BANWO & IGHODALO

SYNOPTIC ANALYSIS OF THE NIGERIA DATA PROTECTION ACT – GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE ("GAID") 2025

APRIL 30, 2025

On March 20, 2025, the Nigeria Data Protection Commission ("**NDPC**" or "**the Commission**"), pursuant to its powers in the Nigeria Data Protection Act ("**NDPA**" or "the **Act**"), issued the NDPA General Application and Implementation Directive ("**GAID**"), which is to take effect from September 19, 2025.

We have highlighted below some of the key provisions introduced by GAID that you need to know.

1. Applicability

With the issuance of the GAID, the Nigeria Data Protection Regulation (NDPR) 2019 will no longer govern data privacy and protection. However, actions taken pursuant to the NDPR prior to the implementation of GAID will remain unaffected. Additionally, as the NDPR 2019: Implementation Framework 2020 was introduced to supplement the NDPR, its applicability as a legal instrument will also cease with the introduction of the GAID. Therefore, the two main laws that will regulate data protection in Nigeria, with effect from September 19, 2025, are the **NDPA** and the **GAID**.

2. Material and Territorial Scope of the NDPA

The GAID mandates, as a constitutional obligation, a careful consideration of both the material and territorial scope of the NDPA vis-à-vis its objectives before decisions that affect individuals' fundamental right to privacy are made.

The GAID directs that in determining the issues of the right of a data subject and question of domiciliation of the data controller or data processor, where the data controller or processor is not domiciled in Nigeria but processes the personal data of data subjects in Nigeria, Sub-Articles 3 and 4 of Article 1 of the GAID shall be relied upon for guidance as follows:

I. In accordance with the principle of universality of civil liberties, every individual is entitled to the protection of their fundamental rights, including the right to privacy, no matter where they are located.

II. Accordingly, the following categories of people shall be entitled to the enjoyment of data subject rights under the NDPA:

(a) data subjects in Nigeria, regardless of nationality or immigration status,

(b) those whose data has been transferred to Nigeria,

(c) those whose data transits through the country (with limited obligations on controllers/processors); and

(d) Nigerian citizens abroad, subject to international law and mutual legal assistance.

III. The rights of the foregoing persons to protection under the Act shall, however, be subject only to the derogations permitted under the 1999 Constitution and any pre-emptory norm or international treaty applicable to Nigeria under International Law.

3. Material Context of Data Processing and the Priority of the NDPA

All individuals, bodies, or authorities involved in personal data processing have a duty of care to carefully assess the material context of personal data processing with a view to ascertaining whether such processing aligns with the constitutional right to privacy. The GAID indicates that the material context of data processing is essentially under the Exclusive Legislative List, 2nd Schedule to the 1999 Constitution, and mandates of Federal Executive Bodies.

Data controllers and processors must consider the material nature of data—including its value, volume, and speed—and implement technical and organizational measures to manage the associated risks, ensuring compliance with the privacy standards set by the NDPA.

4. Statutory Remedy for Double or Multiple Regulatory Frameworks on Data Protection

The GAID, with a view to ensuring clarity and effectiveness in regulating data protection, re-emphasises the clear priority of the NDPA over conflicting laws as enshrined in section 63 of the NDPA. It further directs that where any other law conflicts with the provisions of the NDPA concerning personal data processing, the NDPA takes precedence.

Furthermore, it is worth noting that, in the event of a conflict between the NDPA and the GAID, the provisions of the NDPA will take precedence

5. Evaluation of Exemptions to the Act

Data controllers/processors that are desirous of relying on the exemptions from the applicability of the NDPA under section 3 of the Act are required to comply with those provisions of the Act that are not covered by the exemption, such as principles of personal data processing, lawful basis for data processing, designation of Data Protection Officers (where required), notification in the event of personal data breach, and protection of data subjects' rights. The Commission will hold data controllers or processors accountable for any violation of these provisions.

In assessing data processing activities exempted under the Act, the Commission will consider factors such as the constitutional derogation allowed, the lawful basis for data processing, the impact on data subjects, compliance with data protection principles, the proportionality and necessity of the processing, and the ability of data subjects to lodge complaints with the Commission.

Individuals who process personal data solely for personal or household purposes are required to respect the privacy of the data subject. Such individuals may be held accountable for actions that put the privacy of others at risk, such as:

a. granting permission to data controllers or processors to access phone contacts via software or apps,
b. sharing or transferring personal data without consent,
c. neglecting to properly safeguard devices storing personal data,
d. disclosing personal data verbally or in writing, and
e. unauthorized access to someone else's personal data.

6. Compliance Measures for Data Controllers and Processors

The GAID provides a summarised list of compliance measures expected of data controllers and processors. Some of the key compliance measures include:

- Registration: Data controllers and processors of major importance must register with the Commission as applicable.
- Compliance Audit Report: Compliance audit is to be carried out within 15 months of commencing business, and annually. Thereafter, data controllers and processors of major importance (Ultra High Level and Extra-High Level) are to submit their Compliance Audit Returns (CAR) no later than March 31 of each year.
- Data Protection Officer: A Data Protection Officer (DPO) must be appointed by data controllers and processors of major importance, with additional support if necessary, especially where the data controller or the data processor carries out data processing or interfaces with data subjects on multiple platforms and places.
- Training & Sensitization: Carry out regular scheduled staff training and internal sensitization on data privacy is required.

- Compliance Schedules: Identify all obligations under the NDPA and prepare schedules of compliance.
- Privacy Policies: Organisations must develop and display privacy policies, ensuring transparency in data processing. The GAID also indicated the type of disclosures that will meet the transparency requirements.
- Breach Notifications: Prompt reporting of personal data breaches to the Commission and affected individuals is mandatory.
- Data Subject Rights: Systems must be designed to facilitate easy access, correction, and transfer of personal data for data subjects.
- Data Protection Impact Assessment: DPIAs are to be carried out when required under the NDPA, or when directed by the Commission.
- Semi-Annual Data Protection Reports: Organisations are to maintain semi-annual data protection reports containing a detailed analysis of data processing within six (6) months;
- Monitoring, Evaluation, and Maintenance of Data Security System: Data controllers and data processors are required to undertake scheduled monitoring, evaluation and maintenance of their data security systems in order to guarantee data confidentiality, integrity and availability.

7. Designation as a Data Controller or Data Processor of Major Importance ("DCPMI")

The GAID also provided guidance in the interpretation of certain elements of the statutory definition of Data Controller or Data Processor of Major Importance under section 65 of the NDP Act as follows:

(i) "***Operating in Nigeria***" will be construed to include a data controller or a data processor who may not be domiciled in or resident in Nigeria but targets a data subject in Nigeria. This is in line with the provision of section 2(2)(a) of the NDPA on the Application of the Act, as well as sections 24(3) and 44 on the need to hold accountable data controllers and processors whose processing activities significantly impact the economy, society or security of Nigeria.

(ii) "***of value or significance to the economy, society or security of Nigeria***" the Commission, in carrying out an objective assessment of this requirement, shall take into consideration all relevant factors, including but not limited to the following:

a) The risks that data processing by a data controller or a data processor poses to a data subject if such data controller or data processor is not under the obligation imposed by the NDPA on a data controller or a data processor of major importance as contemplated by section 29(1)(a) of the NDPA;
b) The implication for data sovereignty where data controllers or data processors may advertently or inadvertently transfer data outside Nigeria to the detriment of the economy, society or security of Nigeria;
c) The sensitivity of the personal data involved;
d) Data driven financial assets entrusted by data subjects in the care of the data controller or data processor;
e) Reliance on third-party servers or cloud computing services for the purpose of substantial processing of personal data;
f) Substantial involvement in cross-border data flows;
g) Use of filing systems and automation of data processing;
h) Number of data subjects involved; and
i) The need for international standard certifications for people, processes and technologies involved in data confidentiality, integrity and availability.

8. Registration as a Data Controller or Data Processor of Major Importance ("DCPMI")

In line with the NDPA and Guidance Notice issued on February 14, 2024, GAID emphasizes that data controllers and processors of major importance must comply with the following updated registration and reporting requirements:

a. Mandatory Registration: Data controllers and processors of major importance must register with the Commission in accordance with the Guidance Notice.
b. Obligations of Registration Categories: All entities that are categorized as Ultra High-Level (UHL) and Extra High-Level

(EHL) must register once with the NDPC and thereafter file Compliance Audit Return (CAR) annually. While entities categorized as Ordinary High-Level (OHL) must renew their registration annually, they are not required to submit CAR annually.

c. Notification of Changes: Data controllers and processors of major importance must inform the Commission of any significant changes to the information submitted during their registration within 60 days, via the NDPC's online registration portal or email.
d. Removal from Register: If an entity no longer meets the classification criteria for data controllers and processors of major importance, it may request removal from the register, but such entity must settle any outstanding fees to the NDPC.
e. Public Register: The Commission will publish and update the list of registered data controllers and processors of major importance annually on its official website.

9. Entities Exempted from Registration with the NDPC

Following the decision of the Federal High Court in the case of *Frank Ijege v. Nigerian Data Protection Commission*, the Commission has provided clarification on the entities exempt from registration. The exempted entities include:

a) Traders or artisans who do not transmit personal data as a trade or business object to other data controllers or processors that may process the transmitted personal data for their business goals;
b) Traders with less than fifteen (15) employees, or artisans who do not keep any specific filing system of personal data relating to their customers, except routine phone contact files, receipts data, contact addresses and electronic mail addresses; and
c) Community of friends, professionals or people of common interest who interact on social media platforms.

In addition to the above-listed groups, the Updated Guidance Notice, exempts the following categories of data controllers and data processors of major importance from registration:

a) Community-Based Associations;
b) Faith-Based Organisations;
c) Foreign Embassies and High Commissions;
d) Judicial establishments or bodies carrying out adjudicatory functions; and
e) Multigovernmental Organisations.

10. Summary of Key Points on Filing of Compliance Audit Returns (CAR)

The GAID in Article 10 outlines the requirements for filing CARs and introduces important updates not present in the NDPR and NDPA, such as:

- Periodic Audits: Data controllers and processors must conduct periodic compliance audits to reduce the risk of data breaches, using a risk-based approach that is focused on people, processes, and technologies involved in data processing.
- Privacy Audit Controls: Data controllers and processors must adopt privacy audit controls in line with global best practices.
- Risk-Based Auditing: Data controllers and processors must identify points of risk and determine the appropriate technique and frequency of audit for each point of risk.
- Filing: DCPMI must file CAR annually through a Data Protection Compliance Organisation (DPCO). For those established before June 12, 2023, the CAR must be filed by March 31 each year. After filing, the Commission may issue a Compliance Audit Returns Certificate.
- Filing Fees: The cost of filing CAR with the NDPC has significantly increased, and data controllers and data processors are expected to pay administrative fees to the NDPC. Below is the breakdown of the various applicable fees for filing the CAR with the NDPC:

S/N	Category	Tier	Fees (₦)
1.	Ultra-High Level – UHL	A – 50,000 data subjects and above.	1,000,000
		B – 25,000-49,999 data subjects.	750,000
		C – below 25,000 data subjects.	500,000
2.	Extra-High Level – EHL	A – 10,000 data subjects and above.	250,000
		B – 5,000-2,500 data subjects.	200,000
		C – below 2,500 data subjects.	100,000

- Penalty for Non-Compliance: Penalty for failure to file CAR within the specified time attracts an administrative penalty equal to 50% of the filing fee.
- Additional Information: The Commission can request additional information from data controllers or processors after CAR submission.
- Device Audits: Personal data accessed through an online device by a data controller or processor is susceptible to security breaches via cyber technology. The GAID stipulates that, audit of such devices should be conducted as often as necessary to ensure data security.

11. Data Processing Fees

The updated Guidance Notice states that DCPMIs in the category of MDP-UHL are required to pay an administrative fee of ₦ 5,000 for each processor that is engaged by the DCPMIs, within a period of twelve (12) months. However, when a data controller transfers the data processing activity of its data processor to another data processor, it shall not be required to pay another data processing fee for the new processor within the same twelve (12) month period. Additionally, if a data controller pays for the renewal of registration of its data processors, MDP-OHL category, the data controller will not be required to pay a data processing fee for the same data processor.

12. DPO Responsibilities and Reporting Requirements

Every data controller and data processor must appoint a DPO who may either be a member of staff or an outsourced resource under a service contract. The DPO shall be responsible for all the data protection issues within the organization and shall be required to work with management to resolve such issues.

In the performance by DPOs of their duties, GAID emphasizes that:

a) DPOs must perform their tasks without any coercion, pressure or influence and cannot be dismissed or penalized for carrying out their duties.
b) DPOs must report directly to the management of the data controller or processor.
c) Data subjects must be able to contact the DPO and exercise their rights under the Act.
d) DPOs should be bound by confidentiality obligations in the performance of their duties and may take on other tasks, provided there is no conflict of interest.

The DPO are required to compile and submit a semi-annual data protection report to management, which should be included in the Record of Processing Activities (RoPA) and verified by a DPCO during the compliance audit. The report shall contain the compliance status of the data controller or data processor under the NDPA, particularly taking into account issues listed in Article 13(5) of the GAID.

13. Annual Assessment of DPOs

The NDPC will commence the Annual Credential Assessment ("ACA") of registered DPOs to ensure that each DPO maintains the level of professionalism required to carry out their responsibilities. The DPO assessment will be based on DPO assessment metrics provided in Schedule 3 of the GAID and payment of prescribed fees to the NDPC. The certification and training obtained by a DPO will be the basis of ascertaining fitness to carry out the duties of the office. In addition, a database of Certified DPOs will be created and maintained by the Commission.
DPO certification and verification requirements are as follows:

a) A DPO must follow the Act, GAID, the Code of Conduct for DPCOs, and any other relevant guidelines issued by the Commission, along with any professional body ethics or directives the DPO is bound by.

b) The Commission will verify a DPO's certification as part of the Compliance Audit Return (CAR) or registration process under the Act.

c) The Commission may award verification scores or deny verification if the DPO's proof of Continuous Professional Development (CPD) is not verifiable or lacks credibility.

d) The DPO's certification can be assessed by the Commission for a fee to confirm if the individual is suitable to perform the duties outlined in the Act, especially in ensuring the protection of data subjects' rights at an organisational level.

14. Data Privacy Impact Assessment (DPIA)

A DPIA is mandatory when personal data processing involves significant privacy risks. This includes profiling, automated decision-making, systematic monitoring, or handling sensitive data or data of vulnerable individuals. A DPIA is also required when deploying new technologies, developing communication software, or offering services such as financial, healthcare, e-commerce, education, and hospitality. It applies to the use of surveillance in public spaces, cross-border data transfers, and the creation of legal instruments or policies that involve the processing of personal data of the general public. For example, deployment of Emerging Technologies (ET) such as Artificial Intelligence (AI), Internet of Things (IoT) and blockchain should be preceded by DPIA.

A DPIA exercise must include measures to ensure privacy by design and default, address proactive risk mitigation, privacy-enhancing features, security, and transparency. The DPIA must be submitted before data processing starts or within six months of when processing began before the NDPA and GAID were issued. DPIA report must be vetted by an accredited DPO and shall be part of the audit report filed with the Commission. Failure to conduct a DPIA may result in platform restrictions for the data controller or processor.

15. Exercise of Right to Lodge a Complaint with the Commission

GAID provides that data subjects have a right to lodge complaint or seek redress in furtherance of the right to privacy in the Constitution and the NDPA at the Federal or State High Court through the Fundamental Rights Enforcement Procedure Rules ("**FREP Rules**").

Data subjects may also file complaints with the NDPC, who will carry out a preliminary investigation of the complaint. Where it is convinced through a preliminary evaluation that there has been a violation of the NDPA, the NDPC will open a case file and serve a notice of investigation on the data controller or data processor. The respondent is expected to respond to the complaint within twenty-one (21) days. The NDPC may conduct a Pre-Action Conference to examine the facts and available evidence provided by the parties or obtained by the NDPC through investigations. Where the NDPC has determined that there is a violation of the NDPA, it shall direct remedial action to be taken by the respondent and communicate its decision within seven (7) days.

16. Standard Notice to Address Grievance

The GAID introduces the Standard Notice to Address Grievance ("**SNAG**") for data subjects to file complaints to data controllers or processors. A SNAG may be issued by a data subject upon a reasonable belief that a data controller or data processor has violated that data subject's right to privacy. Issuing SNAG is not a condition for lodging a direct complaint with the NDPC or for instituting an action. It is a standardized template for demanding internal remediation from an organization that may be acting in violation of a data subject's rights. The NDPC can monitor the complaint and institute an investigation where a complaint appears to be unresolved.

17. Legitimate Interest Assessment

In adopting legitimate interest as a lawful basis for processing data, data controllers and data processors are expected to conduct a Legitimate Interest Assessment. A template assessment tool has been provided for data controllers and data processors to adopt

18. Cross-Border Data Transfer

Since the NDPR and the NDPR Implementation Framework will cease to be applicable from September 14, 2025, the NDPA and the GAID provide guidance for cross-border data transfers. The bases for cross-border data transfer are:

a. Adequacy decision by the NDPC
b. Cross-border data transfer instrument approved by the NDPC; and
c. Other lawful bases.

The Commission may recognize a country as providing adequate data protection if it meets key criteria under the NDPA. These include enforceable data subject rights supported by fair judicial or administrative processes, the existence of binding data protection laws that are not subject to arbitrary changes, and a competent and independent supervisory authority with real enforcement powers. Adequacy may further depend on any agreement between the Commission and a competent regulatory authority in the recipient jurisdictions for mutual assistance on enforcement and investigations. The international obligations and commitments of the recipient's country is also considered in assessing adequacy.

In the absence of an adequacy decision, the Commission may approve Cross-Border Data Transfer Instruments (CBDTI) such as codes of conduct, certifications, binding corporate rules, or standard contractual clauses.

19. Data Subject's Vulnerability Indexes (DSVI)

Data controllers and processors must consider a data subject's vulnerability index when designing and implementing technical and organisational measures. This index refers to specific risk factors, such as age, health, financial hardship, physical disability, limited education, lack of digital literacy, or restricted access to data security support, that may make certain individuals or groups more susceptible to harm from data processing. Failing to account for these vulnerabilities could result in unfair processing or a breach of the duty of care. Consideration of these factors is required both before and during the processing of personal data.

DISCLAIMER

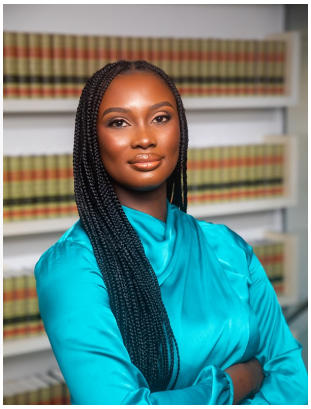
The analysis above highlights general provisions of the GAID and is not intended as a substitute for tailored legal advice. The Data Protection Team at Banwo & Ighodalo stands ready to offer expert legal guidance whenever needed. Kindly contact us at DPT@banwo-ighodalo.com.

CONTACT

Olumide Osundolire

Partner

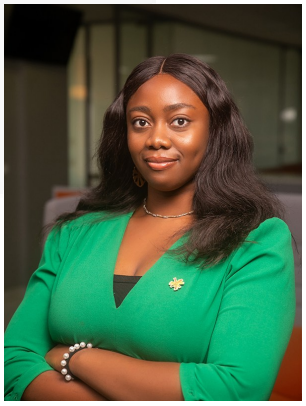
E: Oosundolire@banwoighodalo.com



Ada Aguocha

Senior Associate

E: Aaguocha@banwoighodalo.com



Vanessa Obi

Associate

E: VObi@banwo-ighodalo.com

Abosede Hassan

Associate

E: Ahassan@banwo-ighodalo.com