# Data Localization Laws: Nigeria

**by Jumoke Lambo, Babatunde Olayinka, Chisom Okolie, and Itoro Etim, Udo Udoma & Belo-Osagie with Practical Law Data Privacy Advisor**

Country Q&A | Law stated as of 11-Jun-2021 | Nigeria

A Q&A providing a high-level summary of key data localization requirements in Nigeria. It identifies applicable laws, sector-specific requirements, exceptions, and cross-border data transfer requirements.

1. What are the key data localization laws in the jurisdiction?

The key data localization laws in Nigeria are:

- The Central Bank of Nigeria's mandatory 2011 Guidelines on Point of Sale (POS) Card Acceptance Services:
    - Guideline 4.4.8 requires entities engaging in point of sale (POS) card acceptance services in Nigeria to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic POS and ATM transactions. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers.

- The National Information Technology Development Agency's (NITDA) mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), which aim to encourage indigenous innovation, develop the local ICT industry, and establish intellectual property and data regulation and protection standards, each of which has a set of related strategic goals:
    - Guideline 9.1 requires all Indigenous Original Equipment Manufacturers (companies that produce functional computer devices from component parts bought from other organizations) to assemble all hardware in Nigeria and maintain fully staffed facilities for that purpose.
    - Guideline 11.1(4) requires all telecommunications companies to host all subscriber and consumer data in Nigeria.
    - Guideline 12.1(4) requires all network service companies to host all subscriber and consumer data in Nigeria.
    - Guideline 12.2(1) requires all ministries, departments, and agencies of Nigeria's federal government (MDAs) to host their websites locally and under a registered.gov.ng domain.
    - Guideline 13.1(2) requires all data and information management companies to host all sovereign data in Nigeria.

 

    - Guideline 13.2(3) requires MDAs to host all sovereign data locally on servers within Nigeria.

- The Nigerian Communications Commission's Registration of Telephone Subscribers Regulations, 2011:
    - Article 4 requires the Commission to maintain at its domicile a central database of all registered subscribers' personal information.

## 2. What do the data localization laws cover?

The Central Bank of Nigeria's 2011 Guidelines on Point of Sale (POS) Card Acceptance Services (POS Guidelines) cover all domestic transaction data of cardholders in Nigeria. A cardholder is any person issued a payment card whose account will be debited to settle transactions performed with the payment card. (Guideline 4.4.8 and Appendix 1(b), POS Guidelines.)

The National Information Technology Development Agency's (NITDA) Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (NITDA ICT Guidelines) cover:

- Subscriber and consumer data hosted by telecommunications companies, network service companies, and ICT companies.
- Sovereign data hosted by ministries, departments, and agencies of Nigeria's federal government and information management companies.

(Guidelines 11.1(4), 12.1(4), 13.1(2), and 13.2(3), NITDA ICT Guidelines.)

The Nigerian Communications Commission's Registration of Telephone Subscribers Regulations, 2011 (Telephone Regulations) covers data within the Commission's central database, which includes the biometric and personal information of all persons who subscribe to mobile telecommunication services by purchasing a subscription medium or entering into a subscription contract (Article 1, Telephone Regulations). Personal information includes:

- Name, including mother's maiden name.
- Gender.
- Date of birth.
- Residential address.
- Nationality.
- State of origin.
- Occupation.

 

- Other personal information and contact details specified in the registration specifications.

(Article 1, Telephone Regulations.)

### 3. To which sectors, individuals, and entities do the data localization laws in the jurisdiction apply?

The localization requirement under the Central Bank of Nigeria's 2011 Guidelines on Point of Sale (POS) Card Acceptance Services (POS Guidelines) applies to:

- Merchant acquirers.
- Card issuers.
- Merchants.
- Cardholders.
- Card schemes and card associations.
- Switches.
- POS terminal owners.
- Payments terminal service aggregators.
- Payments terminal service providers.
- Processors.

(Guideline 2 and Appendix 1, POS Guidelines.)

The localization requirements under the National Information Technology Development Agency's (NITDA) Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (NITDA ICT Guidelines) apply to:

- Federal, state, and local council ministries, departments, and agencies in the executive, legislative, and judiciary branches.
- Private sector institutions.
- Business enterprises.
- Individuals.

(Guideline 4.0, NITDA ICT Guidelines.)

The localization requirement under the Nigerian Communications Commission's Registration of Telephone Subscribers Regulations, 2011 (Telephone Regulations) applies to:

 

- Corporate, private, and commercial subscribers of mobile telephone services using subscription mediums in Nigeria
- Subscribers of foreign licensees who roam the network of a licensee in Nigeria.

(Article 3, Telephone Regulations.)

4. What are the main exemptions from the application of the data localization laws?

Article 10(4) of the Nigerian Communications Commission's Registration of Telephone Subscribers Regulations, 2011 allows the transfer of subscriber information outside Nigeria with the Commission's prior written consent.

There are no exemptions under Nigeria's other data localization laws.

5. Do the data localization laws allow for cross-border transfers after storing the data in the jurisdiction? If yes, what are the requirements for transferring data outside of the jurisdiction?

Guideline 13.1(2) of the National Information Technology Development Agency's (NITDA) Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) allows for cross-border transfers or hosting of sovereign data with NITDA's express approval after storing data in Nigeria.

Guideline 13.1(2) provides that NITDA will consider the following in giving its express approval to cross-border transfers or hosting of sovereign data:

- Compliance with the Nigeria Data Protection Regulation 2019 for transfers involving personal data.
- The implication of NITDA's Nigeria Cloud Computing Policy (2019).
- A guarantee that the Nigerian government has unfettered right to access and retrieve its data wherever it is located.
- A commitment to non-disclosure of Nigeria’s government data to any third party without express consent.
- A guarantee of adequate and appropriate data security processes, which NITDA must review and accept before giving approval.
- That the Nigerian government can chose the jurisdiction where data will be hosted.
- An agreement to periodic submission of third-party audit reports for NITDA's review.

 

- Whether the service to be offered to the government is Software as a Service (SaaS) to improve its efficiency or performance.
- Where small- and medium-scale enterprises offer service to the government from a public cloud environment, whether the National Digital Marketplace has registered and verified the service.
- Whether a ministry, department, or agency of Nigeria's federal government is responsible for backing up data in a public cloud.

The Central Bank of Nigeria's 2011 Guidelines on Point of Sale (POS) Card Acceptance Services and the Nigeria Communications Commission's Registration of Telephone Subscribers Regulations, 2011 do not address cross-border transfers.

**END OF DOCUMENT**

 