Review of the NDPA General Application and Implementation Directive (GAID) 2025

April 2025

Introduction

On 20 March 2025, the Nigeria Data Protection Commission published the General Application and Implementation Directive (GAID) 2025 of the Nigeria Data Protection Act (NDPA) 2023. The GAID serves as an instrument to aid the implementation of the Act by providing practical guidance and detailed directives for data controllers and data processors to ensure compliance with the Act.

The GAID comprises fifty-two (52) Articles and ten (10) Schedules, which expand on the data protection framework established by the Act. The GAID defines additional specific requirements, offering more granular interpretations and practical considerations of the Act's implementation.

Our review highlights the key focus areas of the GAID, summarizing new provisions introduced into the data privacy framework while also examining the implications for organisations. Additionally, we have provided our perspectives on certain aspects of the GAID, particularly where data controllers and processors may need to pay close attention. Given the heightened regulatory expectations and enforcement mechanisms, organisations must take a proactive approach in evaluating their data protection strategies to avoid non-compliance risks, reputational damage, and legal penalties.

Based on the NDPC's communication to DPCOs (ISSUE #2, March 2025 Edition of the NDPC Highlights), the GAID will take effect from **19 September 2025.**

The GAID Scope and Applicability

- **Expansion of the Scope of the NDPA**

While the NDPA previously applied to non-resident entities processing the personal data of individuals in Nigeria, Article 1(2) of the GAID expands this by clarifying that it also applies to foreign entities that intentionally "target" Nigerian data subjects, such as through targeted marketing. Additionally, the GAID provides additional categories of data subjects covered by the NDPA:

- Any data subject within Nigeria, regardless of nationality or migration status.
- Any data subject whose personal data is transferred to Nigeria,
- Any data subject whose data is in transit through Nigeria, though in this case, the responsibility of the data controller or processor is limited to ensuring confidentiality, integrity, and availability of the data.
- Any Nigerian citizen outside Nigeria. *See Articles 1(3) & 1(4) of the GAID.*

- **Clarity on what 'Operating in Nigeria' implies for DCPMIs**

Article 8(2) of the GAID provides an important clarification on what constitutes "operating in Nigeria" under Section 65 of the NDPA, which defines a data controller or processor of major importance. Under the new guidance, an entity will be deemed "operating in Nigeria" even without physical presence—so long as it targets data subjects within the country. This aligns with Sections 2(2)(a), 24(3) and 44 of the NDPA, which emphasize the need to hold accountable any entity whose data processing activities significantly impact Nigeria's economy, society, or security.

- **Repeal of the NDPR: Transition to a New Regulatory Framework**

The GAID officially repeals the Nigeria Data Protection Regulation (NDPR) as a legal instrument for data protection in Nigeria. However, this repeal does not invalidate any compliance actions, decisions, or obligations undertaken under the NDPR before the GAID takes effect, ensuring a smooth regulatory transition. *See Article 3 of the GAID.*

- **Applicability of Exemptions Under the NDPA**

Section 3 of the Act outlines specific situations where the Act does not apply, such as when personal data is processed solely for personal or household use (provided it doesn't violate privacy rights), or when data is processed by competent authorities for criminal justice, public health emergencies, national security, journalism, or for legal claims. However, Article 5 of the GAID clarifies that even when exemptions apply, organisations that rely on these exemptions still need to apply the applicable provisions. These provisions include the principles of personal data processing outlined in Section 24 (such as establishing a lawful basis (Section 25)), appointing a Data Protection Officer (Section 32), reporting breaches (Section 40), and upholding data subject rights (Part VI). *See Articles 5 & 6 of the GAID.*

This expansion in the scope of the NDPA strengthens Nigeria's data protection laws by aligning them with global standards like the GDPR, ensuring broader protection and stricter compliance for multinational companies. In addition, organisations such as law Enforcement Agencies, Public Health Organisations, and National Security agencies, relying on NDPA exemptions, should proceed with caution.
While certain obligations may not apply, core data protection requirements remain enforceable, and non-compliance could still expose them to regulatory scrutiny and penalties.

Update on the Annual Audit Requirement for Data Controllers and Processors

The GAID introduces new guidelines regarding the filing of Compliance Audit Returns (CAR) with the Commission. Some of these guidelines include:

- **New filing deadline**

Prior to the establishment of the GAID, the deadline for the filing of annual CAR with the Commission was 15th March. However, the GAID has now established a new filing deadline of **31st March**. Hence, data controllers and processors of major importance (Ultra High Level and Extra-High Level) must now file their CAR in line with this timeline. However, Ordinary-High Level (OHL) entities are required to renew their registration annually with the Commission and are **not required to file** annual CAR upon renewal.

In addition, the GAID also introduces a new requirement for entities established after 12 June 2023 to file their first CAR within 15 months of their establishment and subsequently file on an annual basis. *See Articles 7 & 10 of the GAID.*

- **Increased Compliance Audit Filing Fees**

Prior to the establishment of the GAID, the filing fees were based on the total number of data assets, with a simple structure of ₦10,000 for organisations processing fewer than 2,000 data subjects and ₦20,000 for those processing 2,000 or more. However, under the GAID, the fee structure has been significantly revised, introducing a tiered system based on the Data Controller and Processor of Major Importance (DCPMI) classification and the volume of data subjects processed.

Specifically, in Schedule 10 of the GAID, organisations are categorised under Ultra-High Level (UHL) and Extra-High Level (EHL) tiers with audit filing fees ranging from ₦100,000 to ₦1,000,000, depending on the number of data subjects handled. In addition, where a data controller or data processor fails to file its CAR as and when due, it shall pay, in addition to the stipulated filing fee, an administrative penalty, which shall be 50% of the stipulated CAR filing fee.

Based on the NDPC's communication to DPCOs (ISSUE #2, March 2025 Edition of the NDPC Highlights), implementation of the new audit filing fees begins with next year's (2026) audit cycle.

- **New template for filing CARs**

The GAID introduces a new template for filing NDPA CARs. DCPMIs (i.e., UHL and EHL) are now required to file CAR annually, based on the template provided in Schedule 2 of the GAID or as prescribed by the Commission. Unlike the previous checklist with 66 questions, the new template comprises 41 questions across 5 parts, with 16 of those questions being multiple choice, while the others require Yes/No responses.

- **Data Processing Fees for MDP-UHL**

Under Schedule 7(6) of the GAID, the Commission prescribes fees payable by data controllers and processors based on their data processing activities. A data controller of major importance in the MDP-UHL category must pay ₦5,000 as a data processing activities fee for each processor it engages, valid for 12 months. In addition, if a data controller transfers its processing activity from one processor to another within 12 calendar months, it does not need to pay a new fee for the new processor.

Organisations must take immediate steps to align with the GAID's updated Compliance Audit Return (CAR) requirements, as failure to meet new deadlines, registration mandates, or compliance audit obligations could result in regulatory scrutiny, financial penalties, and reputational risks. Organisations need to also review their privacy compliance budget to accommodate the significant increase in filing fee which may impact audit fees going forward.

New Requirements for Data Protection Officers

The GAID introduces new comprehensive provisions governing Data Protection Officers, establishing clearer obligations for Data Controllers and Processors in their DPO appointments, qualifications, and functions. Some of which include:

- **Position of the Data Protection Officer**

Article 12 of the GAID significantly strengthens the role of and protections for DPOs. It mandates that data controllers and processors implement specific organisational measures to properly support their DPOs, including providing adequate resources, unfettered access to all data processing activities, and ongoing professional training. Importantly, the provision safeguards DPO independence by prohibiting any form of coercion, undue influence, or retaliatory actions against DPOs for performing their duties. The GAID further expands DPO responsibilities by establishing them as direct points of contact for data subjects exercising their rights under the NDPA, while simultaneously imposing strict confidentiality obligations on DPOs. Notably, the GAID permits DPOs to assume additional roles, provided controllers and processors actively prevent any potential conflicts of interest that might compromise data protection responsibilities.

- **Submission of Internal Semi-Annual Data Protection Report by a Data Protection Officer**

Article 13 of the GAID includes a new requirement for DPOs to prepare and submit a semi-annual data protection report to their management. During compliance audits, the report is expected to be verified by a Data Protection Compliance Organisation (DPCO). The GAID highlights thirteen (13) areas for consideration in preparing the semi-annual report, and these include the Assessment of privacy notices and lawful bases for processing, Data types and data protection principles

applied, Need for Data Protection Impact Assessments (DPIAs) and Legitimate Interest Assessments (LIAs), among others.

- **Credential Assessment of a Data Protection Officer**

The GAID outlines in Article 14, a new provision for an Annual Credential Assessment (ACA) to be performed by the Commission to assess the proficiency of DPOs in carrying out data protection responsibilities, including a requirement for DPOs to attain a minimum of 40 CPD training hours annually. The assessment of the DPO will be based on the metrics provided in Schedule 3 of the GAID, and the DPO's credential verification will be undertaken by the NDPC, subject to the payment of the appropriate fees.

To ensure compliance and mitigate regulatory risks, organisations must empower their DPO with the necessary authority, resources, and independence. The DPO should also have a capacity-building plan to track and stay compliant with credential assessments and reporting obligations under GAID. Additionally, an annual compliance calendar with key activities and timelines, including the semi-annual audit, is essential for effective tracking and monitoring of compliance.

Clarification on Privacy Policy and Data Retention

According to Article 27 of the GAID, Data controllers and processors must provide clear, accessible, and understandable privacy information to all data subjects, including vulnerable individuals. When standard privacy policies are ineffective, such as when target data subjects are individuals who have low literacy levels, disabilities, or who speak different languages, alternative communication methods or tailored approaches should be used. This means organisations should consider using flexible delivery options such as simplified language, audio-visual content, infographics, or translated materials. Additionally, the GAID mandates that privacy policies explicitly disclose third-party access, the purpose of such access, and contact details for internal redress mechanisms. It is also important to note that the provision of a privacy policy does not constitute obtaining data subject's consent to data processing. Where consent is legally required, it must be explicitly requested.

- **Publication of Privacy and Cookie Notices**

The GAID introduces stricter requirements for data controllers and processors regarding the display of privacy and cookie notices on their websites. It mandates that these notices must be prominently published on the homepage of their website, ensuring that data subjects have a clear option to accept or decline cookies. To enhance visibility, the GAID specifies that cookie notices should significantly obstruct either the middle, left, or right side of the homepage. Placing them at the bottom of a webpage, where they may go unnoticed, could be deemed a lack of transparency in data processing - *See Article 7 and 19*.

- **Use It, Need It, or Delete It - NDPA's Data Retention Rules**

Personal data must be deleted within six months once its original purpose is complete, unless there is a legal justification for retaining it (Article 49(3)). Data controllers may retain data beyond this period if necessary for legal claims or due diligence, provided appropriate security measures are in place (Article 49(4)). Additionally, if a contract with a data subject does not materialise, any related personal data must be destroyed within six months unless retained for legal claims (Article 21(2)).

Organisations need to be more intentional in developing privacy policies, by paying attention to the target categories of data subjects. Hence, privacy policies need to be worded in a way that the data subjects can understand, bearing in mind any applicable vulnerable groups, as highlighted in Schedule 6 of the GAID.
In addition, the acknowledgment of a privacy policy by the data subject should not be mistaken for consent, as explicit consent is required for specific processing activities where necessary.

Clarifications on Consent

The GAID underscores the importance of informed consent for data processing and recommends exploring alternative lawful bases if consent would undermine the rule of law. The Commission will assess factors like security, public welfare, and proportionality in determining whether consent was properly obtained.

- **Constructive or Implied Consent**

Constructive or implied consent is permitted only in two cases:

- When images are taken at public events for reporting purposes (i.e., not for commercial use without explicit consent). In this case, data controllers must ensure that images do not portray individuals negatively and also inform participants about potential usage.
- When a user closes a prominently displayed website privacy notice, implying consent for data processing necessary for basic functionalities.

- **Cookie Consent**

The GAID introduces extensive provisions on the use of Cookies and other tracking technologies. It provides that the use of cookies and tracking tools on websites must comply with Section 24 of the NDPA, ensuring a balance between the need for tracking technologies and the right to data privacy. Data controllers/processors are required to display a cookie banner in a manner that is conspicuous and obvious to a user or site visitor. Necessary cookies, which do not process sensitive data, financial data or any data stored privately by a data subject, do not need the ticking of a box or similar methods for explicit consent. However, all other cookies must have a specific selection of "yes" or "no," "accept" or "reject" options presented to data subjects. *See Article 19(1)-(6) of the GAID.*

Organisations must carefully document their lawful basis for data processing. If consent is relied upon, then it is a must to implement clear consent mechanisms and management processes.
Organisations also have the responsibility to implement cookie consent mechanisms. Simply closing the cookie banner does not automatically constitute valid consent; consent must be explicitly obtained for tracking, marketing, and other non-essential cookies.

Clarifications on other Lawful Basis

- **Contract**

The GAID introduces additional requirements for data controllers and processors relying on contractual agreements as a lawful basis for processing personal data. Key provisions include:

- **Due Diligence Processing –** At the initial stage of a contract with a data subject, data controllers may process a data subject's personal data for due diligence purposes.
- **Data Retention for Unmaterialized Contracts –** If the contract does not materialize, any collected personal data must be deleted **within six months**, unless a legitimate reason exists to retain it for future legal claims.
- **Early Termination Clause –** Contracts involving data processing must include provisions that allow for termination before the contract's full tenure.
- **Jurisdiction Clause:** Any contract term that attempts to exclude Nigerian courts or the NDP Commission's jurisdiction is void.
- **Alternative Dispute Resolution (ADR) –** Contracts on personal data processing between a data controller/processor and data subject may incorporate ADR mechanisms to resolve disputes, subject to the inherent authority of competent courts.

- **Legitimate Interest**

The GAID in Article 26 has created a stringent rule for organisations to consider before relying on legitimate interest as a lawful basis for a processing activity. Data controllers must thoroughly assess the use of legitimate interest as a legal basis for data processing, ensuring compliance with privacy standards, transparency, ethical practices, and safeguards to protect data subjects' rights by using the legitimate interest assessment template provided in Schedule 8.

- **Vital Interest**

Data controllers or processors can rely on vital interest as a legal basis for processing personal data when consent cannot be obtained and the processing is necessary to protect someone's life or livelihood. To use this basis, three conditions must be met: (1) inaction could cause harm, (2) there's a legitimate expectation that the data would be processed in such urgent cases, and (3) failing to act could be considered negligent. The processing must also be necessary and proportionate to the threat, and the data controller/processor must be able to explain and justify the processing if asked by the data subject, their representative, or an authority. *See Article 24 of the GAID.*

- **Legal Obligation**

The GAID outlines specific circumstances under which personal data can be processed on the basis of a legal obligation. Specifically, the GAID mandates that data processing should be strictly limited to the minimum requirement under a law and should not be used for a voyage of discovery into the privacy of a data subject or in circumstances of establishing a speculative claim. See Article 22(4) of the GAID.

Furthermore, the regulatory authorities enforcing the legal obligation should take into consideration any less intrusive method of processing proposed by the affected data subject, the Commission, the concerned data controller or processor, human rights advocacy groups or the media. In the instance where a data controller/ processor intends to comply with a legal obligation for the processing of personal data, Article 22(6) of the GAID suggests that data controllers or processors may consult their DPO to assess the legality, necessity, scope, and safeguards of any such data request.

In addition, such a data controller or processor may also engage the NDPC in instances where there are concerns about personal data processing in line with such legal obligation/directive.

- **Public Interest**

The GAID introduces two (2) additional conditions where public interest can be relied upon for data processing asides a public health or humanitarian emergency purposes, which include

  - Conditions where there is a clear and present danger to public safety or
  - To address extreme deprivation in the interest of the data subject, aligned with national policy goals or the Sustainable Development Goals (SDGs).

Specifically, it now permits data controllers to process personal data on this legal basis, where there is a need to address severe cases of deprivation for the benefit of the data subject. In exercising this basis, data controllers must also consider the safeguards outlined in Article 23 of the GAID, in addition to those required under the NDPA and any other relevant laws or regulatory instruments.

Furthermore, the GAID emphasizes that the method of processing deployed under this legal ground should be both necessary and proportionate, ensuring that the rights and freedoms of data subjects are not undermined on the basis of public interest. *See Article 25 of the GAID.*

Given the additional requirements provided by the GAID across the lawful basis for processing, it is important for organisations to proactively review the current lawful basis relied upon for various personal data processing activities, by assessing each against new provisions of the GAID, and taking corrective actions. For example, this may entail performing LIAs across processing activities where legitimate interest has been identified as the appropriate lawful basis for data processing. Similarly, where vital interest is relied on as the lawful basis for processing, data controllers need to assess such for adequacy by reviewing against the three (3) key conditions prescribed by the GAID.

Rights of Data Subject

The GAID in Article 7(s-u) requires data controllers and processors to design systems and processes to make data requests and access seamless for data subjects, enable data subjects to easily correct or update their personal data, and allow them to easily transfer data to another platform or person (natural or artificial). Also, the GAID enforces both time-bound and non-time-bound obligations to protect data subjects' rights. In instances where no specific timeline requirements have been established by the NDPA, obligations must be fulfilled within a reasonable timeframe, prioritizing individuals' rights. *See Article 49 of the GAID.*

- **Right to Data Rectification**

The GAID requires that data controllers and processors ensure that the platforms used to process personal data allow for easy data rectification. In addition, where personal data rectification is required to align personal data with the data associated with the subject's National Identification Number (NIN), the provision of an affidavit or newspaper publication may not be required.

Furthermore, in the event that data rectification is necessary to correct an error made by a data controller or processor in entering a data subject's personal data, the data subject should not be required to bear any cost for correcting such error. The GAID mandates that opportunities for the data subject to verify the data before submission should be provided to reduce the probability of erroneous data being inputted by the controller in a permanent format, as the data controller will be required to prove this was the case, in the event of a dispute.

Additionally, the GAID requires all data processing platforms to be designed in a way that may allow a data controller/processor to audit any source of error. *See Article 36 of the GAID.*

- **Right to Data Portability**

The GAID provides 2 conditions upon which the right to data portability may apply, i.e.,

- When their data is provided based on consent or
- When processing is necessary for contract performance.

This right may not apply when data is processed in the performance of public duties unless denying portability infringes the data subject's rights. In addition, the right to data portability should not affect the data subject's ability to request data erasure. *See Article 37 of the GAID.*

- **Right to Lodge a Complaint with the Commission**

The GAID stipulates that the NDPC will establish an electronic platform that allows data subjects to submit complaints. Upon receiving a complaint, the Commission will acknowledge within seven days, review its applicability, and investigate if necessary. Data controllers or processors must respond within 21 days with relevant documentation if an investigation is launched.

The Commission may hold a Pre-Action Conference (PAC) to resolve the issue or summon individuals for evidence. If a violation is confirmed, the NDPC will issue directives for remedial action and communicate its decision to both parties within seven days, with the option to impose temporary protective measures if necessary.

- **Data Subject's Standard Notice to Address Grievance (SNAG)**

Article 40 of the GAID introduces the SNAG (Standard Notice to Address Grievance) as a formal mechanism for aggrieved data subjects, their representatives or civil society organisations to issue complaints to relevant controllers or processors about potential data privacy violations, while demanding remedial action. Upon receiving a SNAG, a data controller or processor would be required to communicate their decision regarding the SNAG to the Commission through the designated electronic platform that may be created by the Commission for tracking SNAGs. The Commission may take executive notice of unresolved SNAGs and initiate direct investigations. A standardized complaint template is provided in Schedule 9 of the GAID.

Organisations must ensure that data subjects are able to exercise their rights by implementing systems that support seamless data access, rectification, portability, and erasure, with rectification processes being cost-free when errors originate from the controller or processor. The GAID establishes a clear compliance mechanism for complaints and dispute resolution through the NDPC's structured frameworks to mitigate regulatory risks and uphold privacy rights. Additionally, the introduction of SNAGs is noteworthy, as this would aid internal dispute resolution of privacy related violations before regulatory escalation, reinforcing accountability and compliance.

Compliance Templates and Schedules

- **Data Privacy Impact Assessment (DPIA)**

Under the NDPR Implementation Framework, certain conditions necessitating the performance of a DPIA were outlined i.e., profiling, automated decision-making with significant effects, systematic monitoring, the processing of sensitive data, and data related to vulnerable subjects, amongst others.

However, with the repeal of the NDPR, the GAID introduces new circumstances requiring the performance of a DPIA. These include the development of communication software for data subjects, financial services processing personal data through digital devices, healthcare services, e-commerce, and even the deployment of surveillance cameras in publicly accessible spaces. Furthermore, the GAID now requires DPIAs for educational services that process student records, hospitality services, and cross-border data transfers.

In addition, Schedule 4 of the GAID provides a template for the performance of DPIAs, and the GAID establishes a requirement for DPIAs to be submitted to the NDPC as part of the annual Compliance Audit Report (CAR). This template comprises 10 sections - the lawful basis and context of processing, necessity and proportionality, consultation of stakeholders identified/potential vulnerabilities, potential disparate outcomes, amongst others.

- **Legitimate Interest Assessment (LIA)**

While legitimate interest was introduced as a 6th lawful basis in the NDPA, the GAID has provided additional requirements to guide controllers in assessing the adequacy for reliance on legitimate interest. Shedule 8 introduces a Legitimate Interest Assessment (LIA) template to help data controllers evaluate the legitimacy of their data processing under Section 25 of the NDPA. It includes three tests:

- Purpose Test (justifying processing needs and compliance),
- Necessity Test (ensuring processing is essential and no less intrusive alternatives exist), and
- Balancing Test (weighing benefits against individuals' rights).

Organisations must document results, review assessments periodically, and update privacy policies to ensure compliance.

- **Schedule for Internal Sensitisation and Training on Privacy**

The GAID in Article 30 mandates organisations to prepare and implement an organisational Schedule for internal sensitisation and training on privacy. The schedule must outline methods for evaluating compliance with the NDPA and other regulatory guidelines. To strengthen compliance efforts, organisations are also required to review their data processing platforms, assign officers for implementation, and set clear timelines for compliance actions.

Additionally, a basic privacy checklist is required to be developed to enable persons engaged in data processing to understand their responsibilities. Furthermore , the GAID introduces a timeline for Data Controllers and Processors to conduct training and awareness on data protection law and practices for its staff. It requires them to conduct these trainings at least within the six (6) months of commencement of their business and then, at a minimum, on an annual basis.

It is important for DPOs and their organisations to familiarise themselves with the new DPIA and LIA templates included in the GAID and also the execution of these assessments to ensure that high-risk data processing activities are properly evaluated, justification for certain processing activities established and adequate mitigants implemented.

Beyond the assessments, organisations must establish new schedules and templates to ensure continuous compliance monitoring. This includes creating structured plans for ongoing awareness initiatives, staff training, security compliance monitoring, amongst others.

Third Party Relationships, Cross-Border Data Transfer & Interoperability

- **Data Processing Agreement (DPA) Requirements**

While Section 29 of the NDPA establishes obligations of data controllers and processors in personal data processing, the GAID has defined specific details that should be in the data processing agreement - the identification of parties, purpose and scope of processing, location (especially for cross-border transfers), lawful basis, roles and responsibilities, etc.

Additionally, sole proprietors, agents, or self-employed individuals handling high-risk data processing must undergo formal data protection training and provide evidence of training for registration as a data processor of major importance.

- **Approval Process for Benchmarking with Interoperable Data Privacy Measures**

The GAID has made provision for instances where organisations may want to consider other data privacy measures outside of what has been established in the Act and GAID. Accordingly, where such organisations intend to benchmark their data processing with an Interoperable Data Privacy Measure (IDPM), which expressly requires directives of the Commission under the NDPA, it is required to seek the approval of the NDPC through a formal application. The application should

comprehensively detail the organisation's data processing context, including business nature, processing purposes, specific IDPM details, jurisdictional origins, ecosystem benefits, use cases, potential disadvantages, and the certified Data Protection Officer's contact information.

- **Update on Cross-border transfer**

Schedule 5 of the GAID establishes a comprehensive framework for cross-border data transfers under the NDPA, outlining three primary grounds for such data transfers as follows:

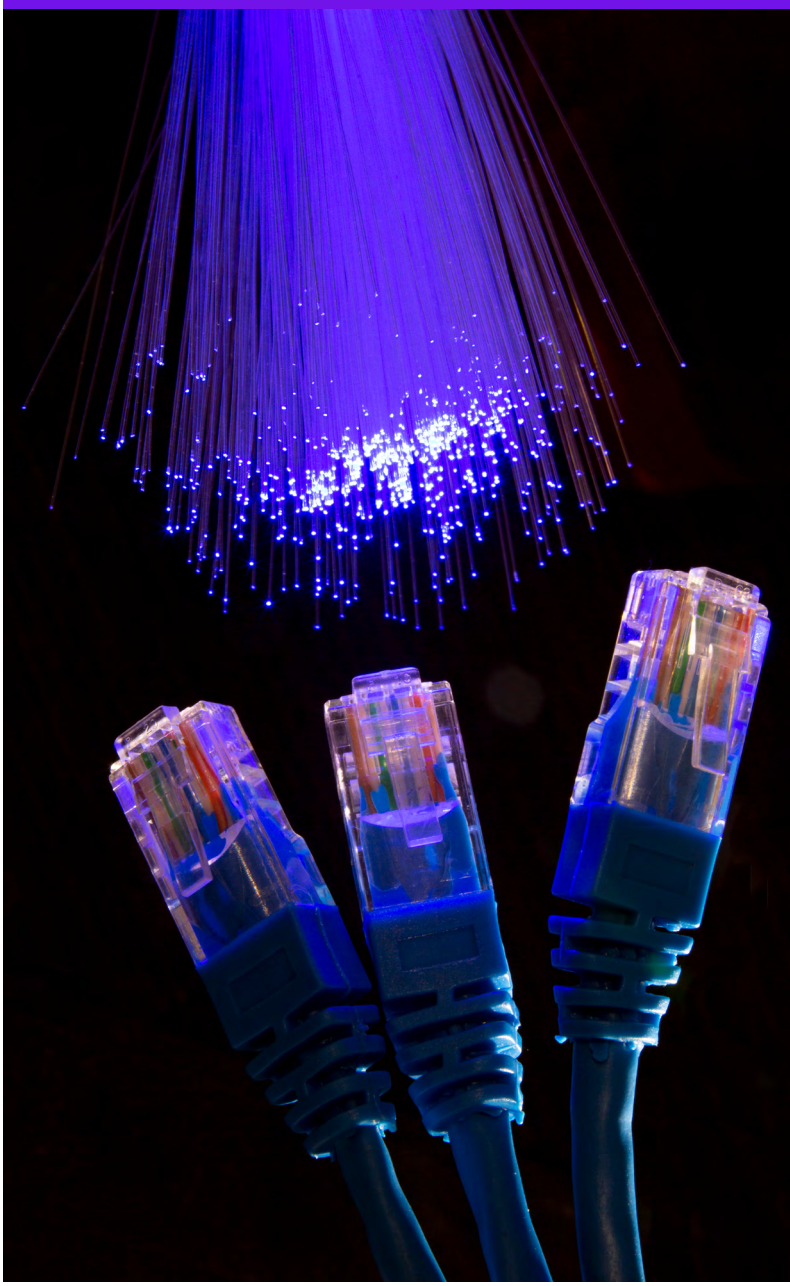
- An Adequacy Decision by the Commission recognising equivalent data protection standards in the recipient country;
- Approved Cross-Border Data Transfer Instruments (CBDTI);
- Reliance on other lawful bases.

The GAID further specifies 6 conditions where the Commission may adjudge a country as affording adequate data protection as Nigeria. These conditions include, the existence of enforceable rights for data subjects, including mechanisms that allow individuals to seek administrative or judicial redress, supported by the rule of law; the presence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection, access of a public authority to personal data; the existence of a data protection law in the recipient jurisdiction, amongst others.

In the absence of an adequacy decision, the Commission may approve Cross-Border Data Transfer Instruments (CBDTI) such as Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), codes of conduct, etc., for a data controller/processor or a group of data controllers and processors. In assessing an application for approval of a CBDTI, the Commission may take into consideration the outcome of an NDPA Compliance Audit conducted by a DPCO in relation to the data controller/processor seeking such approval. In addition, the Commission will also consider evidence demonstrating the data controller's or processor's adherence to global best practices or internationally recognised data protection standards.

Furthermore, the GAID enumerates other lawful bases for cross-border transfers, including for the defence or establishment of a legal claim, public interest, if the purpose of the transfer is for the sole benefit of the data subject, etc.

Notably, the GAID provides much-needed clarity on cross-border data transfers under the NDPA, setting out mandatory elements for data processing agreements, including parties involved, purpose, lawful basis, and transfer locations. It also requires organisations seeking Interoperable Data Privacy Measures (IDPM) to apply to the Commission for approval. Importantly, the GAID outlines three main pathways for lawful cross-border data transfers: an Adequacy Decision by the Commission, use of approved Cross-Border Data Transfer Instruments (CBDTI), or reliance on other lawful bases, reflecting Nigeria's growing alignment with global data protection standards.



Data Security, Software and Emerging Technology (ET)

- **Data security, DPIA, and other measures on ET**

Data controllers must document safeguards and submit compliance reports, including mandatory Data Protection Impact Assessments (DPIAs) to evaluate risks and vulnerabilities. ET tools must be tested in low-risk environments, anonymize data when possible, and undergo repeated retesting if risks are identified. If risks cannot be mitigated, the technology should not be used. Even after deployment, continuous monitoring is required to detect and prevent emerging privacy threats. Organisations using ETs must adhere to global standards, including United Nations resolutions on AI, other global human rights, and data ethics principles. Technologies that violate human rights or pose excessive risks must not be used.

- **Data Processing Software Deployment Measures**

Article 31 mandates data controllers/processors who have deployed or intend to deploy data processing software to track a data subject or enable a communication link with a data subject and processing his or her personal data, to comply with the following obligations: conduct a DPIA prior to deployment of the software, develop the software in accordance with privacy-by-design and privacy-by-default principles, ensure that the software follows data security guidelines or instructions provided in the stores where the software may be downloaded, insert a privacy policy in the software, and provide a privacy statement to prospective users of the software prior to installation. Furthermore, all existing software in use before the issuance of the GAID is required to be updated within six (6) months to achieve compliance with the NDPA and the GAID.

- **Schedule for Monitoring, Evaluation and Maintenance of Data Security System**

In Article 29 of the GAID, Data controllers and processors are mandated to regularly monitor, evaluate, and maintain their data security systems through scheduled activities like training, software updates, vulnerability tests, encryption reviews, and authentication checks. Security measures must be assigned to relevant officers, vetted by a certified information security officer, and conducted frequently based on risk levels to ensure data confidentiality, integrity, and availability.

Organisations must uphold ethical data practices by ensuring transparency, fairness, security, and respect for individual autonomy. Emerging Technologies (ETs) must undergo rigorous testing, including DPIAs, and align with global human rights and data ethics standards. Continuous monitoring is essential to mitigate privacy risks, and technologies posing excessive threats should not be deployed.

Conclusion

The General Application and Implementation Directive (GAID) marks a pivotal shift in Nigeria's data protection landscape, following the formal repeal of the NDPR. With this transition, Data Protection Officers (DPOs) and their organisations must prioritise a thorough understanding of the GAID's provisions, as it now serves as the principal legal instrument guiding the implementation of the NDPA.

Importantly, organisations should adopt a pragmatic approach to identifying quick wins that can be actioned immediately, such as reviewing and updating privacy notices, updating internal training schedules, etc., while also developing a longer-term strategic roadmap for other requirements towards ensuring overall compliance.

The introduction of a mandatory semi-annual audit, reporting, and stricter oversight, highlight the need for a comprehensive compliance framework that prioritizes privacy by design, ethical data processing, and continuous monitoring. Businesses that proactively integrate GAID requirements into their operations will not only mitigate risks but also enhance consumer trust and business resilience. As data protection enforcement in Nigeria intensifies, compliance with the GAID is no longer optional, it is essential for sustainable and responsible data management.

While some elements of the GAID may still require further regulatory clarification, especially in the evolving areas, organisations are encouraged to focus on what is within their control by adopting a risk-based, transparent, and accountable posture in line with the overarching principles of the NDPA.

Ultimately, proactive engagement, continuous capacity building, and timely alignment with emerging guidance from the Commission will be key to sustaining compliance and fostering trust within the ecosystem.

Further Reading

For additional information, access the GAID published by NDPC via the URL below:
https://ndpc.gov.ng/resources/#

For further information, contact:

John Anyanwu
Partner,
Cyber & Privacy
KPMG in Nigeria
T: +234 803 975 4061
E: john.anyanwu@ng.kpmg.com

Olaoluwa Agbaje
Senior Manager,
Cyber & Privacy
KPMG in Nigeria
T: +234 816 960 8200
E: Olaoluwa.Agbaje@ng.kpmg.com

Contributors

Kudirat Tobi Mustapha
Cyber & Privacy
kudirat.mustapha@ng.kpmg.com

Sandra Eke
Cyber & Privacy
sandra.eke@ng.kpmg.com

Obehi Emiowele
Cyber & Privacy
obehi.emiowele@ng.kpmg.com

Mary Adebanjo
Cyber & Privacy
mary.adebanjo@ng.kpmg.com

Abdulqudus Isa
Cyber & Privacy
abdulqudus.isa@ng.kpmg.com

Favour Akinsika
Cyber & Privacy
favour.akinsika@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia