GREENAGE ATTORNEYS LLP

NAVIGATING DATA PRIVACY COMPLIANCE:

THE IMPLEMENTATION OF THE NDP ACT GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (GAID) 2025 AND THE PROSPECTS FOR DATA CONTROLLERS

INTRODUCTION

In compliance with the Nigeria Data Protection Act (NDPA) 2023, the Nigeria Data Protection Commission (NDPC) formally implemented the General Application and Implementation Directive (GAID) 2025 on September 19, 2025. The GAID provides operationalized guidance for the Act's enforcement and explains the responsibilities and compliance protocols for data controllers and processors. With the adoption of this directive, Nigeria has made significant progress toward becoming a jurisdiction with a robust data protection framework that complies with international best practices.

GAID increases the risks of non-compliance, adds new requirements, and tightens oversight, especially for industries handling significant amounts of private or sensitive data. This article provides a summary of GAID's goals, examines the implementation framework, and explores specific prospects for data controllers with particular focus in the banking, healthcare, and telecom sectors.

UNDERSTANDING GAID 2025 FRAMEWORK

With the power provided by the NDPA 2023, GAID functions as a directive. By releasing sector-neutral mandates and compliance resources, it aims to operationalise the Act's general provisions. Key objectives of the GAID 2025 include:

1. Clarification of Data Subjects' Rights:

The rights of data subjects under the NDPA 2023 are strengthened and operationalized by the GAID 2025, which provides clear guidelines for their implementation. These rights are outlined in NDPA Sections 34 and 36-37 and include the following: access to personal data, correction of errors, deletion of data when it is no longer required or legally processed, limitation of processing during disputes, and the ability to object to processing, including direct marketing. To ensure that these rights are not only theoretically but also practically enforceable, GAID requires controllers to create mechanisms that are transparent, accessible, and timely, such as customer portals, opt-out systems, and unambiguous rectification protocols.

2. Lawful Processing and Governing Principles:

Section 24 of the NDPA 2023, which mandates that data be processed in a fair, transparent, and lawful manner, is strengthened by the GAID 2025. It emphasises important concepts like gathering data only for precise and well-defined purposes (purpose limitation), minimising data, making sure information is correct and current, storing data for as little time as necessary (storage limitation), and safeguarding it with robust security measures to preserve confidentiality and integrity. These guidelines establish the norm for how businesses must manage personal data.

Crucially, GAID also explains how legitimate interest can be used as a legal justification for data processing. Businesses can only depend on it if their operations do not conflict with individuals' right to privacy. For instance, In **Banking and Financial Services**, banks can justify fraud detection systems or anti-money laundering monitoring under legitimate interest, provided safeguards are in place to avoid discriminatory profiling. In **Healthcare**, legitimate interest may allow limited use of patient data for research or hospital administration, but always under conditions that prioritize confidentiality and patient consent.In this way, GAID ensures that individual rights are upheld while granting organisations flexibility.

3. Accountability, Governance, and Oversight:

By requiring organisations to demonstrate their adherence to data protection regulations, the GAID 2025 enhances accountability. Data Protection Impact Assessments (DPIAs) are now necessary for high-risk operations like processing telecom subscriber data, handling sensitive medical records, and profiling financial transactions[1] This guarantees that hazards are identified and minimized before damage happens. Companies that handle sensitive data or large amounts of data must also register with the NDPC as Data Controllers or Processors of Major Importance so that the regulator can keep a closer eye on them.

In practical terms, this implies that a telecom provider implementing new AI-powered call monitoring needs to evaluate privacy concerns prior to implementation. Banks and fintech companies that perform extensive credit scoring are required to register with the NDPC and demonstrate adherence to risk mitigation measures. A Data Protection Officer (DPO) must be appointed by a healthcare provider digitising patient records in order to maintain compliance, train employees, and serve as a liaison between patients and regulators. Because of these actions, data protection is now a daily duty in many important industries rather than merely a legal requirement.

4. Emerging Technologies & Cross-Border Data Transfers:

The GAID 2025 acknowledges that big data, cloud computing, and artificial intelligence are transforming how businesses gather and utilise personal data. In order to prevent innovation from compromising privacy, the directive mandates that organisations implement robust safeguards when utilising these technologies. It also establishes guidelines for data sharing outside of Nigeria, permitting transfers only in cases where the recipient nation or organisation can ensure a degree of protection comparable to Nigeria's requirements under the NDPA. For instance, a hospital sharing patient data with foreign specialists or a Nigerian fintech using an international cloud service must first make sure the data is safe, that legal agreements are in place, and that people's rights are upheld.

5. Enforcement, Remediation and Compliance Audits:

The Nigeria Data Protection Commission (NDPC) has more authority under GAID

1 https://lawcarenigeria.com/nigeria-data-protection-act-2023

2 Article 16 & 23 of GAID

2025 to make sure businesses abide by the law. This includes having the authority to conduct compliance audits, look into complaints, and penalise companies that don't fulfil their responsibilities. Crucially, the directive also encourages remediation, pushing organisations to strengthen their systems and fix errors before being subject to harsher penalties. A bank that handles customer data improperly, for instance, might first have to retrain employees and improve its security procedures; however, repeated or significant breaches might result in steep fines. By finding a balance between education and enforcement, this strategy holds organisations accountable while assisting them in improving.

DATA CONTROLLER OR PROCESSOR COMPLIANCE REQUIREMENTS

1. Registration as a Data Controller or Processor of Major Importance (DCPMIs):

Organizations handling large volumes of sensitive data such as processing personal data of over two-hundred (200) data subjects, or processes personal data as an institution or service provider in certain sectors like finance, healthcare, insurance, and telecoms, must register with the Nigeria Data Protection Commission (NDPC). These are classified as Data Controllers or Processors of Major Importance (DCPMIs). Following this registration, they are required to pay registration fee depending on the class of DCPMI they fall under. Based on the categorization under the GAID; Ultra-High level Controllers are required to pay N250,000, Extra-High Level Controllers are required to pay N100,000 while Ordinary-High Level Controllers are required to pay N10,000.

2. Designation of a Data Protection Officer (DPO):

The GAID makes the role of a Data Protection Officer (DPO) significant to data protection compliance. This DPO as designated ensures that institutions regarded as Data Controllers or Processors comply with NDPA and GAID. The role of DPO is one of enormous dimensions within any organization as they are charged with the responsibility of overseeing all data processing activities in which the organization is engaged, thus ensuring that they are fully compliant with the law. Section 32 of the NDPA mandates that all DCPMIs must appoint a DPO (whether a staff or external individual) who advices the organization on data protection compliance, coordinate data breach responses and acts as a liaison between the stakeholders and NDPC. However, appointment of DPO for non-DCPMIs is optional.

The GAID 2025 provides that upon appointment of a DPO, the organization shall provide the DPO with the following:

- Access to all Data processing activities of the organization
- Adequate resources required by the DPO to carry out their responsibilities ranging from the financial budget to technical infrastructure to ease compliance requirements
- The independent judgment of the DPO should be adopted by the organization thus providing them with a neutral work environment
- Engage the DPO in continuous training to enable them broaden their expertise and skills to effectively discharge their duties.
- Avoid conflict of interest with the DPO irrespective of the mode of appointment.

3 https://www.mondaq.com/nigeria/data-protection/1366934/the-nigerias-data-protection-act-2023-a-look-at-key-provisions
4 Article 28 of GAID

3. Data Privacy Impact Assessments (DPIA):

High-risk processing activities, such as those involving sensitive data or emerging technologies like AI, must undergo DPIAs as required under the GAID.

These assessments evaluate potential risks to data subjects and ensure that privacy by design principles are integrated into data processing practices.

4. Cross-Border Data Transfer Mechanisms and Safeguards:

Transfers of personal data outside Nigeria require specific safeguards, including adequacy decisions (where a foreign country provides equivalent data protection), standard contractual clauses, or other approved mechanisms. This aims to protect data integrity and privacy during international data flows.

5. Compliance Audit Returns (CAR) Filing:

Organizations classified as DCPMIs must conduct risk-based compliance audits and submit Compliance Audit Returns (CARs) annually by March 31. These reports are filed through licensed Data Protection Compliance Organizations (DPCOs), failure to comply or late submission attracts penalties.

The GAID stipulates strict enforcement, including penalties for non-compliance, such as fines and sanctions. Enforcement includes compliance audits, penalties for late filing of reports (up to 50% of the original fee), and potential suspension or revocation of registration for persistent violations. For instance in July 2025, a company amongst others was fined N766 million for privacy violations and illegal cross-border data transfers against NDPA provisions.

[1] Article 28 GAID

[1] https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.PDF

[1] https://www.dataguidance.com/news/nigeria-ndpc-fines-multichoice-nigeria-ngn-766m

[5] Article 10 of GAID

[6] Article 9 GAID

[7] https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf
Article 11 GAID

IMPLICATION ON TARGETED SECTORS (TELECOM, BANKFIN, AND HEALTHCARE)

1. Telecommunications Sector:

Telecommunications operators in Nigeria process vast quantities of subscriber data daily, including personal information, geolocation information, call records, and increasingly, financial transaction data through mobile money services. The sector's data-intensive nature places it at the forefront of GAID implementation challenges. For high-risk services like automated profiling, behavioural analytics, and location tracking, Data Protection Impact Assessments (DPIAs) are now necessary. GAID also requires cross-border data transfers to adhere to adequacy standards and documented safeguards, with penalties for noncompliance, since many telecoms depend on global cloud services. Prospects include increased cost (infrastructure, staff, compliance), but also improved credibility, reduced risk of regulatory fines, and alignment with international partners for roaming, data sharing, etc.

In order to monitor compliance, control third-party processors, and implement moral principles in new services like AI-powered customer service or targeted advertising, telecoms must also engage the services of a designated Data Protection Officer (DPO) and establish internal governance frameworks. Lastly, the rights of the customer come first: subscribers must be able to access, update, or remove their data, refuse direct marketing, and comprehend automated system decisions. These steps are intended to lower risks, foster trust, and bring telecom operations into line with international best practices.

2. Banking & Financial Services (BankFin):

Nigeria's financial services sector has undergone rapid digitalization, with fintech innovations, agency banking, and digital lending platforms proliferating. This sector handles highly sensitive financial and personal data, making it a priority area for data protection enforcement. Following this, high-risk operations like automated loan approvals, fraud detection, and credit scoring, banks, fintechs, and other financial institutions must now perform DPIAs and file Compliance Audit Returns (CARs) annually with the Commission. GAID enforces stringent requirements for cross-border data transfers, requiring legal protections and evidence of sufficient protection standards, because many of these services involve data sharing with cloud providers and international payment networks. In line with the implementation and enforcement of GAID 2025, the NDPC on August 25, 2025 issued a compliance notice targeted to companies including financial institutions giving them three weeks to prove their compliance with NDPA otherwise face consequences for noncompliance.

Financial Institutions must designate DPOs, keep an eye on outside service providers like payment processors, and uphold transparent governance frameworks in order to increase accountability. Stronger rights are also granted to customers, who must be able to correct data errors, challenge automated financial decisions (like credit approvals), and object to unsolicited marketing. GAID ensures more equitable decision-making, protects consumers from financial harm, and increases public confidence in fintech innovation and digital banking by implementing these measures.

8 Article 28 GAID
9 https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.PDF
10 https://www.dataguidance.com/news/nigeria-ndpc-fines-multichoice-nigeria-ngn-766m

3. Healthcare Sector

Medical records, test results, and treatment histories are among the most sensitive types of personal data handled by healthcare organisations, such as hospitals, insurers, and digital health providers. Before digitising patient records, implementing AI-based diagnostic tools, or embracing electronic health platforms, this sector must carry out DPIAs and put strong security measures in place in accordance with GAID 2025. Due to the prevalence of cross-border medical data sharing in research and specialist consultations, GAID requires that these transfers adhere to adequacy standards and be supported by robust legal agreements.

Additionally, the directive highlights the critical role DPOs play in healthcare by guaranteeing patient engagement, staff training, and compliance. Most significantly, patients are granted more control over their data: they must have the ability to view their medical records, ask for changes, or restrict the sharing of their information. For instance, a hospital that uses AI to forecast health risks needs to inform patients about the procedure and provide them with opt-out options. In addition to safeguarding patient privacy, these regulations boost trust in digital health services and promote safe innovation in the field.

ENFORCEMENT, COMPLIANCE COSTS, AND STRATEGIC ADVANTAGES FOR THESE SECTORS

- *Data controllers are subject to more stringent regulatory oversight under GAID 2025. Now, the Nigeria Data Protection Commission (NDPC) has the authority to conduct audits, look into complaints, and impose penalties or corrective measures. The severity of the breach, the organization's size, and the number of impacted individuals determine the penalties, so both big telecom companies and smaller fintechs are held responsible.*
- *Operational expenses associated with compliance include hiring Data Protection Officers (DPOs), purchasing secure IT systems, conducting routine audits, educating employees, and securing legal counsel. These expenses, though, ought to be viewed as investments. In addition to lowering the possibility of penalties and data breaches, they also improve consumer confidence and safeguard a company's reputation—two things that are particularly crucial in delicate industries like healthcare and finance.*
- *GAID also gives data controllers new opportunities. Since their procedures will already be in line with international data protection standards, organisations developed to GAID standards may find it simpler to grow into cross-border business, international research collaborations, fintech services, or telehealth solutions. Additionally, ethical and transparent data management can help businesses stand out in the eyes of customers, making them a crucial differentiator in a crowded market.*
- *The greatest benefits will accrue to early adopters of these compliance frameworks. Organisations can lower risks and establish themselves as industry leaders by incorporating GAID principles into their operations right away. These trailblazers have the power to establish standards that others will adhere to, impact*

11 https://techcabal.com/2025/08/26/techcabal-daily-ndpc-plays-hardball/

future regulations, and mould industry best practices.

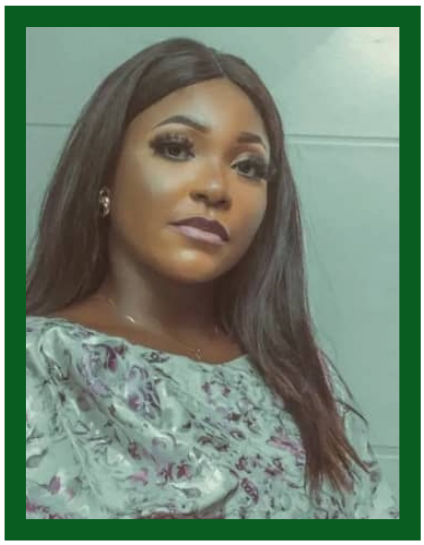
In this sense, GAID transforms compliance into a strategic advantage rather than merely a legal necessity. Data controllers in Nigeria can protect people's rights in the digital economy while simultaneously gaining access to new markets, long-term growth, and credibility by adhering to international best practices.

CONCLUSION

GAID 2025 represents a shift towards proactive data governance, emphasizing transparency, accountability, and risk management for data controllers. With the introduction of compliance audits and DPO reporting, the Commission signals increased regulatory vigilance. The extraterritorial reach compels Nigerian and foreign data controllers alike to adhere to stringent safeguards, driving harmonization with international data protection regimes. Challenges persist, notably the capacity gaps within organizations to fulfill heightened obligations and the need for sector-specific compliance frameworks. Successful implementation demands collaborative stakeholder engagement, continuous capacity building, and adoption of technology-enabled data protection solutions.

Contributors:

Author:
Stella Christian Esq



Co-Author
Jennifer Elekwe

HSE 2, Oniru Resttl. Estate Palace Road Victoria Island Lagos.

07065333142, 08063867491
greenageattorney@gmail.com