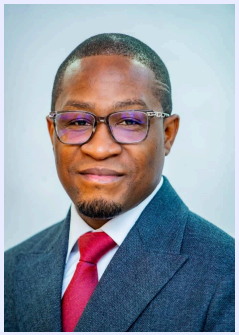
Key Factors for Nigerian Startups to Consider Before a Cross-Border Transfer of Data



GODSON OGHENEOCHUKO
Partner

AANUOLUWAPO ODUNAIKE
Senior Associate

OPEYEMI ADESHINA
Associate

u-law @ulawsocial

When founders chart their expansion beyond Nigeria, they typically envision physical milestones: opening foreign offices, setting up offshore structures, and onboarding international users. The reality is far less synchronised. In today's digital economy, a firm's operational and regulatory footprint can go international long before its expansion strategy does.

Consider a few common scenarios that illustrate this invisible transition. Personal data collected from local customers or employees may already be stored on offshore cloud servers managed by global giants, placing that information physically outside Nigerian borders. Similarly, a foreign Software-as-a-Service (SaaS) vendor or international payment processor may be analysing information on behalf of the Nigerian business. Even giving remote system access to an overseas technical consultant, a remote developer, or an affiliate company for routine operations constitutes an international data flow, potentially triggering key obligations under Nigerian data protection law. In each of these everyday tech setups, protection must travel with the data, legally transforming a local startup into a cross-border data exporter long before its physical expansion begins.

What Exactly is a Cross-Border Data Transfer?

A cross-border data transfer occurs when personal data is transferred outside Nigeria or made accessible to a person, organisation, or system located outside Nigeria.

Personal data includes any information that can identify an individual, whether directly or indirectly. This may include names, email addresses, telephone numbers, identification numbers, financial information, location data, and other information relating to an identifiable person. The concept is broader than many businesses realise. A transfer may occur not only when data is intentionally shared with another organisation, but also where personal data is stored, processed, or accessed outside Nigeria.

Why Does the Law Care?

Imagine a customer shares their personal information with your business because they trust you to handle it responsibly. That expectation does not disappear simply because the information is transferred to or accessed from another country.

The Nigeria Data Protection Act, 2023 ("NDPA") and the General Application and Implementation Directive, 2025 ("GAID") seek to ensure that personal data continues to enjoy an appropriate level of protection even after it leaves Nigeria. For this reason, the responsibility for protecting personal data does not end at the Nigerian border. Organisations transferring personal data remain responsible for ensuring that the transfer is lawful and that appropriate safeguards are in place to protect the information.

In practical terms, a Nigerian business cannot assume that its compliance obligations end once personal data leaves its systems. If something goes wrong, the fact that the data is being stored, processed, or accessed outside Nigeria will not necessarily absolve the organisation of responsibility.

When Can Personal Data Be Transferred Outside Nigeria?

The NDPA does not prohibit cross-border transfers of personal data. However, organisations must ensure that such transfers take place in accordance with the safeguards and conditions prescribed under the NDPA and the GAID.

As a starting point, a data controller or data processor transferring personal data outside Nigeria must ensure that the personal data will continue to receive an adequate level of protection. To achieve this, the NDPA recognises a number of safeguards, including binding corporate rules, contractual clauses, approved codes of conduct, certification mechanisms, and other recognised arrangements capable of protecting the rights and freedoms of data subjects. The GAID refers to these safeguards collectively as Cross-Border Data Transfer Instruments ("CBDTIs").

Where adequate protection cannot be demonstrated through appropriate safeguards, the NDPA permits transfers in certain specific circumstances, including where:

- the data subject has explicitly consented to the transfer after being informed of any associated risks;
- the transfer is necessary for the performance of a contract involving the data subject;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise, or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent; or
- the transfer is made from a public register in accordance with applicable legal requirements.

Organisations should not view cross-border transfers as merely a contractual or administrative exercise. The GAID requires organisations to identify and justify the legal ground for any cross-border transfer, and to implement appropriate technical, organisational, and contractual measures to safeguard personal data before, during, and after the transfer.

Accordingly, before transferring personal data outside Nigeria, businesses should assess:

- the legal basis for the transfer;
- the safeguards or CBDTIs supporting the transfer;
- the risks associated with the transfer; and
- the measures implemented to protect the rights and interests of affected data subjects.

A well-documented transfer assessment can help organisations demonstrate accountability and reduce regulatory risk where personal data moves across borders.

Key Considerations for Start-Ups and SMEs

For many businesses, cross-border transfers arise in the ordinary course of business. Customer information may be stored on infrastructure located outside Nigeria, foreign service providers may process personal data on behalf of the business, or personnel located outside Nigeria may require access to personal data for operational purposes.

In these circumstances, organisations should pay close attention to the legal basis for the transfer and whether appropriate safeguards have been implemented. Where a transfer relies on contractual arrangements, businesses should ensure that such arrangements adequately address data protection obligations and reflect the requirements of the NDPA and the GAID. Organisations should also ensure that data subjects are adequately informed about the processing of their personal data, including any intended cross-border transfers, through clear and transparent privacy notices.

Periodic reviews of data processing activities are equally important. Such reviews can help organisations identify instances where personal data may be transferred outside Nigeria and assess whether additional safeguards, including appropriate CBDTIs or regulatory approval, may be required. Organisations should also maintain adequate records demonstrating the legal basis for the transfer, the safeguards relied upon, and the assessments undertaken in support of the transfer. This will help demonstrate accountability and compliance in the event of regulatory scrutiny.

Failure to properly assess cross-border transfers may expose organisations to regulatory scrutiny, enforcement action, reputational damage, and loss of stakeholder trust.

Conclusion

Cross-border data transfers are a common feature of modern business operations, particularly in a digital economy where cloud infrastructure, global service providers, and distributed teams are the norm. Remember that the obligations imposed by Nigerian data protection law do not disappear because the personal data is not stored or being accessed in Nigeria. Organisations remain accountable for the protection of such data, regardless of where it is stored, processed, or accessed.

The NDPA and the GAID require organisations to ensure that personal data transferred outside Nigeria receive adequate protection and that appropriate safeguards are implemented where necessary.

For start-ups, addressing cross-border transfer issues early can help avoid compliance challenges as the business grows, avoid costly remediation efforts for breaches, and demonstrate a commitment to responsible data governance and the protection of individuals' privacy rights.