OLANIWUN AJAYI

MAY 2025

# Navigating Cross-Border Data Transfers

## KEY INSIGHTS UNDER NIGERIA'S DATA PROTECTION LAWS

**OALP** Technology Innovation and Fintech Newsletter

### INTRODUCTION

In an increasingly digital and interconnected world, cross-border transfer of personal data plays a crucial role in driving commercial expansion, technological innovation, and global collaboration. Businesses, especially technology-driven enterprises, rely on the seamless exchange of data across jurisdictions to enhance efficiency, minimise operating costs, and improve customer experience. However, as the volume of data transfers rises, so do concerns surrounding privacy and security of personal data.

As Nigeria strengthens its position in the international data ecosystem, understanding the legal and regulatory frameworks governing the cross-border transfer of personal data becomes imperative for organisations as well as data subjects. This article provides an overview of how Nigerian data protection laws address the cross-border transfer of personal data and highlights certain limitations to the transfer of personal data outside Nigeria.

### GROUNDS FOR CROSS-BORDER TRANSFER

Cross-border transfer is the transfer of data from one country to another through file sharing or storing on cloud servers physically located in a different country.

The Nigeria Data Protection Act 2023 (**NDPA** or the **Act**) prohibits data controllers[1] and data processors[2] (**DC/DPs**) from transferring personal data[3] from Nigeria to another country unless specific minimum conditions are met.[4] Where a DC/DP needs to transfer personal data outside Nigeria as part of its processes or operations, it must ensure:

- that the recipient of the personal data is subject to a law that affords an adequate level of protection with respect to the personal data; or
- that the recipient of the personal data is subject to binding corporate rules, contractual clauses, code of conduct, or a certificate mechanism (together, **Cross Border Data Transfer Instruments or CBDTIs**) that affords an adequate level of protection with respect to the personal data;[5] or
- that any of the conditions set out in section 43 of the Act or in the General Application and Implementation Directive 2025 (**GAID**) are met.

Each of the grounds/bases highlighted above will be elaborated upon in the ensuing paragraphs.[6]

#### *Transfer based on Adequacy decision*

A DC/DP may transfer personal data to countries, regions, or specific sectors in other jurisdictions that the Nigeria Data Protection Commission (**NDPC**) has determined to have adequate levels of protection similar to those in the NDPA.[7] In assessing whether a country, region, or sector

1. *Data controller means an individual, private entity, public commission, agency, or any other body that, alone or jointly with others, determines the purposes and means of processing of personal data, Section 65, NDPA.*
2. *Data processor means an individual, private entity, public authority, or any other body that processes personal data on behalf of or at the direction of a data controller or another data processor, Section 65, NDPA.*
3. *Personal data means mean any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual, Section 65, NDPA.*
4. *Part VIII, NDPA.*
5. *Section 41(1)(a), NDPA.*
6. *DCs/DPs are required to record the basis of any personal data transfer and the adequacy of the protection.*
7. *Section 42(4), NDPA.*

meets this 'adequacy' requirement, the NDPC generally evaluates whether the country, region or sector upholds principles that are substantially similar to those governing the processing of personal data under the NDPA,[8] taking into consideration the following factors:[9]

*Availability of Enforceable Data Subjects' Rights*

The NDPC will consider the availability of enforceable data subjects' rights, including the ability of data subjects to enforce their rights through administrative or judicial redress and the presence of the rule of law. For this purpose, the NDPC will prioritise jurisdictions or sectors where:

01 the rights of data subjects are recognised in a statute or subsidiary legislation;

02 dispute resolution fora are reasonably accessible without barriers or undue constraints; and

03 the judicial or administrative platforms operate impartially, independently, and with respect for human rights;[10]

*Inter-agency Instruments*

The NDPC will consider the existence of an appropriate instrument between the NDPC and the data protection authority in the recipient jurisdiction that provides for investigation of data breaches, enforcement of cross-border decisions, and inter-governmental information sharing;[11]

*Functioning Supervisory Authority*

Another point of consideration is the existence of a functioning, independent, competent data protection or similar supervisory authority with adequate enforcement powers. This could be an executive body established by a sovereign authority or an administrative body under the establishment of a sovereign authority[12] provided that the decisions of such body are only subject to adjudication by a court.

*Access to Personal Data*

The NDPC will consider whether any public authority has access to the personal data being transferred offshore. This includes scrutiny of the mode of access, degree of derogation from privacy rights, the extent of the access and whether same is necessary;[13]

*An Effective Data Protection Law*

There should be a statute in force that is: (x) not subject to any overriding law, (y) not likely to be amended to suit transient causes, (z) not likely to be repealed by administrative regulations, and (xx) amendable only to laws that seek the protection of larger freedoms;[14]

*International Commitments*

The NDPC will consider any binding international commitments and conventions that may impact data flows, enforcement of data subjects' rights, and the efficacy of bilateral agreements between Nigeria and the recipient jurisdiction.[15]

*Transfer Based on CBDTI*

Additionally, the NDPA permits DC/DPs to transfer personal data offshore where the transfer is carried out further to a CBDTI. In selecting a preferred CBDTI, DC/DPs must ensure that the CBDTI enables:

- proper monitoring of data flows;
- accountability between or among the transferor(s) and recipient(s) of the personal data;
- access to remedy for data subjects; and
- personal data sovereignty.[16]

Importantly, the CBDTI must be submitted to the NDPC for approval before the DC/DPs can rely on same for the purpose of cross-border transfers. In appraising the proposed CBDTI, the NDPC will consider the results of any data protection audit conducted on the DC/DP by a licensed data protection compliance organisation (**DPCO**), as well as evidence of the DC/DP's adherence to reputable standards of data protection.[17]

8. *Section 42(1) NDPA.*
9. *Section 42(2) NDPA.*
10. *Paragraph 2(a), Schedule 5 GAID.*
11. *Paragraph 2(b), Schedule 5 GAID.*
12. *Paragraph 2(e), Schedule 5 GAID.*
13. *Paragraph 2(c), Schedule 5 GAID.*
14. *Paragraph 2(d), Schedule 5 GAID.*
15. *Paragraph 2(f), Schedule 5 GAID.*
16. *Paragraph 4, Schedule 5 GAID.*
17. *Section 42(5) NDPA, Paragraph 5, Schedule 5 GAID.*

*Transfer based on the Special Conditions*

Lastly, in the absence of an adequacy decision or an approved CBDTI, the NDPA and the GAID permit a DC/DP to transfer personal data outside Nigeria if at least one of the following conditions are in place: upon.

- the data transfer is based on a compelling legal right or duty, different from the DC/DP's business interests;[18] or

- the data subject consented[19] to the transfer, and such consent has not been withdrawn at the time of transfer. For this condition to be met, the data subject must be made aware of any risks in relation to the transfer of data, and there must be a clear indication that the data subject also understands the risks involved;[20] or

- the transfer is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract. Where personal data is required to be transferred prior to the execution of a contract, the DC/DP should ensure an 'agreement in principle' exists with the data subject, that is, a series of affirmative actions by the data subject that leads to a reasonable inference of constructive consent by the data subject;[21] or

- the transfer is for the sole benefit of the data subject,[22]
  - and it is not reasonably practicable to obtain the consent of the data subject and
  - if it was reasonably practicable, the data subject would likely give consent; or

- the data transfer is necessary for reasons of public interest;[23] or

- the data transfer is necessary for the establishment, exercise or defence of legal claims;[24] or

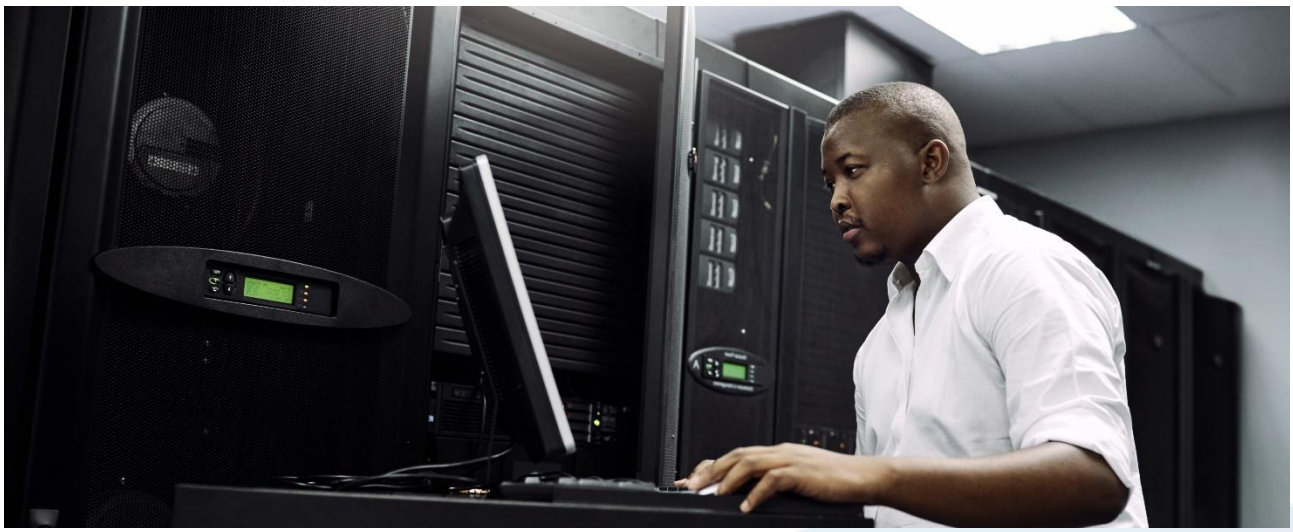
- the transfer is necessary to protect the vital interest of the data subject or of other persons, where a data subject is physically or legally incapable of giving consent.[25]

## FORM OF CBDTIs AND APPLICATION FOR APPROVAL OF CBDTIs

Nigeria currently lacks specific, standardised forms of CBDTIs, in contrast to the United Kingdom (**UK**) which has released template International Data Transfer Agreements (**IDTAs**) and Addendum to the Standard Contractual Clauses (**SCCs**).[26] In light of this, DC/DPs have to submit bespoke drafts of their select CBDTIs to the NDPC for review and approval. In assessing such drafts, the NDPC will take into account the results of a data protection compliance audit carried out on the DC/DP by a DPCO and any demonstrated alignment by the DC/DP with international best practices or recognised data protection standards.

To improve regulatory clarity and promote consistency, the NDPC could consider issuing standard forms of each CBDTI adapted to the Nigerian legal and regulatory context that organisations can adopt or build upon.

18. *Paragraph 6(b) & (c), Schedule 5 GAID.*
19. *Consent is defined under the Act as any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent. Section 65, NDPA.*
20. *Paragraph 6(d)(iv)-(v), Schedule 5 GAID.*
21. *Paragraph 6(d)(vi)-(vii), Schedule 5 GAID.*
22. *Paragraph 6(d)(viii), Schedule 5 GAID.*
23. *Paragraph 6(d)(iii), Schedule 5 GAID.*
24. *Paragraph 6(d)(i), Schedule 5 GAID.*
25. *Paragraph 6(d)(ii), Schedule 5 GAID.*
26. *The International Data Transfer Agreement (IDTA), international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions were issued pursuant to Section 119A of the Data Protection Act 2018 and came into force on 21 March 2022 following Parliamentary approval. The IDTA and Addendum replaced standard contractual clauses for international transfers; Information Commissioner's Office, "International data transfer agreement and guidance" available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/ accessed 12 May 2025.*



## LOCALISATION CONSIDERATIONS

Lastly, although the NDPA recognises that DC/DPs may transfer personal data offshore subject to aforementioned safeguards, cross-border data transfers may be entirely restricted or subjected to prior approval of other regulatory bodies where the sensitivity of the data or the profile of the DC/DP warrants additional regulatory scrutiny. For instance, the Central Bank of Nigeria (**CBN**) requires that Bank Verification Number of customers be hosted within Nigeria's territorial boundaries and prohibits its transfer outside the country without the express consent of the CBN. Similarly, secret, sensitive government and citizen data generated by federal ministries, departments, and agencies, state and local public institutions, or government-owned or affiliated entities must be stored on cloud infrastructure physically located within Nigeria.

## CONCLUSION

The regulation of cross-border personal data transfers in Nigeria plays a critical role in balancing the demands of international trade and economic growth with the growing need for data protection. While the NDPA and the GAID offer a commendable foundation for the regulation of cross-border transfers of personal data, there remains room for improvement. To align Nigeria's data protection regime with global standards, it is essential to draw on the experiences of more developed jurisdictions such as the UK and the European Union. In particular, the issuance of standard-form CBDTIs would bring clarity and consistency to the current framework. Additionally, publication by the NDPC of a detailed list of jurisdictions or sectors deemed to offer adequate protection and regularly updating same would enhance transparency and support businesses in their cross-border operations, while fostering data subjects' rights.

23. *Paragraph 1.11(ii) Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for The Nigerian Banking Industry 2021.*
24. *This data is classified as "sensitive" because the loss of confidentiality, integrity, or availability of the data could have serious, adverse, and material effects on the data subject or related entities; Article 9.0 (iii) Nigeria Cloud Computing Policy 2019.*

# FOR MORE INFORMATION, PLEASE CONTACT:

**Damilola Salawu,**
Partner
*dsalawu@olaniwunajayi.net*

**Hopewell Nwachukwu,**
Senior Associate
*hnwachukwu@olaniwunajayi.net*

**Vwakpo Ekpagha ,**
Associate
*vekpagha@olaniwunajayi.net*

**Ikenna Okpalaeze,**
Associate
*iokpalaeze@olaniwunajayi.net*

**Ifeoluwa Adeniran,**
Associate
*iadeniran@olaniwunajayi.net*