nigeria is in scope even if one leg is abroad
stored	Every copy at rest	Replicas, backups, snapshots, DR copies, logs, exports and analytics copies, not just the primary database
and managed	Processing, administration and access	The application tier, the administrators and the people with login access must also be in Nigeria
in Nigeria	Physical location	The circular does not say who must own the facility (see section 4)
in accordance with data protection laws	The Nigeria Data Protection Act 2023 and the NDPC GAID 2025 apply on top	Any payment data that still leaves Nigeria is a cross-border transfer needing an NDPA basis
fully comply effective January 1, 2027	Not "by", "effective"	You must already be compliant on that morning. There is no transition period

3. What counts as payments transaction data

CBN has not published a definition. The working test we use with clients:

> If deleting the record would make it impossible to reconstruct, dispute or audit a payment, treat it as payments transaction data.

For a microfinance bank, that typically includes:

- The core banking ledger: accounts, balances, postings, loan disbursements and repayments, interest and fee entries
- Channel transactions: mobile app, internet banking, USSD, agent banking and POS
- NIBSS NIP and other switching records, settlement and reconciliation files

- Card data attached to transactions, authorisation and authentication records, OTP and device-binding logs
- Statements, transaction reports and regulatory returns built from the above
- KYC and BVN data linked to Nigerian accounts (arguably customer data rather than transaction data, but every legal reading we have seen advises treating it as in scope, and the NDPA covers it regardless)
- The technical copies: application logs and traces that contain payloads, message queues, caches, backups, snapshots, data-warehouse extracts and spreadsheets on staff laptops

What is usually out of scope, and can stay where it is: HR and payroll, marketing and CRM without transaction content, the corporate website, internal wikis and email that carries no statements or transaction detail, source code and build pipelines, and monitoring metrics with no payment fields.

4. What the circular does not say

Clients are often told the circular requires things it does not. It is silent on:

- A definition of payments transaction data
- Any list of approved infrastructure, certification, or mention of cloud, hyperscalers or local availability zones
- Backups, disaster recovery or replication (although "stored" and CBN's public "full lifecycle" comments cover them in practice)
- Foreign staff access, group-shared platforms and outsourcing
- An attestation form, audit template or penalty schedule. The circular refers to supervisory sanctions under applicable law

The open question: does an AWS Local Zone count as "in Nigeria"? The plain text says yes: it is physical infrastructure in Lagos. CBN has not confirmed this in writing, and some local data-centre operators argue for a stricter "Nigerian-owned facility" reading. Our position is to build on the plain-text reading, document the physical location, keep encryption keys under the bank's control, and design so that the same work carries over to an AWS Outposts rack or a Nigerian colocation facility if CBN later takes the strict view. We will tell you plainly if that guidance changes.

5. Questions we are asked most

QUESTION	OUR ANSWER
Can we stay in Ireland or the US and just encrypt everything?	No. The circular is about location, not confidentiality. An encrypted copy abroad is still stored abroad, and encrypted personal data is still personal data under the NDPA.
Can the application run abroad with the database in Lagos?	No. The service that reads and writes the data is managing it, and it holds payment data in memory, logs, traces and queues. It is also slower: every request would cross continents twice inside NIBSS timeouts.
Can we split the database and move only the financial tables?	Only by workload, never by table. A system that genuinely never touches payments can stay with its own database. Splitting one transactional database across countries creates cross-border joins and two-phase commits on a ledger.

QUESTION	OUR ANSWER
Can backups or DR go to Cape Town or Europe?	No. Another region is another country. Backups and the DR site must be in Nigeria. On AWS this needs care, because some default backup mechanisms write to the parent region (section 7).
Our core banking system is provided by a vendor. Is that our problem?	Yes. Ask the vendor in writing where production, backups, DR and support access sit. If any are offshore, you need a migration plan from them or an alternative.
What about SaaS tools and APIs we call?	Each one is a data flow. A Nigerian-hosted service is fine. A foreign SMS, email, fraud, analytics or support tool that receives transaction details needs to be replaced, have the payment fields removed, or be documented with an NDPA transfer basis and an accepted risk.
Who is allowed to log in?	Every person and machine identity with access to payment data is part of "managed". Offshore administrators, group SOC tooling and vendor support access all need an answer. On AWS, the Nitro system and customer-managed encryption keys address provider operator access.
Is localisation enough?	No. CBN expects the institution to be able to access, protect and recover the data and continue operating when something fails. The NDPA, and CBN's cybersecurity framework, apply in parallel.

6. Our method: five steps

Every engagement follows the same five steps. Only the answers differ from one institution to the next.

STEP	WHAT WE DO	WHAT YOU GET
1. Classify	List every system and mark it payment path, payment-adjacent (reports, analytics, notifications, support tools that carry payloads) or non-payment. Only the first two move. Dormant systems are deleted first	A signed-off system classification
2. Map the copies	For every payment-path system, trace the primary store, replicas, backups, snapshots, logs, queues, exports, vendor calls and human access	A data map where every row has a Nigerian location, or a documented NDPA basis and an accepted risk
3. Choose the landing zone	Match the workload to the right in-country option (section 7)	A target architecture and bill of materials
4. Plug the leaks	Close the routes by which cloud services copy data back out of the country by default: snapshots, logs, load-balancer logs, object storage, managed queues	A design with no hidden offshore copies
5. Build resilience in Nigeria	High availability inside the zone as the floor, a second in-country site as the target, with tested restores	Documented RPO and RTO, restore test results, and a resilience roadmap

We resist both extremes: "move everything" is expensive and unnecessary, and "move only the database" is not compliant.

7. Where "in Nigeria" can be on AWS

OPTION	WHEN IT FITS	WHAT IT OFFERS	LEAD TIME
AWS Local Zone, Lagos	Containers or virtual machines with self-managed databases. The fastest route for 1 January	EC2 compute (T3, C5, M5, R5, G4dn), EBS gp2 storage, ECS on EC2, EKS, Application Load Balancer, Direct Connect at Rack Centre Lagos, Elastic Disaster Recovery	Days. Nothing to order
AWS Outposts in a Lagos colocation facility	Workloads that need managed databases or object storage in country, or a second AWS site in Nigeria	Adds RDS on Outposts, S3 on Outposts and local EBS snapshots	Weeks to months, multi-year commitment, Tier III facility needed
Nigerian colocation or local cloud	Appliance or licensing constraints, a strict "Nigerian-owned facility" reading, or an independent second site	Whatever the provider offers; often used for the backup vault or DR copy	Varies by provider

For most microfinance banks we recommend the Lagos Local Zone as the primary site for 1 January, with a second in-country site (Outposts or colocation) added in the first quarter of 2027.

What the Lagos Local Zone does not offer, and what we use instead

NOT AVAILABLE IN THE LAGOS ZONE	OUR REPLACEMENT
Amazon RDS (PostgreSQL, SQL Server, MySQL)	Self-managed database on EC2 with a standby on a separate host and automatic failover. SQL Server licence-included EC2 is available in the zone
AWS Fargate	ECS on EC2: same container images and task definitions, new capacity provider
Amazon S3	An object store we run inside the zone, or S3 on Outposts
Amazon SQS and AWS Lambda	Worker containers on ECS with a queue in the zone (a database job table, RabbitMQ or Redis Streams)
Amazon ElastiCache	Redis on EC2 in the zone
NAT Gateway	NAT instance in the zone
Site-to-Site VPN	Software VPN on EC2, or Direct Connect at Rack Centre Lagos
Elastic Beanstalk, Amazon SES	Containerised services on ECS; a Nigerian mail provider, or notifications without transaction detail

The leaks we close

These are the defaults that copy data back to the parent region in Cape Town. Most local providers do not know about them.

- **EBS snapshots.** Snapshots of Lagos volumes are stored in Cape Town. We back up databases with in-zone tools to in-zone storage and do not snapshot payment-data volumes.
- **CloudWatch Logs.** Logs that carry payloads are payment data. Payload-bearing logs stay in a log store inside the zone; only redacted metrics go to CloudWatch.
- **Load balancer access logs.** These write to S3 in the region. We switch them off or confirm they carry no payment fields.
- **Container images and control plane.** ECR images, the ECS scheduler, IAM and KMS keys live in the region. They hold code and configuration, not transaction data, and we document that. Banks that want zero key dependency outside Nigeria can use AWS KMS External Key Store with an HSM in Lagos.
- **Capacity.** Lagos capacity is thinner than a full region. We size on instance types we have proven launch reliably there and recommend capacity reservations for production.

8. What we build

Our Lagos reference architecture is written in Terraform and has been deployed and tested end to end in the Lagos Local Zone. For a typical microfinance bank it includes:

- An Application Load Balancer in Lagos serving the bank's API and channel endpoints
- ECS on EC2 running the bank's services across multiple hosts, so one host failure does not take a service down
- A primary and standby database on separate hosts with automatic failover
- Encrypted backups to a backup host and an object store, both inside the zone, with a tested restore before cutover
- A log store inside the zone for payload-bearing logs, with redacted metrics only to CloudWatch
- Private subnets for every data store and core banking host, with no administrative ports open to the internet
- A NAT instance and, where needed, VPN or Direct Connect to NIBSS, switches and partners
- Customer-managed encryption keys and an access matrix listing every identity with access to payment data and where it works from

Indicative run cost for a minimal highly available footprint starts at around USD 3,500 per month at Lagos on-demand prices, before Savings Plans. Actual sizing follows discovery. Removing the offshore estate, and the dormant systems we usually find, offsets part of this.

9. What microfinance banks should check now

- **Core banking provider.** Where are production, backups, DR and vendor support access hosted? Get it in writing.
- **Channels.** Where do the mobile app, internet banking, USSD and agent banking back ends run? USSD aggregators and SMS gateways often sit offshore.
- **Card and switching partners.** Confirm their hosting and what fields you send them.

- **Notifications.** SMS and email alerts usually carry amounts, balances and references.
- **Reporting and exports.** Where do statements, regulatory returns and finance extracts go: email, shared drives, staff laptops?
- **Access.** Who outside Nigeria (group IT, vendors, contractors) can log in to production systems or databases?
- **NDPA status.** NDPC registration, Data Protection Officer, and transfer instruments for any residual cross-border flows.

10. Timeline to 1 January 2027

Six weeks remain. That is tight but achievable for the payment path, because our landing zone is already built and proven. The order of work:

WEEK	WORK	EXIT CRITERION
1	Discovery: system classification, data map, vendor hosting, access list	Signed-off inventory
1 to 2	Build the Lagos landing zone from our reference architecture	Non-production stack running in Lagos
2 to 4	Migrate non-production, test the payment path, prove a restore	Regression passed in Lagos
4 to 5	Replicate production data, rehearse and then perform the cutover in a low-traffic window	Production serving from Lagos
6	Remove payment data from offshore locations, assemble the evidence pack	Evidence pack ready
Q1 2027	Second in-country site for resilience	Documented and tested DR inside Nigeria

Anything that cannot be finished by 1 January (for example a vendor that cannot relocate in time) goes into a written remediation plan with dates and an interim control, so the bank can show CBN exactly where it stands.

11. The evidence pack

Expect CBN to start compliance reviews in January. We hand over:

- The system classification and data map
- The target architecture and the as-built configuration showing every payment-data resource in the Lagos zone
- Backup locations, retention and restore test results
- The access matrix: every identity with access to payment data and its location
- Vendor hosting confirmations
- AWS compliance reports from AWS Artifact and the physical facility details
- Residual cross-border flows, each with its NDPA basis

12. What we usually find along the way

Localisation projects surface security issues that would fail a CBN examination on their own, and the migration is the cheapest time to fix them: databases and servers open to the internet, audit logging (CloudTrail) switched off, production payment services on interruptible capacity, unowned databases and stale backup exports in storage buckets. We fix these as part of the move.

13. Getting started

To begin, we need:

1. An architecture diagram or a read-only view of your AWS accounts
2. The list of systems, vendors and integrations on the payment path
3. Database sizes, growth and peak transaction rates
4. Current backup locations and RPO and RTO targets
5. The list of people and systems with access to production data, with their location
6. Any correspondence with CBN or counsel on the circular

We then send a discovery questionnaire and a first classification for you to correct, usually within two working days.

Digitspot Solutions Ltd · AWS Partner