OSUNTUYI & TOKAN-LAWAL LAW

NEXA ADVISORY

OTL LAW & NEXA ADVISORY

DATA PROTECTION AND PRIVACY KNOWLEDGE MANAGEMENT SERIES

Tuesday, 6 January 2026

Articles in the Series

ABOUT THE SERIES

Published between September and November 2025, the Data Protection and Privacy Knowledge Management Series is a 12-part article series designed to educate, elevate, and influence privacy practice in Nigeria's rapidly evolving digital ecosystem. Together, OTL Law & Nexa Advisory created a fresh approach to Data Protection Knowledge Management, blending Nexa's expertise in privacy compliance with OTL Law's strong legal advisory experience.

ARTICLE 1: WHAT IS PERSONAL DATA?

Exploring personal data: its definition, categories, and exclusions.

Hello everyone, and welcome to this short but value-packed crash course on data protection and privacy compliance for players in the Nigerian and African tech ecosystem. This is the first of twelve articles in the Nexa Advisory & OTL Law Data Protection Knowledge Management Series designed for founders, engineers, privacy lawyers, enthusiasts, business owners, business advisers, and anyone with a keen interest in data protection and privacy compliance.

My name is 'Tife Ekundayo, I am a lawyer and privacy consultant with multi-jurisdictional experience across the African, European, and United States markets. I am collaborating with the experts at OTL Law to bring you this series. While I have a background as a Nigerian-trained lawyer, I have, over the past few years, studied and practised technology law (with a focus on privacy and security) in the European Union. During this period, I have noticed a gap between how privacy is applied globally and how it is approached across the African continent. Our goal with this series is, therefore, to simplify privacy knowledge and compliance for individuals and entities in Nigeria and across the African continent.

The series will begin with the basics and gradually explore how to build a privacy compliance programme for any business. This is not meant to be an extensive or technical resource. Rather, it is a practical guide that can support both privacy beginners and professionals. Your comments, questions, and feedback are also appreciated.

With that, we welcome you to this series. Prepare to journey from being a privacy novice to a semi-expert in privacy in the next twelve weeks.

What is Personal Data?

Understanding what qualifies as personal data is the foundation of any data protection journey. Whether you are building a tech product, offering legal advice, or working with user information, you must know what you are protecting and why it matters.

Personal data is now a global priority, and Africa is also paying close attention. There is a growing conversation about personal data, how it is processed, and the risks involved. To begin this series, it is therefore important to explain what personal data is and what it is not.

Personal data refers to the information relating to an identified or identifiable natural person. This identified or identifiable natural person is referred to as the data subject. Personal data always refers to a "natural person", that is, a human being. Information about legal persons, companies, or other legal persons created by the law does not qualify as personal data. Also, personal data always refers to information that relates to an identified or identifiable person. This means that the information must be about a person whose identity is obvious from the data itself (identified) or who can be identified using other additional information (identifiable), taking into account all reasonable means and technological advances that can make it easy to identify such a person.

What are the Common Types of Personal Data?

Information like names, phone numbers, home addresses, email addresses, online addresses (e.g. IP addresses, user IDs), identification numbers (e.g. social security numbers, national identity numbers), financial information (e.g. bank account numbers, card information) are the common types of personal data.

Categories of Personal Data

There are two categories of personal data. We have personal data and "special categories of personal data" or "sensitive personal data". Sensitive personal data is personal data that requires enhanced protection because it inherently poses more risks to the data subject. Under the Nigerian laws, these include information about a person's race or ethnic origin, genetic or biometric data, health status, sex life (or sexual orientation), political beliefs or affiliations, religious or philosophical beliefs, or trade union membership. In some jurisdictions (e.g. California), sensitive personal data may also include financial information like bank account numbers, social security numbers, passport numbers, and precise geolocation. Some data protection frameworks (e.g. Modernised Convention 108, South Africa's Protection of Personal Information Act) include information about offences, criminal proceedings, and convictions, and related security measures in the list of special categories of (or sensitive) personal data.

What is NOT Personal Data?

Based on the definitions above, the following types of information are not personal data:

- Company registration numbers or public business IDs
- Generic company email addresses (when they do not contain personal data)
- Information about public bodies or government agencies
- Technical data such as device type or browser information
- Aggregated data that cannot be linked to a specific individual

Another example is truly anonymised data. This is data that has been stripped of all identifiers and cannot be traced back to any individual.

Pseudonymisation v. Anonymisation

Pseudonymisation refers to the process of keeping "identifiers" or information that will help identify a data subject separate from the personal data itself. Pseudonymised personal data cannot be attributed to the data subject without additional information, which is kept separately (the key). Pseudonymised data remains personal data. A common example of pseudonymisation is encryption. The key that enables the identification of personal data must be kept safe and secure at all times.

Anonymisation, on the other hand, refers to the process of permanently stripping personal data of identifiers (or information that links the data to the data subject). By stripping data of identifiers, they no longer relate to an identified or identifiable person. Anonymised data are therefore no longer personal data.

Short Test

Which of the following contains personal data?

1. Mr. John Doe of 123, Liberty Union Square, with phone number +123456789 is a known patient of ABCD Dialysis Centre and visited in 6 times in May, June and July, 2025.
2. The patient, MJD, (Patient #12345) visited 6 times in the past 3 months.
3. Patient MJD visited 6 times in the past 3 months.
4. a.tokanlawal@otllaw.com
5. info@otllaw.com

ARTICLE 2: USERS OF PERSONAL DATA: DATA CONTROLLERS VS DATA PROCESSORS

Now that we understand the concept of Personal Data, the next step is to examine the players involved in data processing. Key players include the data subject, the data controller, and the data processor. Other players include the recipients and third parties.

Key Players

In our first article titled, "What is Personal Data?" a data subject was defined as the natural person to whom the personal data relates, i.e., the individual who can be identified from a set of personal data.

A data controller is the person or organisation that determines the purposes and means of data processing. For example, a clothing store receives an order for a dress. The buyer's address, for example, is the personal data, and the store is the controller who will determine how the buyer's address will be used solely for delivery and the buyer's email is used solely to confirm their order. If two or more parties make these decisions together, they are known as joint controllers.

A data processor processes personal data on behalf of a data controller. The data processor does not make any decision regarding the purposes and means of personal data. They only act on the instructions of the data controller. Unlike the data subject, the data controller and processor can be a natural (an individual) or legal person.

This distinction is important because it helps determine each party's legal obligations. In practice, a Data Processing Agreement (DPA) outlines these responsibilities between the controller and the processor.

Other Key Players

A third party is a natural or legal person other than the data subject, controller, processor, or someone under the controller's or processor's direct authority who is authorised to process the data.

A recipient is a natural or legal person who receives personal data.

A sub-processor is a third party engaged by a data processor to perform specific data activities on their behalf. Practically speaking, all sub-processors are third parties, but not all third parties are sub-processors.

Data Controllers and Processors of Major Importance

The Nigeria Data Protection Act 2023 ("NDPA") introduced an additional category referred to as Data Controllers and Processors of Major Importance. These are individuals or organisations whose data processing activities are especially significant to the country's economy, public interest, or national security. This designation imposes additional regulatory obligations and an organisation may fall into this category if:

- It processes the personal data of more than 200 individuals within 6 months;
- It offers commercial ICT services on a digital device that stores personal data and belongs to someone else; or
- It operates in key sectors such as aviation, healthcare, finance, education, communications, hospitality, tourism, or e-commerce.

These controllers and processors are further classified as follows:

- Ultra-High Level (UHL)
- Extra-High Level (EHL)
- Ordinary-High Level (OHL)

The Nigeria Data Protection Act-General Application and Implementation Directive ("NDPA-GAID") provides additional details on these classifications.

Responsibilities of Data Controllers and Processors

Traditionally, data controllers were expected to meet most compliance obligations. However, in recent years, the responsibilities of data processors have increased significantly. Under the NDPA and the NDPA-GAID, both controllers and processors have nearly identical duties.

As outlined in Article 7 of the NDPA-GAID, these obligations include:

- Registering with the Nigerian Data Protection Commission (NDPC);
- Conducting a data protection compliance audit within 15 months of starting business, and thereafter annually;
- Filing Compliance Audit Returns (CAR) by 31 March each year;

- Maintaining proper documentation of all data processing activities
- Preparing a data protection report within six months of commencing business;
- Organising privacy training and awareness programmes for staff;
- Appointing a Data Protection Officer (DPO) where applicable; and
- Publishing clear and accessible privacy policies and notices on websites, apps, and other platforms.

Now that you have learnt the difference between a data controller and a processor, you are one step closer to full compliance. Remember, the role you play defines your legal responsibilities, and getting it right from the start helps avoid confusion and regulatory breaches.

If you are still unsure about your role in your organisation's data ecosystem, let us know by responding to this email. We are happy to help clarify. Stay tuned for Article 3 and feel free to share this article with colleagues who work with data.

Short Test

Identify the correct role (Data Controller, Data Processor, or Neither) in the following examples:

1. FinTechCo decides to collect and analyse customer spending habits to offer personalised savings advice.
2. SecureCloud Ltd hosts customer data and processes it according to FinTechCo's instructions.
3. Nedu, a freelance developer, creates a website but does not handle or access user data.

Bonus Question:

Which Nigerian legal document defines the categories of Data Controllers and Processors of Major Importance?

ARTICLE 3: UNDERSTANDING THE CORE PRINCIPLES OF DATA PROCESSING

This series is progressing quickly and we are moving to the technical parts, or the meat of the matter, as I like to call it. In this article, we will discuss the key principles of data protection and their compliance objectives.

Data protection principles are the best place to begin for anyone who wants to understand data protection as both a right and a business practice. Many compliance obligations flow directly from these principles, and it is difficult to meet global standards without being familiar with them.

Although the wording may differ slightly across jurisdictions, the core principles remain consistent worldwide. For this article, we will begin with Article 6 of the European Union General Data Protection Regulation ("EU-GDPR" or "GDPR"), which provides a clear and instructive framework. To make it more relevant to our African tech ecosystem, we will also reference the Nigerian law equivalent found in Section 24 of the Nigeria Data Protection Act 2023 ("NDPA") and Article 15 of the NDPA-General Application and Implementation Directive 2025 ("NDPA-GAID").

The principles of data processing are:

- Lawfulness, transparency, and fairness of processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Security
- Accountability

Lawfulness, Transparency & Fairness of Processing:
The lawfulness principle states that all personal data must be processed lawfully. To be processed lawfully, the data controller must have a legal basis for processing the data. These legal bases include consent, contract, vital interest of the data subject or a third party, public interest, or the legitimate interest of the data controller (we will discuss these legal bases in detail in the article 4).

Fairness implies that data processing must be fair. The NDPA-GAID describes fairness as freedom from prejudice and exploitation, and consistency with civil liberties in a democratic society. Fairness implies that data subjects must be able to understand what is happening with their personal data. It can also mean that data controllers should act ethically when processing personal data.

The last pillar of this principle dictates that personal data must be processed in a transparent manner in relation to the data subject. Transparency means that data controllers must notify data subjects about how their data is going to be used. It means that data controllers should provide information to data subjects before processing starts, keep information readily accessible to data subjects during processing, and make data available to their data subjects upon their request.

While lawfulness, fairness, and transparency might feel like three different principles, practically, they go hand in hand. You cannot fulfill the principle of fairness, for example, without honouring the principle of transparency. You cannot be fair in processing without finding a legal basis for processing. This is why they are often described as one.

Purpose Limitation

The principle of purpose limitation dictates that every purpose of processing must be defined before processing commences. The NDPA and the NDPA-GAID state that personal data should be collected for "specified, explicit, and legitimate purposes", and data should not be "further processed in a way incompatible with the original purpose(s)". Data processing for undefined and/or unlimited purposes is therefore unlawful.

While describing what this means, the NDPA-GAID mentions that the purpose must describe the declared and exact intention of the data controller (specified), the words used to describe the purpose of processing must be free from ambiguity (explicit), and the purpose must describe a bona fide intention of data processing (legitimate). Purposes which override the rights and interests of data subjects, incompatible with public policy, or outrightly illegal are illegitimate.

Example: A fintech company collects customers' biometric data for the purpose of identity verification when opening a digital wallet. Under the purpose limitation principle, this biometric data cannot later be repurposed for unrelated activities — for example, the company cannot use the same fingerprints or facial scans for targeted advertising, credit scoring, or selling insights to third parties.

These new processing purposes (advertising or credit scoring) will require a new and separate legal basis for processing. Permitted related uses of the biometric data may include fraud prevention, account recovery, or regulatory compliance (e.g., CBN KYC/AML requirements) since these are directly connected to the original purpose.

Please note that the key term here is compatibility. Further processing must be compatible with initial processing. A compatible further processing is one that makes it possible to achieve the original purpose or is an innovative progression of the original purpose. To determine compatibility, the data controller should take into account:

- any link between the original purpose and intended further purposes,
- the context in which personal data has been collected. Particularly, the reasonable expectations of the data subjects based on their relationship with the controller,
- the nature of the personal data,
- the consequences of the intended further processing for data subjects, and
- the existence of appropriate safeguards in both the original and intended further processing operations.

Important note: Both the GDPR & the NDPA permit further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. These further processing still require appropriate safeguards like anonymisation or pseudonymisation.

Data Minimisation

This principle states that data processing must be limited to what is necessary to fulfil a legitimate purpose. Only such data that are adequate, relevant, and not excessive to the purpose of processing should be processed. The NDPA-GAID describes it this way: personal data should be "adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed."

This principle aims to reduce the risk of excessive data collection for a particular processing purpose. For example, in hiring environments, only personal data necessary to move candidates further in the hiring process should be collected. Personal data, like annotated and certified copies of birth certificates, would be considered excessive for such a process.

Example: An e-commerce platform in Abuja requires customers to create an account to order household goods. To process the order, it legitimately needs the customer's name, delivery address, phone number, and payment details. Collecting personal data like Bank Verification Number (BVN), National Identification Number (NIN), marital status, or religion would breach the principle of data minimisation.

Under data minimisation, organisations must ensure that only the data strictly necessary for the stated purpose is collected and processed, nothing more.

Data Accuracy

Accuracy implies that data controllers must ensure that all personal data is correct at all times. Controllers should not use information without taking steps to ensure, with reasonable certainty, that such data are up to date. Inaccurate data must therefore be erased or rectified without delay.

The NDPA-GAID says that data controllers should ensure that personal data is "accurate, complete, not misleading, and where necessary, kept up to date, having regard to the purposes" of processing.

This obligation to keep personal data accurate is contextual, that is, it is relative to the context of data processing. There are instances where updating stored personal data is legally prohibited (for example, medical records). This is because the purpose of storing data is to document events as a historical snapshot. It would therefore be inappropriate (and even illegal) to update medical records even if findings mentioned in the record later turn out to have been wrong.

Conversely, there are situations where it becomes absolutely necessary to regularly update and confirm the accuracy of personal data, due to the nature of the processing and having regard to the risks inherent in such processing operation. A good example of this is credit arrangements. Financial institutions ought to occasionally confirm that the creditworthiness of the customer is correct at every given time. This can be done by updating dedicated databases on the customer's credit history.

Storage Limitation

Storage Limitation relates to the duration of processing. That is, personal data should not be stored (or retained) for longer than is necessary to achieve the lawful bases for which the data was collected. This means that personal data must be discarded as soon as the purpose of processing has been exhausted.

Data controllers must use reasonable efforts to ensure that personal data is stripped of all identifiers after the purpose of processing has been achieved. This can be done by outright deletion or anonymisation. Data controllers must also specify a time limit for retention of personal data. These time limits should be subject to periodic review. This can be achieved by creating and monitoring data retention policies.

Using the example of the Abuja-based e-commerce platform referenced above, if the e-commerce company keeps customers' personal data (name, delivery address, phone number, payment details) only for as long as it is needed to deliver the order, handle returns, and meet tax or regulatory obligations, and deletes or anonymises the personal data after order fulfilment, then the company has complied with the storage limitation principle. Conversely, if the platform were to keep delivery addresses and payment details indefinitely, even after the customer has closed their account and no legal requirement exists, it would be in breach of the storage limitation principle.

Important note: There are instances where the law requires longer storage of personal data (for example, in some jurisdictions, companies are obliged to store financial data and other tax information for seven years). The GDPR permits these exceptions if they are provided by law, respect the essence of fundamental rights and freedoms, and are necessary and proportionate for pursuing a limited number of legitimate aims. These aims would usually include protection of national security, protecting the rights and fundamental freedoms of others, investigating and prosecuting criminal offences, and so forth. In all of these cases, data controllers should always implement appropriate safeguards for the personal data.

Security

This principle requires controllers to implement appropriate technical or organisational measures during processing to ensure the integrity, availability, and confidentiality of personal data. This means that personal data must be protected against accidental, unauthorised or unlawful access, use, modification, disclosure, destruction or damage (this is known as a data breach). To determine a commensurate security measure, controllers should take into account the state of the art, the costs of implementation, the nature and scope of processing, and the risk inherent in the processing activity. It logically follows that sensitive personal data will require more stringent security measures than other categories of personal data.

These appropriate organisational or technical measures could include anonymisation, pseudonymisation, encryption of data at rest and in transit, access controls, secure authentication, and so forth.

Accountability

Accountability dictates that data controllers and processors should actively and continuously comply with data protection obligations and principles. They should also be able to demonstrate accountability by keeping necessary records and documentation. Data protection is a self-assessment procedure. Controllers and processors must implement appropriate technical and organisational measures to show that they are compliant in all phases of data processing. This can be done by keeping records of processing activities, designating an independent data protection officer, undertaking necessary assessments for specific processing operations, ensuring data protection by design and default, and so forth.

This brings us to the end of our discussion on principles of data protection. In practice, these principles work together to set the foundation for lawful processing. Data controllers and processors must apply all of them consistently to demonstrate compliance. These principles also create concrete obligations, which we will discuss in detail in the next article.

Short Test

1. Which principle requires that data must only be collected for specific, clear, and lawful reasons?
    a. Data Minimisation
    b. Accuracy
    c. Purpose Limitation
    d. Security
2. Which of the following is a way to meet the security principle?
    a. Keeping data forever in case it is useful later
    b. Encrypting personal data both in storage and in transit
    c. Collecting more data than necessary to be thorough
    d. Ignoring risks if the data looks harmless
3. If data is kept longer than necessary for its original purpose, this may breach the storage limitation principle. (True or False)
4. Fairness in data processing means that data subjects must be able to understand how their personal data is being used. (True or False)

Bonus Question

Which principle makes organisations responsible for proving that they follow data protection obligations?

ARTICLE 4: LAWFUL DATA PROCESSING: LEGAL BASES FOR PROCESSING DATA

Welcome again to another article in the Nexa Advisory & OTL Law Data Protection Knowledge Management Series. We are moving quickly from the introductory concepts into the technical aspects of data protection. This week, we'll be discussing the legal bases for processing personal data, building on the principles of data processing we discussed last week. This discussion moves us into the rules of lawful processing and compulsory data protection obligations.

If you recall from our last article, one of the principles of data processing is lawfulness. This means that data controllers must have a legal basis for processing personal data. In this article, we will discuss these legal bases in detail and explain how data controllers can incorporate these into their processing operations for compliant processing.

This is also one of my favourite data protection topics to discuss with Nigerian privacy enthusiasts because it helps debunk the myth that consent is the strongest pillar of data processing or that every processing operation requires consent. At the end of this article, you will see why consent is actually the least desirable legal basis for processing.

For personal data to be processed lawfully, it must be based on any of the following legal bases (or grounds) of processing:

- consent of the data subject,
- a contractual relationship between the data subject and the controller or processor,
- compliance with a legal obligation of the controller,
- protection of the vital interests of the data subject or a third party,
- performance of a task in the public interest,
- legitimate interest of the controller.

Consent

Consent means that a data subject has given clear permission for their data to be processed for a specific purpose. Both the GDPR and the NDPA require that consent must be freely given, specific, informed, and unambiguous. Where processing is based on consent, the controller must be able to demonstrate that consent was obtained. However, consent is often seen as the most volatile and weakest ground for processing because it can be withdrawn at any time, and withdrawal must be as easy as giving consent. For this reason, regulators frequently advise controllers to avoid over-reliance on consent unless it is absolutely necessary.

Another important point is that consent may be interpreted as not freely given if there is a clear imbalance of power between the parties. For example, in an employment relationship, an employee may feel pressured to give consent to their employer even if they do not really want to. In such situations, consent may not be considered valid.

The NDPA-GAID provides more clarity on situations where consent must be used as a legal basis. These include direct marketing, processing of sensitive personal data, and the processing of children's data. For these activities, no other ground of processing will suffice.

Controllers should also remember that consent must always be documented. If challenged, it is the responsibility of the controller to prove that valid consent was obtained.

Contract

Personal data may be processed where it is necessary to enter into or perform a contract with the data subject. This does not mean that any data processing linked to a contract is automatically lawful. Rather, the processing must be strictly necessary for the performance of the contract or for pre-contractual steps taken at the request of the data subject. For example, if a customer orders goods from an online store, the store needs the customer's name, address, and payment details to deliver the product. These are necessary for fulfilling the contract. However, using the same data for unrelated profiling or targeted advertising would not fall under this ground, as it is not necessary for the contract itself.

The NDPA and NDPA-GAID adopt the same approach: processing must be necessary and proportionate to the performance of a contract. Where the purpose can be achieved without processing personal data, this ground should not be used.

Legal Obligation

Controllers may process personal data where it is necessary to comply with a legal obligation. For example, financial institutions are often required by law to retain transaction records for a fixed number of years for tax or anti-money laundering compliance.

This ground is particularly strict: the legal obligation must be laid down in law. It cannot be based on company policy or internal practices. The governing legislation must also respect the fundamental rights and freedoms of the data subject.

Vital Interests

Processing may also be justified where it is necessary to protect the vital interests of the data subject or another person. This is usually limited to matters of life and death or situations of grave danger. For example, if a hospital shares a patient's medical records with another hospital in an emergency where the patient is unconscious and unable to consent, this would be justified on the basis of vital interests.

The NDPA-GAID also frames vital interests narrowly. It should only be used where processing is essential to protect someone's life, health, or safety, and where no other legal basis is available.

Public Interest

Both the GDPR and the NDPA recognise that personal data may be processed for the performance of a task carried out in the public interest or in the exercise of official authority. This ground often applies to public authorities or private entities carrying out delegated public functions. Examples include processing for public health surveillance, census exercises, or voter registration.

Legitimate Interest

Legitimate interest allows controllers to process data where it is necessary for their legitimate interests or those of a third party, except where such interests are overridden by the rights and freedoms of the data subject.

This ground gives organisations flexibility, but it must be balanced carefully. The controller must carry out a legitimate interest assessment (LIA), weighing their interest against the privacy rights of the data subject. For example, using CCTV cameras in a store to prevent theft may be justified under legitimate interest. However, excessive surveillance of employees without a clear purpose may fail this test.

Importantly, under both the GDPR and the NDPA, legitimate interest is never a lawful basis for processing sensitive personal data.

Special Note on Sensitive Data

Sensitive personal data (called "special categories of data" under GDPR) includes information on health, race, ethnic origin, religion or belief, political opinions, union membership, genetics, biometrics, and sexual orientation. Because of its sensitive nature, this category of data attracts stricter rules. Both the GDPR and the NDPA recognise that sensitive data requires higher protection, but their approaches differ.

Under the GDPR (Article 9): processing of special categories of data is prohibited unless one of several exceptions applies. These include:

- Explicit consent of the data subject.
- Processing necessary for carrying out obligations in the field of employment, social security, and social protection law.
- Processing necessary to protect the vital interests of the data subject or another person where the data subject is unable to consent.
- Processing by a not-for-profit body in the course of its legitimate activities.
- Processing of data manifestly made public by the data subject.
- Processing necessary for legal claims or courts acting in a judicial capacity.
- Processing necessary for reasons of substantial public interest, based on law.
- Processing for health or social care purposes.
- Processing for public health purposes.
- Processing for archiving, research, or statistical purposes in the public interest.

Under the NDPA and the NDPA-GAID, the position is narrower. Sensitive data may only be processed on the basis of explicit consent of the data subject, unless otherwise provided by law. The NDPA-GAID also highlights that direct marketing and children's data fall within categories where consent is the only valid basis.

Please note that explicit consent differs a little from the consent required to process other types of personal data. Explicit consent requires more information, more legal safeguards, and an even bigger opportunity to object to the processing at any point in time.

Controllers must always remember that legitimate interest can never be used for processing sensitive personal data. Where consent is relied upon, it must be explicit, unambiguous, and properly documented.

Conclusion

Lawful processing requires careful consideration of the appropriate legal basis. While the GDPR provides a range of options, Nigerian law under the NDPA and NDPA-GAID often require stricter reliance on consent, especially for sensitive data. Controllers should therefore avoid using consent where another, stronger legal basis is available and should document their decision-making process for accountability.

Short Test

1. Which of the following is not a valid legal basis for processing personal data?
    a. Consent
    b. Contract
    c. Convenience
    d. Legal obligation
2. True or False: Consent is always the strongest and most reliable basis for data processing.
3. Which legal basis applies when a hospital shares a patient's medical data in a life-or-death emergency?
    a. Consent
    b. Vital interests
    c. Public interest
    d. Contract
4. Under the NDPA, which of the following activities requires consent as the legal basis?
    a. Processing of children's data
    b. Direct marketing
    c. Processing of sensitive personal data
    d. All of the above

Bonus Question: Which principle requires controllers to document their reasoning when choosing a legal basis for processing?

ARTICLE 5: DATA PROTECTION IMPACT ASSESSMENTS

Exploring DPIAs: what they are, their importance, and how to conduct them

Welcome to Article 5 of our Data Protection and Privacy Knowledge Management Series. We are now a quarter of the way into the series and the discussion is getting more technical. In Articles 1 to 4, we explored the fundamentals of data protection. Now, we will discuss the concept of Data Protection Impact Assessments (DPIAs): what they are, their importance, and how to conduct them.

What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a process designed to help organisations identify, evaluate, and mitigate the risks that their data processing activities pose to individuals' rights and freedoms.

Under Article 35 of the GDPR, controllers are required to carry out a DPIA when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons." The Nigeria Data Protection Act 2023 (NDPA) adopts the same approach, requiring DPIAs for high-risk processing activities (see Section 29). The NDPA-GAID 2025 provides even more detail by specifying risk indicators and the situations in which a DPIA must be conducted.

Put simply, a DPIA is both a risk management tool and a compliance mechanism. It ensures that privacy risks are identified early and that safeguards are integrated into processing "by design and by default."

When Must a DPIA Be Carried Out?

Both the GDPR and NDPA require DPIAs where processing is likely to result in high risks to data subjects. Examples of high-risk processing include:

- Large-scale processing of sensitive personal data (such as health, biometric, or genetic data).
- Systematic and extensive profiling of individuals, especially where decisions have legal or significant effects (e.g. credit scoring).
- Monitoring publicly accessible areas on a large scale (e.g. use of CCTV in smart cities).
- Use of emerging technologies like AI, facial recognition, or big data analytics.

The NDPA-GAID specifically highlights:

- Processing children's personal data.
- Processing that involves cross-border transfers.
- Processing that could significantly affect data subjects' rights and freedoms in Nigeria.

In practice, it is not always clear which processing activity amounts to a high-risk processing. However, if you are unsure whether your processing requires a DPIA, then you should perform a DPIA and err on the side of caution.

Other African frameworks echo similar requirements. For example, Kenya's Data Protection Act 2019 (Section 31) also mandates DPIAs for high-risk processing, aligning with both the EU and Nigerian models.

Why are DPIAs Important?

Legal compliance – They are mandatory under both the GDPR and the NDPA when processing is likely to pose high risks.
Accountability – A DPIA demonstrates that an organisation has taken steps to comply with the principles of fairness, transparency, and accountability.
Risk reduction – By identifying and addressing risks at the planning stage, organisations can prevent costly data breaches and reputational damage.
Building trust – DPIAs show customers, regulators, and partners that privacy and data protection are taken seriously.

How to Conduct a DPIA

A DPIA is not a box-ticking exercise. It is a structured, iterative process. According to the GDPR, NDPA, and NDPA-GAID, a DPIA should do the following:

1. Describe the Processing Activity
    - Nature, scope, context, and purpose of processing.
    - Categories of data subjects and personal data involved.
2. Assess Necessity and Proportionality
    - Confirm whether the processing is necessary for the purpose.
    - Consider if less intrusive means could achieve the same objective.
3. Identify Risks
    - What risks could arise for data subjects? Examples: unauthorised access, discrimination, identity theft, reputational harm.
4. Evaluate Likelihood and Severity
    - Use risk matrices to assess both the probability of the risk occurring and its potential impact.

5. Identify Safeguards and Mitigation measures
    - Technical: encryption, pseudonymisation, access control.
    - Organisational: staff training, policies, limited retention.
    - Legal: contracts, data processing agreements, cross-border transfer safeguards.
6. Document and Review
    - Keep a written record of the DPIA and the steps taken.
    - Submit to the regulator when required (e.g. NDPA requires submission in some high-risk cases).
    - Review regularly as technology or processing changes.

Role of the Data Protection Officer (DPO) in DPIAs

Both GDPR and NDPA require that, where a DPO is appointed, the DPO should be closely involved in the DPIA process. They provide expert advice, ensure objectivity, and act as a bridge with the supervisory authority.

The Bottom Line

A DPIA is not just a regulatory burden. It is an opportunity for organisations to embed privacy by design, anticipate compliance challenges, and earn trust in the digital economy. In the African tech ecosystem, where trust deficits are high, conducting DPIAs proactively can distinguish responsible businesses from the rest.

Short Test

1. Which of the following is NOT a scenario that typically requires a DPIA?
    a. Large-scale processing of health data
    b. Profiling for automated credit decisions
    c. Sending newsletters to customers who opted in
    d. Deploying facial recognition in airports
2. True or False: A DPIA is optional under the NDPA and is only recommended, not required.
3. What is the role of the Data Protection Officer in the DPIA process? Select all that apply
    a. To approve all processing contracts
    b. To provide advice and ensure compliance during the DPIA
    c. To act as the organisation's IT manager
    d. To eliminate the need for a DPIA altogether

ARTICLE 6: A DEEP DIVE INTO THE NDPA-GAID 2025

Exploring the General Application and Implementation Directive 2025

Welcome again to another week in our Data Protection and Privacy Knowledge Management Series. We are steadily building our understanding of data protection and privacy, and in this article, we will take a closer look at the General Application and Implementation Directive 2025 (GAID 2025/the Directive). The Directive is a critical instrument issued by the Nigeria Data Protection Commission (NDPC/the Commission), formerly the Nigeria Data Protection Bureau (NDPB), to guide the implementation of the Nigeria Data Protection Act 2023 (NDPA).

While the NDPA establishes the substantive rights and obligations of data subjects, controllers, and processors, the GAID 2025 provides clarity on how these obligations should be interpreted and operationalised. If you think of the NDPA as the law itself, the GAID 2025 is the manual that shows you how to comply in practice.

What is the GAID 2025?

The GAID 2025 provides guidelines, clarifications, and practical steps to help organisations comply with the NDPA. It is binding in nature, which means that organisations cannot treat it as optional. It is not unusual for data protection authorities to issue such guidance. For example, the European Data Protection Board (EDPB) issues guidelines and recommendations to interpret the EU GDPR. In South Africa, the Information Regulator issues practice notes under the Protection of Personal Information Act (POPIA). In the United Kingdom, the Information Commissioner's Office publishes guidelines and directives to guide compliance with the UK GDPR. The GAID 2025 performs a similar function in Nigeria by addressing grey areas and aligning local practice with international standards.

Key Areas Covered by the GAID

1. Clarification of Key Terms

The GAID 2025 defines and clarifies concepts introduced in the NDPA. For example, it provides a detailed clarification of data protection concepts such as:

Consent: the GAID 2025 specifies circumstances where consent is valid, including for direct marketing, processing of sensitive data, and processing children's data.

Classification of Data Controllers and Processors of Major Importance (DCPMIs): the GAID 2025 specified the criteria for classifying DCPMIs and their compliance obligations.

2. Lawful Basis of Personal Data Processing

The GAID 2025 builds on section 25 of the NDPA by giving examples of when each legal basis can be relied upon. For instance, it states that:

- Consent is required for direct marketing or when processing sensitive data.
- Contractual necessity should not be used unless the processing is objectively required to perform the contract.
- Vital interest should be interpreted narrowly, limited to life and death or urgent health emergencies.

This guidance is crucial for avoiding misuse of any stated legal basis and ensuring that controllers choose the most appropriate ground.

3. Special Categories of Personal Data

The GAID 2025 confirms that sensitive personal data in Nigeria can only be processed based on the consent of the data subject. This differs from the EU GDPR, which provides multiple grounds for processing sensitive data under Article 9.

4. Data Protection Impact Assessments (DPIAs)

The GAID 2025 outlines when DPIAs are mandatory, such as:

- introduction of new technologies,
- large-scale processing of sensitive personal data,
- processing that involves profiling or automated decision-making with legal or significant effects,
- systematic monitoring of publicly accessible areas.

This aligns closely with EU GDPR Article 35 but adds Nigeria-specific thresholds. The GAID 2025 also prescribes that DPIAs must be filed with the NDPC in certain high-risk cases, which is not a requirement under the GDPR.

5. Cross-Border Data Transfers

The GAID 2025 introduces a more detailed framework for cross-border transfers, building on section 41 of the NDPA. It specifies:

- conditions for adequacy decisions by the NDPC,
- appropriate safeguards where adequacy does not exist (such as standard contractual clauses), and
- limited derogations for exceptional circumstances.

This provision ensures Nigeria aligns with global expectations while protecting data subjects against unlawful transfer of data outside the country.

6. Accountability and Governance Measures

The GAID 2025 requires data controllers and processors to implement governance structures to demonstrate compliance. These include:

- appointing Data Protection Officers (DPOs) in certain circumstances,
- maintaining records of processing activities,
- conducting regular audits and training, and
- adopting privacy by design and default in system development.

This moves Nigerian organisations towards international best practice and ensures they are proactive rather than reactive in managing compliance.

Key New and Codified Obligations Under GAID 2025

Below is a summary of the new or clarified obligations introduced by GAID 2025, with references to the directive and commentary sources.

Obligation	What GAID Requires	GAID / NDPA Reference	Why This Matters
Territorial Reach / Operating in Nigeria	Expands "operating in Nigeria" to include organisations not domiciled in Nigeria but targeting Nigerian data subjects.	GAID Art. 1(2), Art. 8(1)-(2)	Foreign organisations must assess whether their Nigerian-targeted processing triggers GAID obligations.
Status of the NDPA/Repeal of NDPR	GAID supersedes NDPR as a regulating instrument, but NDPR-era actions remain valid. Where NDPA and GAID overlap, NDPA supersedes	GAID Art. 3(3)	Confirms compliance must align with only NDPA and GAID.
Classification & Registration (DCPMI)	Entities must register if classified as Data Controllers/Processors of Major Importance. Ultra-High Level (UHL) & Extra-High Level (EHL) must register once and file Compliance Audit Returns (CAR); Ordinary High Level (OHL) must renew registration annually.	GAID Art. 7–9, Schedule 7	Classification affects compliance burden, reporting, fees, and oversight.
Data Protection Officers (DPOs)	DPOs must be designated by UHL and EHL DCPMIs.	GAID Art. 7(1)(i), Art. 11 - 14, Schedule 3	DPOs are independent compliance officers within the company. They oversee compliance, training, and serve as liaison with NDPC.
Compliance Audit Return (CAR) & Filing Fees	UHL and EHL must file CAR through a Data Protection Compliance Organisation (DPCO). OHL may have lighter obligations. New fees apply.	GAID Art. 7(1)(b - c) & Schedules 2 & 10	Enables NDPC oversight but introduces cost and reporting demands.
Obligation to Prevent Misuse	Controllers must take steps to restrict access or suspend processing if the NDPC notifies them of platform misuse or breach. Failure to act constitutes a compliance violation.	GAID Art. 32	Controllers and processors must act swiftly on NDPC directives.
Standard Notice to Address Grievance (SNAG)	Introduces SNAG, enabling data subjects to lodge complaints and seek remediation directly.	GAID Art. 40 & Schedule 9	DPOs must create systems to handle and respond to SNAGs.
Data Processing Agreements (DPAs)	GAID sets mandatory clauses in DPAs: parties, obligations of the parties, purpose of processing, location of processing, evidence of NDPA compliance, amongst others.	GAID Art. 34	Existing contracts must be updated to align with GAID standards.
Monitoring of Security Systems	Controllers/processors must regularly monitor, evaluate, and maintain their data security systems.	GAID Art. 29	Security obligations are ongoing, not one-off.
Data Subjects' Vulnerability Index (DSVI)	Controllers should benchmark security measures by the level of vulnerability of data subjects. DPOs must develop and maintain a DSVI to justify security measures. Example, personal data of vulnerable classes like children, elderly and persons with (physical and cognitive) disabilities will require stronger security measures.	GAID Schedule 6	Measurement of the efficiency of appropriate organisational and technical measures must take into account the status of data subjects.

Practical Steps for Data Protection Officers

Below is a non-exhaustive list of practical steps for Data Protection Officers (DPOs) to take note of based on the GAID 2025:

- Review your classification (Ultra-High, Extra-High, or Ordinary High Level). Your classification determines how much oversight and reporting you must do.
- Audit your DPAs. Make sure your data processing contracts contain the GAID-mandated clauses. If not, update them quickly.
- Update your privacy assessments, especially Data Protection Impact Assessments (DPIAs), to conform with the standard of the NDPA-GAID. Consider adopting the NDPA-GAID template in Schedule 4.
- Adapt your privacy notices. Ensure they are clear, accessible, and if necessary, available in alternative formats for vulnerable users.
- Prepare for SNAGs. Build internal processes to log, respond to, and resolve complaints under the new SNAG procedure.
- Stay responsive to NDPC notifications. If the Commission reports misuse of your platform, act quickly to restrict access and avoid liability.
- Schedule regular security reviews. GAID requires ongoing monitoring and evaluation of your data security measures.
- Budget for fees and CAR filing. Especially if you fall into UHL or EHL categories, compliance comes with both procedural and financial implications.

Conclusion

The GAID 2025 represents a maturing of Nigeria's data protection landscape. It brings clarity, harmonisation, and new burdens. For DPOs and compliance teams, the Directive is not optional guidance but a playbook for lawful operations in Nigeria.

Short Test

1. True or False: The NDPR remains valid alongside the GAID and NDPA.
2. Which GAID mechanism allows data subjects to lodge complaints directly with controllers?
   a. CAR
   b. SNAG
   c. DPIA
3. What classification system does GAID introduce for data controllers and processors, and why does it matter?
4. Why must organisations schedule regular security reviews under GAID?

ARTICLE 7: CROSS-BORDER DATA TRANSFERS

Understanding the Rules for International Movement of Personal Data under the Nigeria Data Protection Act - General Application and Implementation Directive 2025 (NDPA-GAID 2025)

Welcome to Article 7 of our Data Protection and Privacy Knowledge Management Series. We are now halfway through our journey, and the discussion has taken a global turn. In articles 1 - 6, we explored the fundamental concepts of data protection, from lawful processing and Data Protection Impact Assessments (DPIAs) to accountability and data protection principles. In this article, we turn our attention to an important topic in today's digital ecosystem: cross-border transfers of personal data.

In a world where cloud hosting, remote work, and global collaboration are standard practice, personal data often moves beyond national borders. Yet, every transfer must preserve the rights of Nigerian data subjects.

The Nigeria Data Protection Act (NDPA) and the General Application and Implementation Directive 2025 (GAID 2025) provide the rules that govern these international data movements, with detailed provisions in Schedule 5 (Guidance on Cross-Border Data Transfer). Now, let us examine what these provisions mean for organisations operating within and outside Nigeria.

1. The Legal Basis for Transfers

Section 41 of the NDPA provides the general rule that personal data may be transferred outside Nigeria only if the recipient country, territory, or organisation provides an adequate level of protection, or if one of the conditions specified in Section 43 applies.

The GAID 2025, in Schedule 5, builds on this rule and identifies two primary legal bases for lawful cross-border transfers, as well as a set of derogations for exceptional cases.

2. Basis One: Adequacy Decisions

An adequacy decision means that the Nigeria Data Protection Commission (NDPC) has determined that a particular country, territory, or international organisation provides protection for personal data that is substantially equivalent to Nigeria's standards. Transfers to such jurisdictions are treated as if the data were processed within Nigeria, meaning no further authorisation is required.

Under Schedule 5 of the GAID 2025, adequacy is determined by evaluating several factors, including:

- Whether the recipient country has a data protection law that is effectively enforced;
- Whether there is an independent supervisory authority;
- Whether data subjects have effective legal remedies in the recipient country; and
- International commitments of the recipient country, including membership of global organisations.

Section 42(4) of the NDPA confirms that the NDPC will publish and update a list of adequate countries or territories. This list may draw inspiration from the EU's adequacy list under Article 45 of the GDPR, but the NDPC retains discretion to make its own determinations.

The NDPR Whitelist (Historical Context)

Before the NDPA and GAID 2025, the Nigeria Data Protection Regulation 2019 (NDPR) created a whitelist of countries considered to offer adequate protection. That list included: Member states of the European Economic Area (EEA), the United Kingdom, Canada, Israel, New Zealand, Switzerland, and Argentina.

Although this list is not automatically carried over to the NDPA–GAID 2025 regime, it remains a useful benchmark. Until the NDPC issues a new adequacy list under Schedule 5, these countries may be considered "likely" to qualify for adequacy recognition, given their comparable data protection regimes. Below is a comparative overview of recognised adequate jurisdictions:

Category	Countries / Jurisdictions	Basis
Adequate under the GDPR (as of October 2025)	Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea (South Korea), Switzerland, the United Kingdom, and Uruguay.	European Commission Adequacy Decisions under GDPR Article 45
Adequate under the former NDPR	Member states of the European Economic Area (EEA), all African member-countries of the Malabo Convention 2014, the United Kingdom, Brazil, Canada, China, Japan, New Zealand, Switzerland, Togo, and other EU-recognised adequate countries.	NDPR Implementation Framework 2020 (Annex A)
Likely to be recognised under the NDPA/GAID	The same jurisdictions as above, pending NDPC confirmation. African jurisdictions with established frameworks such as Kenya, Ghana, Mauritius, and South Africa may also be recognised.	GAID Schedule 5(5)

3. Basis Two: Cross-Border Data Transfer Instruments (CBDTIs)

When adequacy has not been determined, controllers and processors can still lawfully transfer personal data outside Nigeria using Cross-Border Data Transfer Instruments (CBDTIs).

According to Paragraph 3 of Schedule 5, CBDTIs are legally binding instruments that ensure the protection of personal data after it leaves Nigeria. They impose enforceable rights and obligations, ensuring that the data continues to be handled in a way consistent with Nigerian law. The GAID 2025 recognises several forms of CBDTIs, including:

- Contractual Clauses Approved by the NDPC – These may be standard clauses developed by the NDPC or custom agreements submitted for prior approval. They function much like the Standard Contractual Clauses (SCCs) under the GDPR.
- Binding Corporate Rules – Multinational groups or affiliates can adopt internal rules binding all entities involved in cross-border processing.
- Codes of Conduct or Certification Mechanisms – Where approved by the NDPC, an organisation may rely on adherence to a certified data protection code or framework that includes enforceable commitments by the foreign recipient.

Every CBDTI must contain:

- Enforceable data subject rights;
- Effective remedies for breaches;
- Assurance of oversight by a competent authority; and
- Mechanisms to monitor compliance and report to the NDPC.

This approach reflects the NDPA's principle of accountability and ensures that protection travels with the data.

4. Derogations for Exceptional Circumstances

When neither an adequacy decision nor a CBDTI exists, Paragraph 6 of Schedule 5 introduces derogations — limited exceptions that permit transfers in specific, exceptional situations.

Derogations are intended only for occasional or one-off transfers, not for regular or large-scale data exports. Continuous reliance on derogations would breach the accountability principle.

Transfers may proceed under the following circumstances:

- Explicit Consent – Where the data subject has explicitly consented to the transfer after being informed of the risks involved.
- Contractual Necessity – Where the transfer is necessary for the performance of a contract between the data subject and the controller, or to implement pre-contractual measures at the data subject's request.
- Public Interest – Where the transfer is necessary for important public interest reasons recognised by law.
- Legal Claims – Where necessary for the establishment, exercise, or defence of legal claims.
- Vital Interests – Where necessary to protect the vital interests of a person who cannot give consent.

Controllers relying on derogations must document the justification, record the risk assessment, and notify the NDPC where applicable.

5. Key Takeaways for Compliance Officers

Action Point	GAID 2025 / NDPA Reference	Why It Matters
Confirm if your recipient country has an NDPC adequacy decision	NDPA s. 42; GAID Sch. 5 para. 2	Transfers to adequate jurisdictions are straightforward and low risk.
Use an approved CBDTI if no adequacy decision exists	GAID Sch. 5 para. 3	CBDTIs ensure continued protection and accountability.
Avoid relying on derogations for regular transfers	GAID Sch. 5 para. 6	Derogations are for exceptional, one-off cases only.
Document and justify each cross-border transfer	NDPA s. 41(2) & GAID Sch. 5	Demonstrates accountability and compliance readiness.
Review vendor and intra-group transfer agreements	NDPA s. 39; GAID Sch. 5	Ensures processors outside Nigeria uphold equivalent standards.

Conclusion

Cross-border transfers are often the most complex part of data protection compliance. The GAID 2025 now provides a structured, risk-based framework for Nigerian organisations to follow, combining global best practice with local accountability. Data Protection Officers should map all international personal data flows, classify them under either adequacy, CBDTI, or derogation, and maintain proper documentation.

Short Test

1. Under the GAID 2025, what are the two main legal bases for cross-border data transfer?
   a. Adequacy and CBDTIs
   b. Consent and Contract
   c. Legitimate Interest and Public Interest
   d. NDPC approval only
2. True or False: Derogations under Schedule 5 of the GAID are intended for continuous data transfers between Nigeria and foreign entities.
3. What must a CBDTI include to be valid under the GAID?
   a. NDPC approval
   b. Enforceable rights for data subjects
   c. Effective remedies for breaches
   d. All of the above

ARTICLE 8: COMPARATIVE DATA PROTECTION PRACTICES ACROSS AFRICA

Highlights of frameworks in South Africa, Kenya, Ghana, and the African Union — common challenges in enforcement, awareness, and harmonisation

Welcome again to another edition of our Data Protection and Privacy Knowledge Management Series. We have spent the last seven weeks examining Nigeria's data protection framework and its evolving directives. In this article, we take a step back to look across the African continent; how other jurisdictions have structured their data protection regimes, and the practical challenges of implementation.

1. South Africa: A Mature Framework with Active Enforcement

South Africa's Protection of Personal Information Act 2013 (POPIA) remains one of the most comprehensive and operational data protection laws on the continent. The POPIA had a commencement date of July 2020 and one year compliance grace period. It came fully into force in July 2021 and is enforced by the Information Regulator of South Africa. The Regulator has broad powers to investigate complaints, issue enforcement notices, and impose fines.

In recent years, it has opened investigations into large-scale data breaches and issued compliance orders to organisations in the private and public sectors — a clear sign that enforcement is active and maturing (POPIA, 2013; Information Regulator SA, 2023).

POPIA's structure and principles are similar to the GDPR , covering key areas such as lawful processing, security safeguards, data subject rights, and cross-border transfers. Its challenge remains awareness and compliance across small and medium-sized enterprises, which form the backbone of the South African economy.

2. Kenya: Growing Compliance Culture and a Strong Regulator

Kenya's Data Protection Act, 2019 established a comprehensive framework aligned with international standards. The Office of the Data Protection Commissioner (ODPC) is responsible for enforcement and has issued key regulations, including

the Data Protection (General) Regulations, 2021, Registration of Data Controllers and Processors Regulations, 2021, and the Complaints Handling and Enforcement Procedures, 2021.

The ODPC has also released a Data Protection Handbook and DPIA guidance to help businesses comply (ODPC, 2022). Under the Act, data controllers and processors must register with the ODPC and are required to notify the regulator and affected individuals of personal data breaches (Kenya DPA 2019, ss. 18–24).

Practical compliance challenges in Kenya include limited technical expertise and high costs of implementing security safeguards. However, Kenya's regulatory approach has been proactive and transparent, with the ODPC frequently engaging in awareness and stakeholder education.

3. Ghana: Building Capacity within an Established Legal Framework

Ghana was one of the early adopters of data protection legislation in Africa. Its Data Protection Act, 2012 (Act 843) predates both Kenya's and Nigeria's frameworks. The Data Protection Commission (DPC Ghana) oversees implementation, registration, and enforcement.

Under the Act, all data controllers and processors operating in Ghana must register with the DPC and ensure fair, lawful, and secure processing of personal data (Ghana DPA, ss. 18–21). While the legislative structure is strong, the DPC continues to face capacity constraints and funding challenges that affect its ability to conduct widespread enforcement. Nevertheless, the Commission has launched annual awareness programmes and registration drives to improve compliance rates across industries.

4. The Continental Picture: The Malabo Convention and the African Union Data Policy Framework

At the continental level, the African Union Convention on Cyber Security and Personal Data Protection (commonly called the Malabo Convention) serves as Africa's first treaty dedicated to cybersecurity and personal data protection. Adopted in 2014, it aims to create a harmonised standard for African Union member states and to promote cooperation between national authorities (AU, 2014).

However, while many AU member countries have signed the Convention, fewer have ratified it, and practical implementation is slow. Despite this, the Malabo Convention remains a symbolic foundation for regional harmonisation efforts and has inspired several national laws, including Nigeria's NDPA 2023 and Kenya's DPA 2019.

Complementing the Convention is the African Union Data Policy Framework (2022), which sets out continental priorities for data governance, cross-border data flows, and responsible data innovation. The Framework encourages interoperability among AU member country laws, sustainable digital economies, and regional cooperation among supervisory authorities.

5. Common Challenges Across Africa

While progress across Africa is encouraging, several shared challenges persist:

- Enforcement Gaps: Many regulators, though legally empowered, struggle with funding and personnel limitations that delay investigations or hinder continuous oversight.
- Low Public Awareness: Data protection remains a niche topic for most data subjects. Awareness campaigns have not yet matched the scale of technological adoption.
- Harmonisation Difficulties: With over 30 national data protection laws now in force, aligning rules on cross-border transfers, adequacy, and jurisdiction remains a continental challenge.
- Digital Divide: The uneven distribution of digital literacy and infrastructure means some regions and sectors lag behind in both compliance and enforcement.

6. The Road Ahead

African regulators are increasingly engaging through platforms like the Network of African Data Protection Authorities (NADPA) to share best practices and build consistency in enforcement. The long-term goal is to establish harmonised mechanisms that facilitate safe data flows across the continent while respecting national sovereignty and innovation.

As Nigeria moves ahead with its NDPA 2023 and GAID 2025, the continent can look to cross-border regulatory dialogue as a pathway to balanced, sustainable digital development.

Short Test

1. Which South African authority enforces the POPIA?
    a. The Ministry of Justice
    b. The Information Regulator
    c. The Data Protection Commissioner
    d. The Constitutional Court
2. Under Kenya's Data Protection Act, who is responsible for issuing compliance regulations?
    a. The ICT Authority
    b. The Office of the Data Protection Commissioner
    c. The Communications Authority
    d. The Ministry of Technology
3. True or False: Ghana's Data Protection Commission does not require data controllers to register.
4. What is the name of the African Union treaty focused on data protection and cybersecurity?
    a. Addis Ababa Protocol
    b. Malabo Convention
    c. Nairobi Accord
    d. Kigali Framework
5. Which AU policy document seeks to harmonise data governance across African countries?
    a. AU Digital Strategy 2020
    b. AU Data Policy Framework
    c. African Continental Free Data Agreement
    d. ECOWAS Cyber Policy

ARTICLE 9: DATA BREACHES AND YOUR ORGANISATION'S RESPONSE PLAN

How to prepare for and respond to data breaches, and who to notify.

Welcome again to our Data Protection and Privacy Knowledge Management Series and we hope you are learning a lot. In articles 5 - 8, we explored Data Protection Impact Assessments (DPIAs), the Nigeria Data Protection Act 2023's General Application and Implementation Directive 2025 (NDPA-GAID 2025), cross-border data transfers, and compared data protection frameworks across Africa and the African Union.

In Article 9, we turn to a subject that every data protection professional must be prepared for: data breaches. Every smart privacy professional must have a plan to navigate personal data breaches. This is because even the most compliant organisation can experience a breach. The real test of accountability lies not in whether a breach happens, but in how efficiently it is detected, contained, and reported.

1. What is a Data Breach?

Section 65 of the Nigeria Data Protection Act (NDPA) 2023 describes a personal data breach as a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There are three broad categories of data breaches:

Type	Description	Example
Confidentiality breach	When data is disclosed or accessed by an unauthorised person.	Sending payroll data to the wrong recipient.
Integrity breach	When data is altered or corrupted without authorisation.	Malware changing customer records.
Availability breach	When data is lost or becomes temporarily or permanently unavailable.	Server crash or ransomware attack.

2. The NDPA's Approach to Data Breach Management

The NDPA 2023 and its NDPA-GAID 2025 improved the structure in place to address data breaches. Both instruments set out specific timelines, responsibilities, and documentation requirements for controllers and processors.

a. Processor's Obligation to Notify

When a data breach occurs, the data processor must immediately inform the data controller once it becomes aware of the breach. The processor is also legally obliged to respond to all information requests from the controller, to enable the controller to meet their own notification obligations.

This early notification should include available technical details such as the nature of the breach, the likely impact, and steps already taken to contain it. This duty is provided under Section 40(1) of the NDPA and Article 33(2) of the NDPA-GAID 2025.

b. Controller's Obligation to Notify

The data controller has the main responsibility for assessing and reporting breaches. Once aware of a breach (either directly or through a processor), the controller must determine whether the incident is likely to pose a risk or a high risk to the rights and freedoms of affected data subjects. This is typically done through a data breach assessment.

If the breach is likely to result in a risk, the controller must:

- notify the Nigeria Data Protection Commission (NDPC) within 72 hours of becoming aware of the breach.
- notify the affected data subjects.

This procedure is provided in Section 40(2) of the NDPA and expanded in Article 33 of the GAID.

3. Determining When a Breach is "High Risk"

The NDPA-GAID 2025 explains what factors may elevate a breach from simple risk to high risk. According to Article 33(2), controllers should consider:

- The type and sensitivity of personal data involved, especially if it includes biometric, health, or financial data.
- The number of individuals affected.
- The potential for identity theft, financial loss, or reputational damage.
- The ease with which the individuals can be identified from the data.
- The availability of safeguards such as encryption or pseudonymisation.

If these factors suggest that the breach could significantly affect individuals' rights, the incident qualifies as high risk, requiring direct communication with the affected data subjects.

4. Contents of a Breach Notification

Section 40(3) of the NDPA states that the notification to data subjects must be written in plain and clear language, explaining the breach, the context of the breach, the safeguards the controller has put in place, and other measures the data subjects can take to protect themselves and their personal data.

Article 33(5) of the NDPA-GAID 2025 lists the specific information that must be included in a breach notification to the NDPC or affected data subjects. The notification should include:

- A description of the nature of the breach, including the categories and approximate number of data subjects and records involved.
- The name and contact details of the Data Protection Officer.
- The likely consequences of the breach.
- The measures taken or proposed to address the breach and mitigate its effects.
- If notification is delayed, the reasons for the delay.
- If not all information is available immediately, the controller may submit the remaining details in phases, as long as there is no undue delay.

5. Record-Keeping and Accountability

Both controllers and processors must keep a detailed record of all personal data breaches, regardless of whether those breaches were reported to the NDPC (section 40(8), NDPA). This record is typically called a (Personal) Data Breach Register. This record should include:

- The facts of each breach.
- The impact(s) of each breach.
- The remedial action(s) taken, including notification of data subjects and supervisory authorities.

Maintaining this record helps organisations demonstrate compliance with the accountability principle in section 24 of the NDPA, and it supports internal learning and process improvement.

6. Building a Response Plan

Every organisation should have an internal breach response plan that clearly defines roles, escalation procedures, and communication channels. The plan should include:

1. Detection and Containment – Isolate affected systems and prevent further unauthorised access.
2. Internal Reporting – Report immediately to the Data Protection Officer or incident response team.
3. Risk Assessment – Evaluate whether the breach presents a risk or high risk to affected individuals.
4. Notification – Notify the NDPC and affected data subjects (if necessary) within 72 hours.
5. Documentation – Keep a full record of the event and decisions taken.
6. Review – Assess what went wrong and improve technical and organisational measures.

7. Why This Matters

Timely and transparent management of data breaches is essential for compliance and trust. Reporting within the required timeframe and keeping accurate records show accountability and preparedness. Failure to notify or unjustified delay can attract administrative sanctions under section 48 of the NDPA and could damage public trust in the organisation's data practices.

Thank you for following this series so far. In the next article, we will discuss how to build a privacy programme for your startup or MSME.

Short Test

1. Who must first notify whom when a processor becomes aware of a data breach?
    a. Controller notifies processor
    b. Processor notifies controller
    c. NDPC notifies both
    d. None of the above
2. Within how many hours must a controller notify the NDPC of a reportable breach?
    a. 24 hours
    b. 48 hours
    c. 72 hours
    d. One week
3. True or False: All breaches must be reported to the NDPC, regardless of risk level.
4. What must every controller and processor maintain internally, even for unreported breaches?
    a. Data inventory
    b. Breach register
    c. Compliance certificate
    d. DPIA record
5. Which of the following factors helps determine whether a breach is high risk?
    a. Sensitivity of the data involved
    b. Type of computer used
    c. Number of staff in the organisation
    d. Colour of company logo

ARTICLE 10: BUILDING A PRIVACY PROGRAMME FOR STARTUPS AND SMES

Practical Steps for Data Privacy Governance, Policies, and Compliance.

Welcome back to OTL Law and Nexa Advisory's Knowledge Management Series on Privacy and Data Protection. We have spent the past nine articles unpacking the building blocks of data protection. We have discussed topics ranging from the principles of privacy, the lawful bases for processing, the importance of assessments, to key obligations under the Nigeria Data Protection Act (NDPA) and the General Application and Implementation Directive (GAID 2025).

In this tenth article, we bring it all together.

A privacy programme is the architecture of compliant processing. It is the organisation's roadmap to embedding privacy principles into everyday operations. While principles and obligations provide the "what" of compliance, a privacy programme explains the "how".

For startups and small to medium-sized enterprises (SMEs), a privacy programme provides structure, consistency, and accountability. It ensures that data protection is not a one-off activity but an integrated part of the business culture.

1. Leadership Commitment and Accountability

Every privacy programme begins with clear ownership. Founders and executives must recognise that data protection is a business responsibility, not just a legal one. Leadership sets the tone for compliance and determines how seriously the rest of the organisation will take it.

Section 32 of the NDPA requires data processors and controllers of major importance to designate a Data Protection Officer (DPO). The DPO must have independence, expertise, and direct access to senior management. Smaller entities may rely on a licensed Data Protection Compliance Organisation (DPCO) to discharge this function until they can build internal capacity.

Practical Steps for Privacy Leaders:

- Secure executive sponsorship and allocate a privacy budget.
- Create a data protection steering committee that meets regularly.
- Include privacy performance indicators in organisational goals.

2. Map Your Data and Processing Activities

A privacy programme cannot function without understanding what data the organisation processes. Data mapping is the foundation of compliance because it provides visibility into where personal data is collected, how it moves, and why it is processed. Each organisation should document:

- The categories of personal data collected.
- The purpose for which data is processed.
- The lawful basis under the NDPA or GAID 2025.
- The data retention period.
- Where data is stored and who has access.
- Any third-party processors or vendors involved.
- Any cross-border transfers that occur.

This record forms the Data Map, which supports the Record of Processing Activities (ROPA) required under the NDPA and GAID 2025. It also helps demonstrate accountability and identify potential compliance gaps before an audit or investigation.

Practical Steps for Privacy Leaders:

- Use a spreadsheet or simple database to record data flows.
- Consistently review and update the ROPA (monthly or quarterly, depending on the size of your privacy programme).
- Work with heads of departments to validate details of data processing.

Example: Simplified Data Mapping Sheet

	Data Category	Source / Collection Point	Purpose of Processing	Lawful Basis	Storage Location	Access (Internal / External)	Cross-Border Transfer	Retention Period	DPIA Conducted
1.	Employee personal details (name, contact, ID, bank info)	HR Onboarding Form	Employment management, payroll	Contract	Local HR Server (Nigeria)	HR Dept, Payroll Vendor	No	5 years post-employment	Yes
2.	Customer contact data (email, phone)	Website signup form	Customer account creation, notifications	Consent	Cloud CRM (EU Server)	Marketing, Customer Support	Yes (EU)	2 years post-account closure	No
3.	Website analytics (cookies, device info, IP)	Website cookies	Service improvement, fraud detection	Legitimate Interest	Analytics Dashboard (Nigeria)	IT Dept, Security Vendor	No	1 year	No
4.	Financial transaction data	Payment gateway API	Payment processing and fraud prevention	Contract	Cloud Payment Processor (US)	Finance Team, Payment Vendor	Yes (US via CBDTI)	7 years (tax requirement)	Yes
5.	Customer complaints data	Contact form, SNAG submission	Dispute resolution	Legal Obligation	Local Server	Legal Team, DPCO	No	3 years post-resolution	Yes

3. Develop Core Policies and Procedures

Policies give structure to your privacy programme. They set out the organisation's stance on data protection and establish procedures for day-to-day operations.

Every organisation should have:

- Privacy Policy,: Explains to data subjects how their data is collected, used, and safeguarded.
- Data Retention and Disposal Policy: Defines how long data will be stored and how it will be securely deleted.
- Data Breach Response Policy, 2025: Describes how to identify, contain, report, and record breaches.
- Access Control and Security Policy: Outlines who can access personal data and for what purpose.
- Vendor Management Policy: Ensures that contracts contain required data protection clauses and that vendors comply with the NDPA and GAID 2025.

Practical Steps for Privacy Leaders:

- Use the templates provided by the NDPC or DPCOs as a starting point.
- Keep all policies in a shared, version-controlled repository.
- Review and update policies annually or when business processes change.

4. Build Awareness and Train Continuously

People are central to every privacy programme. A well-informed team helps reduce the risk of breaches and strengthens organisational resilience. It is important to train the entire staff about ethical data processing. Most importantly, the customer service (or customer support or customer excellence) team must be trained on every processing activity and the organisation's approach to processing. This allows them to relay important information to users about the organisation's data processing culture.

Article 30 of the GAID 2025 requires POs to ensure that all personnel receive regular training appropriate to their role.

Practical Steps for Privacy Leaders:

- Include data protection awareness in employee induction.
- Provide refresher training every quarter.
- Track participation and test understanding through short assessments.
- Include case studies from Nigerian and international enforcement actions.

5. Integrate Privacy by Design and by Default

"Privacy by Design and by Default" means embedding privacy into systems and processes from the outset, not as an afterthought. The GAID 2025 encourages data processors and controllers to prioritise privacy by design and by default to guarantee compliance with the principles of data processing (Schedule 1, Paragraph 2, GAID 2025).

Practical Steps for Privacy Leaders:

- Involve the DPO in all new projects at the design stage.
- Apply techniques such as data minimisation, pseudonymisation, and encryption.
- Conduct Data Protection Impact Assessments (DPIAs) fin accordance withor high-risk processing.
- Create a privacy checklist for developers and product managers.

6. Manage Vendors and Cross-Border Transfers

Startups often rely on cloud platforms and international service providers. This reliance introduces compliance obligations around third-party management and cross-border transfers.

Schedule 5 of the GAID 2025 provides clear guidance on Cross-Border Data Transfers. Data may only be transferred outside Nigeria where:

- The destination country or organisation ensures an adequate level of protection, or
- The parties have executed a Cross-Border Data Transfer Instrument (CBDTI) approved by the NDPC.

Practical Steps for Privacy Leaders:

- Maintain a vendor register indicating the transfer mechanism used.
- Update data processing agreements to meet GAID 2025's mandatory clauses.
- Conduct annual vendor due diligence and request updated security certifications.

7. Monitor, Audit, and Continuously Improve

A privacy programme is not a static document. It must evolve with the business and regulatory expectations.

The NDPA and it's GAID requires DPOs to submit Internal Semi-Annual Data Protection Reports. It also requires data processors and controllers of major importance to file Compliance Audit Returns (CARs) through licensed DPCOs.

Practical Steps for Privacy Leaders:

- Conduct annual internal audits and management reviews.
- Maintain logs of breaches, complaints, and subject rights requests.
- Track corrective actions in a compliance register.
- Benchmark practices against NDPC and international standards.

Conclusion

A privacy programme brings together every aspect of data protection we have discussed so far. It is the framework that translates principles, legal obligations, and assessments into a structured system for everyday practice. It ensures that privacy compliance is intentional, documented, and demonstrable.

For startups and SMEs, building a privacy programme may appear daunting, but starting small is perfectly fine. Begin with leadership commitment, policy documentation, and training. Then, build out data mapping, audits, and continuous improvement as your organisation grows. A well-designed privacy programme strengthens trust, reduces risk, and demonstrates accountability to clients, partners, and regulators.

If you still have questions or you need help with building a privacy programme for your organisation, you can respond to this email and we'd be sure to assist you.

In the next article, we will discuss data subject rights and how organisations can operationalise requests for access, correction, deletion, and portability.

Short Test

1. What is the purpose of a privacy programme?
    a. To market data services
    b. To provide a roadmap for compliant data processing
    c. To replace legal advice
    d. To manage customer engagement only
2. Under which NDPA provision must organisations designate a DPO?
    a. Section 32
    b. Section 25
    c. Section 7
    d. Section 15
3. What is the primary purpose of data mapping?
    a. To understand the flow and purpose of personal data
    b. To track website visitors
    c. To assess employee satisfaction
    d. To review system backups
4. Which GAID Schedule addresses Cross-Border Data Transfers?
    a. Schedule 4
    b. Schedule 5
    c. Schedule 7
    d. Schedule 9
5. True or False: Privacy by Design is applied only after a product is launched.

ARTICLE 11: DATA SUBJECT RIGHTS: LEGAL OBLIGATIONS AND PRACTICAL STRATEGIES FOR EFFECTIVE COMPLIANCE

Understanding what the law requires and how organisations can respond efficiently and confidently

We are almost at the end of our Privacy and Data Protection Knowledge Management Series. In the last few articles, we explored lawful processing, risk assessments, and privacy programmes. This week, we are shifting our focus to one of the most practical and human aspects of data protection: the rights of data subjects.

Privacy is a fundamental human right guaranteed by the Nigerian constitution and data protection is an extension of that right. At the heart of every data protection law is the idea that individuals should have control over their personal data. Data subject rights turn that idea into action. They give data subjects the ability to request access to, correction of, and even the deletion of their personal data. For organisations, honouring these rights is both a legal duty and a test of how well their privacy framework actually works.

In this article, we will discuss what these data subject rights (DSRs) are, what the law requires when they are exercised, and how organisations can handle them efficiently and confidently.

The Nigeria Data Protection Act (NDPA) 2023 and the General Application and Implementation Directive (GAID) 2025 place DSRs at the centre of accountability. It is not enough to have policies. Organisations must be able to receive, verify and fulfil requests in a way that is timely, secure and auditable.

1. Data Subject Rights

The NDPA sets out the principal rights of data subjects in sections 34 to 38. The GAID 2025 provides practical direction on how those rights should be exercised in articles 36 to 39. It also introduces the Data Subject's Standard Notice to Address Grievance (SNAG) procedure in article 40, allowing data subjects to lodge a standard notice to seek remediation.

Below is a short summary of the main rights, with the legal references:

Right	What it means	Reference
Right to be informed	Data subjects must know in adequate detail all that the data controller intends to do with their data. The right to be informed is relevant before processing and is related to the principle of transparency of processing.	NDPA s. 34 (1)(a)
Right of access	Data subjects must be able to request information about how a data controller has processed their data. This right is relevant during or after processing.	NDPA s. 34(1)(b)
Right to rectification	Data subjects can request correction of inaccurate or incomplete personal data. This is related to the principle of accuracy of processing.	NDPA s. 34(1)(c); GAID art. 36
Right to erasure (or right to be forgotten)	Data subjects can request deletion of their data, in certain circumstances. For example, where processing is unlawful or consent is withdrawn.	NDPA s. 34(1)(d) and 34(2); GAID art. 38
Right to restriction of processing	Data subjects can request that processing be limited in certain situations while issues are resolved.	NDPA s. 34(1)(e)
Right to data portability	Data subjects can request their data in a structured machine-readable format to transfer to another controller.	NDPA s. 38; GAID Art. 37
Right to withdraw consent	Data subjects may at any point during processing, withdraw their consent to the processing of their personal data, where the legal basis of that processing was consent. Withdrawal of consent must be as easy as giving consent.	NDPA s. 35
Right to object	Data subjects may object to the processing of their personal data based on legitimate interests or for direct marketing.	NDPA s. 36
Right not to be subject to automated decision making	Data subjects have the right to not be subject to fully automated decision-making, including profiling, especially where processing carries legal implications. They can request human intervention for this kind of decision-making.	NDPA s. 37
Right to lodge a complaint with the NDPC	Data subjects have the right to report non-compliant processing of their personal data to the Nigeria Data Protection Commission (NDPC). This has been made easy by the newly introduced SNAG Procedure	NDPA s. 46, GAID art. 39 & 40

Data controllers and processors can refer to the above table when drafting policies, notices and DSR procedures so that operational rules align with the statute and the directive.

2. How organisations should receive and manage data subject requests

Operationalising rights means building the people, process and technology elements into your privacy programme. Below are practical steps that privacy leaders should implement.

a. **Set up clear intake channels**

Provide multiple secure channels for DSR receipt, for example an online form, a dedicated email address and physical mail. Make the process obvious in privacy notices. The GAID 2025 expects accessible routes for exercising rights.

b. **Verify identity securely and proportionately**

Before disclosing data, verify the data subject's identity. Use a risk-based approach. For low-risk requests, email verification may suffice. For more sensitive data consider two factor verification or a certified identification document. Always log the type of verification method used.

c. **Keep a Data Subject Request Log**

Record every request and every action taken. A consistent log supports accountability and makes NDPC audits easier. Below is a practical template you can adopt in practice:

Ref No.	Date Received	Requestor Name	Contact Details	Type of Request	Identity Verified (Y/N)	Date Verified	Assigned To	Response Deadline	Action Taken	Date Completed	Notes
DSR-001	2025-09-01	Jane Doe	jane@example.com	Access	Y	2025-09-01	DPO	2025-10-01	Provided copy of records	2025-09-10	Redacted third party data
DSR-002	2025-09-03	John Smith	+2348012345678	Erasure	N	2025-09-04	Ops Lead	2025-10-03	Assessed retention conflicts	2025-09-20	Retention required for tax law

d. **Track timelines and extensions carefully**

Neither the NDPA nor the GAID 2025 provide for a specific time for data controllers to respond to DSR requests. Section 34 of the NDPA states that data controllers should honour data subject's requests without constraint or unreasonable delay. Other privacy regimes like the General Data Protection Regulation (GDPR) require data controllers to respond within one month of receipt of the request. Complex or numerous requests can be extended by up to two months, but the data subject must be informed of the reason for the delay within one month.

e. **Use a role based workflow**

Designate and train first line staff to triage requests, e.g. customer service officers, a verification team to authenticate requests, a legal or privacy owner to review complex requests, and an operations team to extract or delete data. The Data Protection Officer (DPO) should have overall oversight and final sign off.

f. **Prepare for common operational issues**

Common operational issues in honouring data subject's rights requests include:

- Data fragmentation. Use your data map to locate data across systems.
- Third party data. Confirm whether the data is held by a processor and coordinate fulfilment. Data Protection Agreements or clauses should require processors to assist with DSRs.
- Conflicting legal obligations. If retention obligations exist under other laws, document the legal exception and explain it to the data subject.

g. **Communicate clearly and in plain language**

Provide responses that are concise, intelligible, and free of technical jargon. If the request is refused, explain the legal basis for the refusal and provide details of the right to lodge a complaint, including the use of the SNAG procedure.

3. Common lawful grounds for refusing or limiting requests

The NDPA and GAID 2025 allow controllers to refuse manifestly unfounded or excessive requests. When refusing DSR requests, controllers must explain the reason and inform the data subject of the right to complain to the NDPC. Typical lawful grounds for limitation include:

- Requests that would adversely affect the rights and freedoms of others, such as revealing third party personal data.
- Requests that are manifestly unfounded or excessive. The controller may only charge a reasonable fee where allowed.
- Where legal retention obligations override erasure requests. Document the conflict and provide a partial response where possible.

Record every refusal carefully in the DSR log, stating the legal basis for the refusal and any appeal route.

4. Data portability and secure transfer

For portability requests, provide data in a structured, commonly used, machine readable format such as CSV or JSON. When transmitting the data, use secure channels and validate the receiving controller. Confirm whether the data subject wants the data sent directly to another controller and document consent for that transfer.

Portability does not require you to create new data or transform data into a proprietary format. It covers data provided by the data subject and data generated by their activity.

5. SNAG procedure and escalation

The SNAG procedure in article 40 of GAID 2025 provides a standard notice mechanism, using the praecipe form in schedule 9 of the GAID, for data subjects to lodge complaints and seek remedies. Controllers should:

- Build a process to receive SNAG notices, log them and escalate to the appropriate functional owner.
- Respond to the SNAG without undue delay (reasonably, within one month) and keep the data subject informed.
- Where internal remedy is insufficient, inform the data subject of their right to escalate to the NDPC.
- Ensure your DSR and SNAG processes are aligned so that a complaint or a rights request is handled consistently and tracked in the same governance tools.

6. Practical notes for privacy leaders

- Embed DSR request handling into the privacy programme and test it regularly through simulations.
- Keep a published contact and an easy to use request form on your website. Visibility reduces friction and shows accountability.
- Train customer facing staff to recognise suspected DSR requests and escalate them immediately.
- Maintain a playbook for complex requests with template letters, verification steps and legal references.
- Review processor agreements to ensure contractual cooperation and set response time expectations.

Conclusion

Data subject rights are at the centre of every privacy framework. They remind us that personal data ultimately belongs to the individual. For organisations, honouring these rights goes beyond having policies on paper. It means putting real systems in place to receive, assess and respond to requests properly.

In our next and final article, we will turn to two industries where these rights are often put to the test, fintech and health-tech. We will explore their unique challenges and how they can apply everything we have learned in this series to achieve real compliance in practice.

Short test

1. Under the NDPA, within what period should a controller respond to a valid DSR request?
2. Name two items that should be recorded in a Data Subject Request Log.
3. Which GAID 2025 article introduces the SNAG grievance procedure?
4. True or false: Portability requires controllers to convert data into a proprietary format.
5. What should you do if a deletion request conflicts with a statutory retention obligation?

ARTICLE 12: DATA PROTECTION IN THE FINTECH AND HEALTHTECH SECTORS

Analysing sector-specific challenges and emerging norms.

Welcome to the last article of the OTL Law & Nexa Advisory Knowledge Management Series on Data Protection and Privacy in Nigeria and Africa. We have journeyed through the concept of personal data, data protection, the roles, responsibilities, and principles of data processing, data subject rights, and building a privacy programme.

In this final article, we will spotlight the fintech and healthtech sectors, discussing their peculiar data processing needs, specific challenges, emerging norms and practical steps for DPOs to ensure continued compliance. These sectors are important because of the nature of the data they process and the risks involved in their processing activities.

1. Understanding the Fintech Context

Fintech companies rely on data for almost every part of their operations. They collect and process Know Your Customer (KYC) records, transaction histories, credit information, device fingerprints, behavioural analytics and, in several cases, biometric identifiers. Both the nature of this data and the laws regulating financial services make processing in this sector particularly sensitive.

2. Why Fintech Data Processing Requires Careful Governance

- Biometric Information for KYC: Financial institutions often process biometric information (e.g. fingerprints and facial recognition) for Multi-Factor Authentication (MFA) to guarantee the security of users' data. This biometric information is regarded as sensitive data and as such, requires a higher level of protection.
- Long-term retention obligations: Financial regulations often require fintech organisations to store transactional records, accounting information, and KYC documents for about seven years. Long retention increases exposure to security incidents and therefore requires strong governance.

- Revealing nature of financial data: Unauthorised access to financial data can expose spending habits, financial strength, loan history, and behavioural patterns. In some African countries, such as Ghana, financial data is classified as sensitive data.
- Additional industry security standards: Fintech organisations that process cardholder data must comply with PCI DSS in addition to NDPA and GAID 2025 requirements.
- Frequent cross-border processing: Fintech platforms often rely on global service providers for cloud hosting, transaction processing, analytics or communication. Part 8 of the NDPA and schedule 5 of the GAID 2025 apply to these transfers.

3. Practical Steps for Continued Compliance in Fintech

a. Identity Verification and KYC Processing

1. Document the lawful basis for each category of KYC data.
2. Provide layered privacy notices that explain the use of biometrics or automated verification.
3. Conduct DPIAs for all biometric and fraud detection tools.
4. Align retention periods with regulatory requirements and delete KYC data promptly once retention lapses.
5. Implement strict access controls and audit trails for identity data.

b. Transaction Records and Long-term Storage

1. Map every database or platform storing transaction history.
2. Separate active data from archived records.
3. Encrypt all records in transit and at rest.
4. Implement deletion workflows for data older than the seven year retention period.
5. Review retention obligations annually, especially when regulations change.

c. Fraud Monitoring and Automated Processing

1. Provide clear information to users about profiling and automated decisions.
2. Maintain human oversight for automated transaction blocking.
3. Conduct accuracy reviews and fairness assessments of fraud detection systems.
4. Document automated decision processes in line with GAID 2025 requirements.
5. Include all fraud systems in annual DPIA reviews.

d. **Third Party and Vendor Management**

1. Record all processors and sub-processors in the vendor register.
2. Use regulator-compliant Data Protection Agreements (or Addendums).
3. Verify security safeguards and cross-border transfer mechanisms.
4. Conduct vendor risk assessments at least annually.
5. Maintain updated evidence of compliance reports from high risk vendors.

4. High Security Obligations in Fintech

Fintech organisations operate in one of the most attacked digital environments. Their security measures must therefore exceed the standard baseline. Key expectations include:

a. Robust access control systems: Fintech systems should implement role-based access control, multi-factor authentication and session timeouts. Administrative access should be monitored with privileged access management tools.

b. Encryption across all environments: Encryption must be applied in transit and at rest. Sensitive fields such as card numbers, bank details and unique identifiers should be tokenised.

c. Pseudonymisation and data minimisation: For analytics or fraud modelling, fintech organisations should use pseudonymisation techniques that separate identity from behavioural data. Only the minimum data required for each use case should be processed.

d. Cloud security: Fintech platforms using cloud hosting should:

   i. Implement network segmentation.
   ii. Enable continuous monitoring.
   iii. Deploy intrusion detection and prevention systems.
   iv. Maintain incident logging and real-time alerts.

e. Use of Privacy Enhancing Technologies: Techniques such as differential privacy, secure multiparty computation, encrypted analytics and tokenisation strengthen compliance when processing high volumes of financial data.

5. Understanding the Healthtech Context

Healthtech organisations process special category data such as diagnoses, treatment history, genetic information, reproductive health data, mental health records and biometric measurements. These are sensitive data as defined in section 65 of the NDPA.

6. Why Healthtech Data Processing Requires Stronger Safeguards

a. Intrinsically sensitive nature of health data: Misuse of medical records can result in discrimination, stigma, financial disadvantage and long-term harm.
b. Vulnerability of data subjects: Some patients are considered vulnerable (e.g. children, and mentally challenged patients) under schedule 6 of the GAID 2025,and therefore require enhanced transparency and care.
c. Complex retention obligations: Medical records must often be retained for long periods for continuity of care.
d. Cross-border flows in telemedicine: Cloud-based health platforms regularly transmit data across borders. The NDPA and schedule 5 of the GAID 2025 apply to these flows.

5. Practical Steps for Continued Compliance in Healthtech

a. Consent and Transparency
    i. Obtain explicit consent for processing special category data.
    ii. Use clear and accessible notices tailored to patient literacy levels.
    iii. Separate consent for research or secondary uses.
    iv. Maintain a detailed consent register.
    v. Provide clear instructions for withdrawal of consent.
b. Access Control and Clinical Systems
    i. Use strict role-based access rules for medical records.
    ii. Maintain audit logs that record every access.
    iii. Enforce multifactor authentication.
    iv. Review access permissions regularly.
    v. Segregate clinical, administrative and analytics systems.
c. Data Security and Storage
    i. Encrypt health data in transit and at rest.
    ii. Use pseudonymisation or anonymisation for research.
    iii. Maintain secure backup and disaster recovery plans.
    iv. Implement device-level security for clinicians who use mobile tools.
    v. Conduct DPIAs for new clinical technologies.
d. Telemedicine and Cross-Border Storage
    i. Map all telemedicine processing activities and the locations of hosted data.
    ii. Review cross-border transfers in line with part 8 of the NDPA, including ensuring that international partners meet adequacy or CBDTI requirements.
    iii. Use secure video and messaging platforms.
    iv. Inform patients where international hosting is used.

6. High Security Obligations in Healthtech

Health information requires some of the strongest protections in data governance. Controllers must focus on:

a. Explicit consent management

Explicit consent is the default for processing health data. Consent must be freely given, specific, informed, recorded, and easily withdrawn.

Healthtech DPOs should consider implementing digital consent dashboards and paper-based alternatives for in-clinic patients.

b. Enhanced security controls

Health organisations should use:

1. Advanced encryption.
2. Strong authentication protocols.
3. Secure endpoint devices.
4. Regular penetration testing.
5. Automated threat detection on clinical systems.

c. Additional controls for special category data

Records relating to genetics, mental health, reproductive health or HIV status should be stored with heightened safeguards and strict access control rules.

Conclusion

Fintech and healthtech organisations operate in data intensive environments that involve high risk processing, long retention periods and sensitive categories of information. Their compliance responsibilities are therefore more demanding. A strong privacy programme, clear governance structures, regular DPIAs and robust security measures are essential to ensure safe processing and build user trust.

This article concludes the OTL Law & Nexa Advisory Data Protection and Privacy Knowledge Management Series for players in the Nigerian and African tech ecosystem. We hope the series has provided clarity, structure and practical guidance for every organisation that seeks to build compliant and responsible data processing practices.

OSUNTUYI & TOKAN-LAWAL LAW

NEXA ADVISORY

THANK YOU

ABOUT OTL LAW

Founded in 2022 by **Isaac Abayomi Osuntuyi** and **Adefoworola "Tope" Tokan-Lawal**, Osuntuyi & Tokan-Lawal Law (OTL Law) is a boutique law firm based in Lagos, Nigeria's commercial hub, providing premium legal services to individuals, families, and entities both domestically and internationally. Their combined wealth of experience and extensive legal knowledge forms the foundation for efficient and effective legal representation.

email: info@otllaw.com

ABOUT NEXA ADVISORY

Nexa Advisory is a boutique legal, compliance, and data protection consultancy bridging the gap between operational growth and regulatory integrity. Nexa exists at the nexus of law, governance, and business.

'Tife Ekundayo is a lawyer and privacy consultant with multi-jurisdictional experience spanning Africa, Europe, and the United States. She advises businesses and institutions on data protection, privacy compliance, and technology law, with a focus on bridging the gap between global best practices and Africa's evolving digital landscape. Through Nexa Advisory, 'Tife helps organisations build practical and scalable regulatory and privacy programmes that foster trust and innovation.

email: info@nexaadvisory.co

instagram: @nexa_advisory