NIGERIA

Cross-Border Sharing of Data

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law is provided. This includes what data the law applies to, the categories of data, the key individuals in the NDPA, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of the NDPA and to begin to assist users in navigating the NDPA. It is not comprehensive, and users of the NDPA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. The Nigeria Data Protection Act (NDPA) is in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. Therefore, it is not a regulation that was introduced specifically to regulate research.

As research processes vast quantities of personal data, the NDPA applies but it is only one of several laws that must be complied with when transferring data for research.

Health Research Regulations and Cross-Border Data Sharing

In addition to the national laws listed below, there are several international treaties and conventions that have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) and the Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS ('the ECOWAS Data Protection Act 2010'). Nigeria has not ratified the Malabo Convention.

The relevant national legislation and guidelines are:

- Constitution of the Federal Republic of Nigeria
- National Health Act
- National Code of Health Research Ethics 2007

These laws set out the legal and ethical requirements that must be met for the conduct of research in Nigeria. There are no extra requirements for the cross-border sharing of data in this legislation.

Nigeria Data Protection Act

In addition to these legal and ethical requirements, the Nigeria Data Protection Act (NDPA) applies to the processing of all personal data, but in acknowledging the importance of research special provisions are in place that deal with the processing of data purely for research purposes given the importance of research. The Nigeria Data Protection Regulation (NDPR) (and other legal instruments made by the National Information Technology Development Agency or the Nigeria Data Protection Bureau) was not repealed by the NDPA. The NDPR is still in force unless the relevant section conflicts with the NDPA. Therefore, it is arguable that the NDPR can be used to supplement the NDPA where there is the need for further clarity on the criteria set out in the NDPA.

In addition to the NDPA, the Nigeria Data Protection Commission has issued some guidance documents, which can be found here:

- Guidance notice: registration of data controllers and data processors of major importance 2023;
- Code of conduct for data protection compliance organisations (DPCOs) 2023

The conditions set out in the NDPA must all be met for research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in the NDPA are discussed below. This is not a thorough assessment of the NDPA as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal data for research.

The Main Actors Defined in the Nigeria Data Protection Act

	Legal definition	**Layman explanation**
Data subject	An individual to whom personal data relates.	The person to whom the data relates.
Data controller	An individual, private entity, public Commission, agency or any other body which, alone or jointly with others, determines the purposes and means of processing of personal data.	The person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).
Data controller or data processor of major importance	A data controller or a data processor who is domiciled, resident in or operating in Nigeria and who processes or intends to process personal data of more	

	than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria, as the Commission may designate.	
Data processor	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.	Someone that is not directly employed by the data controller but who processes personal data under the direction of the data controller (e.g., a consultant).
Data Protection Officer	Not defined in the Act.	An individual who ensures that an institution complies with the Act.
Commission	The Nigeria Data Protection Commission established under the NDPA.	The independent body established to monitor and enforce compliance with the law.

Categories of Data Listed in the Nigeria Data Protection Act

	Legal definition	**Layman explanation**
Personal data	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	Data/information about a particular person, which can identify him or her.
Sensitive personal data	Personal data relating to an individual's (a) genetic and biometric data, for the purpose of uniquely identifying a natural person; (b) race or ethnic origin; (c) religious or similar beliefs, such as those reflecting conscience or philosophy; (d) health status; (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; or h) other information prescribed by the Commission as sensitive personal data under the Act.	Personal data relating to or information about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.

Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis.	
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person	A kind of processing where the direct identifiers of personal data are removed (e.g., a name) so that it is impossible to identify the person without adding other information. This is often called coded data. Data protection law still applies to pseudonymised data.

The NDPA applies to the processing of personal data

Generally, data protection law applies only to personal data. This is data that refers to an identified or identifiable person. For data that does not fall under the definition of personal data, the data protection law does not apply. The NDPA, like many other data protection laws, applies specifically to the processing of personal data.

De-identification and pseudonymisation of personal data

The NDPA refers to de-identification and pseudonymisation. Pseudonymisation is when information is removed from the data so that it is impossible to identify an individual and that information is kept separate by using technical and organisational measures. Data that has been pseudonymised does fall under the NDPA.

Although de-identification is mentioned in the NDPA, it is not defined. De-identification is one of the technical and organisational measures which a data controller may use to ensure the security, integrity and confidentiality of the personal data in its control, in order to guard against inter alia misuse, unauthorised disclosure, or access. In the absence of specific guidance and clarity in the alternative on this point, it seems that de-identified data falls within the NDPA.

If a data controller uses pseudonymisation and de-identification techniques, the data controller is required to regularly test that the measures used are effective, updated when necessary and that any new measures are instituted to address any shortcomings in current methods or to address new risks.

Categories of personal data

Data that is not personal data does not fall under the NDPA. While the exact parameters of what is non-personal is unclear from the NDPA, several types of data are clearly considered personal:

- personal data;
- sensitive personal data (including biometric data);
- pseudonymised data; and
- de-identified data.

The first three types of data (personal, sensitive personal (including biometric) data and pseudonymised data) are defined and an assessment would need to be made to consider whether data falls under these definitions. Unfortunately, given the lack of a definition of de-identified data, it is unclear what qualifies as de-identified data. Furthermore, whether pseudonymisation is merely a safety measure, or whether it amounts to non-personal data in the hands of the data recipient who does not have access to the identifying data set, is unclear.

To determine whether data to be shared is anonymised, it is important to make an assessment, which can be challenging. There is no guidance from the Commissioner on this point, but the data controller may wish to follow the guidance set out to be followed under the GDPR on how to make an assessment to determine whether data has been anonymised – including anonymisation techniques.

The test for anonymisation is always objective, but it can be interpreted in two ways: context-specific (relative approach) or context-agnostic (absolute approach).

As such, the test for determining whether data is anonymised can be approached in two ways:

1. **Context-Agnostic Test**: Is there anyone in the world who can identify the data subject from the data? This test assesses whether any individual, regardless of context, could identify the data subject.
2. **Context-Specific Test**: Can a specific holder of the data identify the data subject from the data? This test evaluates whether the specific data recipient, given their context and resources, can identify the data subject.

The choice of approach affects the treatment of pseudonymised data. For example:

1. **Context-Agnostic Test**: If Data Controller A sends pseudonymised data to Data Controller B (with A retaining the means to identify individuals), the dataset is not considered anonymised.

2. **Context-Specific Test**: If Data Controller A sends pseudonymised data to Data Controller B, the dataset *might* be considered anonymised in the hands of Controller B. However, a test is necessary to determine if the dataset is indeed anonymised for Data Controller B.

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would not be anonymous.

The second test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset *may* be anonymous in the hands of Data Controller B. A test would be needed to determine whether the dataset is anonymous in the hands of Data Controller B.

In the absence of direction from the Commissioner on a test, the data controller will have to decide. In making this decision, general points may be worth keeping in mind (many of which come from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and therefore fall under data protection regulations.
- Consider all means of identification that could be used by a person, for example, available datasets.
- Consider objective factors that are *reasonably likely* to be used, such as technology, resources and time, to identify.
- One could follow the GDPR test which states that if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or it is impossible to infer a link between two pieces of information in a dataset, then the data is anonymous.
- Genetic data is considered sensitive personal data. It not only falls under the Data Protection Act but also has a higher level of protection.

- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, in particular as genetic data is an identifier. In considering whether a genomic dataset can be considered anonymised, context matters – the objective factors associated with the data.

Special Note on Genetic and Genomic Data

Genetic data is considered to be sensitive data. It has a higher level of protection under data protection law. There is ongoing debate about whether genomic datasets can ever truly be considered not to be personal data, in particular as genetic data is an identifier. In its definition of genetic and biometric data, the NDPA provides that genetic data is sensitive data where it is "for the purpose of uniquely identifying a natural person" and where it allows or confirms "the unique identification of that individual". Therefore, in deciding whether the genomic dataset that you hold can be considered to fall outside of the definition of personal data, remember that context matters. Therefore, consider whether your data allows for anyone to identify the data subject.

Key Principles That Must be Met in Terms of the Nigeria Data Protection Act

1. *Lawfulness, fairness, and transparency:* A data controller or data processor must ensure that personal data is processed in a fair, lawful and transparent manner. Lawful means that there must be a legal basis for the processing of the personal data as set out in the Act. Genetic (and biometric) data is considered to be *sensitive personal data*. Generally, the processing of sensitive personal data including genetic data is prohibited unless the processing is for certain purposes including medical care or community welfare (to be carried out by a healthcare or similar service provider bound by a duty of confidentiality), public health and scientific research.
2. *Purpose limitation:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Special provisions deal with purpose limitation, for example, "further processing for archiving purposes in the public interest, scientific, historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes".

3. *Adequacy:* Personal data must be adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed.
4. *Storage limitation:* Personal data should be retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed.
5. *Accuracy:* Personal data must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal data collected is accurate.
6. *Security safeguard:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.
7. *Security, integrity and confidentiality:* A data controller and data processor must implement appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.
8. *Accountability and duty of care:* A data controller or data processor owes a duty of care to the data subject in respect of data processing and must demonstrate accountability in respect of the principles contained in the Act.

Data Subject Rights in Terms of the Nigeria Data Protection Act

Data subjects have rights that the data controller must protect. These rights are the:

1. *Right to be informed:* The data subject has the right to confirm whether the data controller or processor is storing or processing his/her personal data. When a data controller is processing personal data, a data subject has the right to be informed of the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients who the personal data has been or will be disclosed to, *in particular* recipients in third countries or international organisations, and for how long the data will be stored. Furthermore, where personal data is not collected directly from the data subject, the data subject has the right to be informed about its source.
2. *Right to rectification and erasure:* A data subject has the right to request from the data controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject or to object to such processing.

3. *Right to lodge a complaint:* A data subject has the right to lodge a complaint with the Commission.
4. *Rights in relation to automated decision-making and profiling:* A data subject has the right to be informed about the existence of automated decision-making, including profiling, and its significance and envisaged consequences. Furthermore, the data subject has the right not to be subject to a decision based solely on automated processing of personal data, including profiling, and which produces legal or similar significant effects concerning the data subject.
5. *Right of access:* The data subject has a right to obtain a copy of his/her personal data that the data controller has in its possession or is processing such data in a commonly used electronic format. An exception is when providing such data would impose unreasonable costs on the data controller. In such a case the data subject may be required by the data controller to bear some or all such costs.
6. *Right of correction and erasure:* The data subject has the right of correction, or if correction is not feasible, deletion of his/her personal data that is inaccurate, out of date, incomplete or misleading. The data subject also has the right to erase personal data concerning him/her and to restrict data processing in certain circumstances.
7. *Right to withdrawal of consent:* A data subject must have the right to withdraw consent to the processing of his/her personal data at any time. This will apply where consent is the lawful basis of processing.
8. *Right to object:* A data subject must have the right to object to the processing of his or her personal data and the data controller must discontinue the processing unless the data controller can demonstrate a public interest (not defined) or other legitimate grounds that override the fundamental rights and freedoms and interests of the data subject. Likewise, a data subject has a right to object to the processing of his or her personal data for direct marketing purposes, including profiling.
9. *Right to data portability:* A data subject has the right to data portability. Therefore, a data subject can receive personal data concerning him/her in a structured, commonly used, and machine readable format from the data controller and the personal data can be transmitted without any hindrance directly from one data controller to another, where technically possible.

Cross-Border Data Sharing

The NDPA also has additional provisions in place that must be met when personal data is to be transferred outside of the country. These additional provisions are in place to ensure that data subjects continue to be protected once the data leaves the country.

Cross-border transfers of personal data is not defined in the Act, but provisions on cross-border data sharing would apply when the data is being sent to a data controller in another country. It could also *arguably* include where a researcher outside of Nigeria is given access to the personal data stored in a database, biobank or cloud hosted in Nigeria.

Requirements for lawful transfer of data outside Nigeria

To transfer personal data outside of Nigeria under the NDPA, there must be a lawful basis for this transfer. This can be one of the following:

1. The recipient of the personal data is subject to a law, binding corporate rules (BCR) or contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection to personal data in accordance with the Act. The data controller or processor must:
    a. establish the basis of the cross-border transfer of personal data in terms of the conditions stipulated; and
    b. determine, through an assessment, whether the level of protection afforded by the recipient country is "adequate" for the purposes of this Act.

Considerations when considering adequacy

In considering adequacy, the data controller or processor can consider:

- the availability of the data subject's enforceable rights and ability to enforce such rights through administrative and judicial redress;
- availability of any appropriate instrument in place between the Commission and a competent authority in the recipient jurisdiction that guarantees 'adequate' data protection;

- access of the public authority to personal data;
- the existence of an effective data protection law;
- the existence of an independent and competent data protection or similar supervisory authority;
- the relevant country being bound by international commitments or conventions and its membership of any multilateral or regional organisations.

Regarding determining adequacy of the law in the recipient country, the list developed by NITDA in the NDPR Implementation Framework is applicable.[1]

Other legal bases that can be relied upon in the absence of adequacy

1. The data subject consents to the transfer of personal data outside Nigeria. The data subject must be informed about the possible risks of such transfer in the absence of adequate protections.
2. The transfer is necessary for the performance of a contract to which the data subject is a party to or it is necessary to take steps at the request of a data subject before entering a contract.
3. The transfer is for the sole benefit of a data subject and it is impractical to get the consent of the data subject. Furthermore, if the data subject were able to give consent, he/she would most likely have provided this consent.
4. The transfer is necessitated by important public interest reasons. The Act does not, however, define public interest.
5. The transfer is necessary for the establishment, exercise, or defense of legal claims.
6. 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.

[1] Annexture C 'Countries deemed as having adequate data protection laws' Nigeria Data Protection Regulation 2019: Implementation Framework https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf