DUALE, OVIA & ALEX-ADEDIPE

Unpacking the General Application and Implementation Directive (GAID) 2025 Series 2: Operational Compliance and Data Subject Rights

TELECOMMUNICATION, MEDIA AND TECHNOLOGY (TMT)

The second part of the General Application and Implementation Directive 2025 (**GAID**) analysis shifts focus from the foundational and institutional framework of Nigeria's data protection, established in Series 1, to the practical, operational duties required for compliance. This transition moves from examining who is involved to analysing how they must function in practice.

The Series 1 thoroughly examined the institutional framework of the GAID, including the foundational roles of the Nigeria Data Protection Commission (**NDPC**), Data Protection Officers (**DPOs**), and various sectoral regulators.

This Series 2 will address how these frameworks translate into tangible, daily compliance expectations for data controllers and processors. It underscores a fundamental principle of the Nigeria Data Protection Act (**NDPA**): Emphasizing that compliance under the GAID is an ongoing operational duty, not a one-off certification exercise.

Key Operational Duties

To meet this standard, controllers and processors must embed privacy principles deeply into their organizational structures and processes. Key requirements include:

- **Privacy by Design and Default:** Integrating data protection safeguards from the initial design of systems and services.

- **Strengthened Internal Governance:** Establishing robust internal policies, procedures, and training programs.

- **Demonstrable Accountability:** Maintaining detailed records and mechanisms to prove compliance to both the NDPC and data subjects.

This operational focus is crucial for safeguarding the rights of data subjects, which is the central purpose of the GAID, thereby establishing the practical application of the NDPA**.**

Article 15: Principles of Personal Data Protection

The GAID reaffirms the NDPA principles: fairness, lawfulness, transparency, purpose limitation, data minimisation, storage limitation, accuracy, confidentiality, accountability, and duty of care. These must be integrated across the data lifecycle, from collection to deletion, using appropriate technical and organisational measures.

Article 16: Lawful Bases of Data Processing

Controllers must establish one or more lawful bases (such as consent, contract, legal obligation, vital interest, public interest, or legitimate interest) before processing any data. This basis must align with Nigerian laws and international human-rights standards. Notably, the GAID expressly prohibits reliance on consent for activities that could propagate hate, atrocities, or violations of child rights.

Article 23: Evaluation of Lawful Bases

To ensure integrity, every lawful basis must be evaluated for necessity, proportionality, duty of care, and availability of redress. This evaluation is subject to review by regulators and adjudicators.

Articles 26–27: Transparency and Fair Processing

Controllers have an ongoing duty to provide clear, accessible, and comprehensive information to data subjects, covering the controller's identity, processing purposes, lawful bases, recipients, retention periods, and available rights. Privacy notices must be regularly updated and written in plain language.

Implications: Failure to embed the principles in internal policies, training, and security structures constitutes a breach of both the NDPA and GAID. Selecting an inappropriate or poorly documented lawful basis invalidates the processing. Controllers must document their reasoning for each choice in their Records of Processing Activities (ROPAs**)** to withstand scrutiny. Transparency is continuous; inaccurate or outdated privacy notices are a compliance failure.

Consent must be informed, explicit, and freely given. Withdrawal must be as easy as granting it, and refusal cannot disadvantage the data subject. Consent is mandatory for activities like direct marketing, processing sensitive data, handling child data, cross-border transfers without adequacy, incompatible further processing, and automated decision-making. For cookies, explicit consent is required for all non-essential types, and cookie policies must clearly disclose the controller, purpose, duration, and withdrawal methods.

Article 21: Reliance on Contract

Processing for contractual necessity is permitted, including due diligence activities. If the contract does not materialise, all personal data must be deleted within six months, unless retained for legitimate legal claims.

Article 22: Reliance on Legal Obligation

This GAID anchors the NDPA under a legal obligation (law or court order) to the constitutional right**.** Any processing must be reasonably justifiable for essential public interests (like public safety) and limited to the minimum data required. The DPO serves as an internal check, verifying the demand's competence and proportionality. The framework demands considering less intrusive methods. Finally, it provides recourse: seek guidance from the Commission against administrative orders, or approach a competent court against judicial orders.

Articles 24 & 25: Vital and Public Interest

Vital Interest applies narrowly, typically in emergencies, only when necessary to protect life or livelihood and failure to act would cause harm. Public Interest processing, permissible in areas like public-health emergencies, requires a mandatory written evaluation report balancing proportionality, risk, and alternative measures.

Implications: Consent is a demonstrable standard**.** Controllers must deploy automated

consent and cookie management tools. Contract-based processing requires automated data-deletion triggers for failed or terminated contracts to prevent unlawful retention. The DPO's role is critical in validating legal obligations. Reliance on Vital or Public Interest grounds must be evidenced by documented justification and evaluation to avoid enforcement risk.

Article 28: Data Privacy Impact Assessment (DPIA)

The GAID stressed that the DPIA is mandatory where processing poses high risks to data subjects' rights and freedoms. Existing high-risk operations must complete a DPIA within six months, and new operations must do so before commencement.

Article 29: Monitoring, Evaluation, and Maintenance of Data Security Systems

Data controllers and processors must establish a structured schedule for the continuous monitoring, evaluation, and maintenance of security systems, including personnel training, vulnerability assessments, and encryption reviews. This must be overseen and documented by a qualified information security officer.

Articles 30 & 31: Internal Sensitisation and Software Deployment

All personnel handling data must undergo routine sensitisation and training. Before deploying any tracking or processing system, controllers must conduct a DPIA and ensure the software is built with privacy-by-design and privacy-by-default.

Article 34: Data Processing Agreement (DPA)

A written DPA is mandatory for all delegated processing, detailing purposes, security controls, and accountability. Both the controller and processor share joint responsibility under the NDPA.

Article 35: Benchmarking with Interoperable Data Privacy Measures (IDPMs)

Data controllers and processors may adopt globally recognised privacy standards (IDPMs) to align with NDPA principles, but mandatory NDPC approval is required.

Implications: The DPIA requirement institutionalises accountability and privacy-by-design. Failure to conduct a DPIA can lead to operational restrictions. The GAID shifts the security approach from reactive to preventive, demanding documented evidence of continuous maintenance. Privacy protection is a shared organizational responsibility reinforced by mandatory training. Privacy must be engineered into software architecture (Privacy-by-Design), not added later. The absence or poor execution of a DPA exposes both parties to joint liability. Implementing unapproved IDPMs constitutes non-compliance.

Article 32: Measures Against Privacy Breach Abetment

Data controllers and processors have a duty of vigilance to prevent their platforms from being used for privacy violations. Upon notification from the NDPC of misuse, they must immediately suspend or restrict the offending party. Failure to act promptly is treated as abetment, attracting the same penalties as direct breaches.

Article 33: Data Breach Notification

Data controllers and processors must notify the NDPC within 72 hours of detecting a breach that threatens individual rights. Data subjects and law enforcement must also be informed where high-risk harm exists.

Articles 36–38: Core Data Subject Rights

- **Right to Rectification:** The right to correct inaccurate or incomplete data via simple channels.
- **Right to Data Portability:** The right to receive and transmit one's data to another controller, applicable when processing is based on consent or contractual necessity.
- **Right to be Forgotten:** The right to request deletion when data is no longer needed, consent is withdrawn, or processing is unlawful (subject to exceptions like legal obligations). Controllers must also ensure third parties delete the data.

Articles 39 & 40: Complaint and Grievance Mechanisms

- **Right to Lodge a Complaint:** Any data subject may file a complaint with the NDPC. The controller has 21 days to respond after notification.

Standard Notice to Address Grievance (SNAG): A voluntary, pre-complaint mechanism where a subject alerts the data controller and processor of an alleged breach. The data controller or processor must promptly investigate and document remedial action.

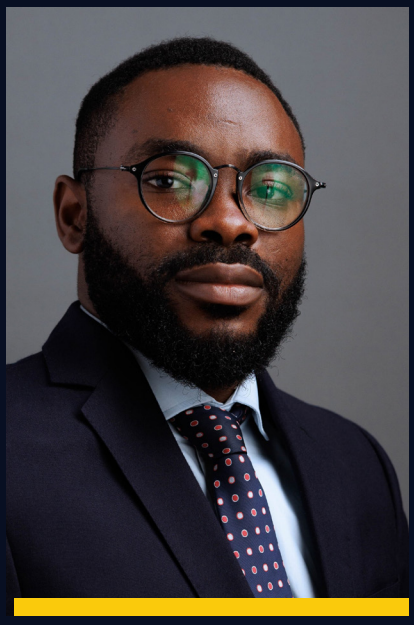
Implications: Inaction following an NDPC alert amounts to a substantive breach. Robust incident response frameworks with rapid escalation and reporting protocols are critical for the 72-hour breach notification. Organisations must build interoperable, machine-readable export systems for portability and maintain auditable deletion procedures for the Right to be Forgotten. The SNAG promotes early dispute resolution, encouraging a transparent and proactive compliance culture to avoid escalation and enforcement.

Conclusion

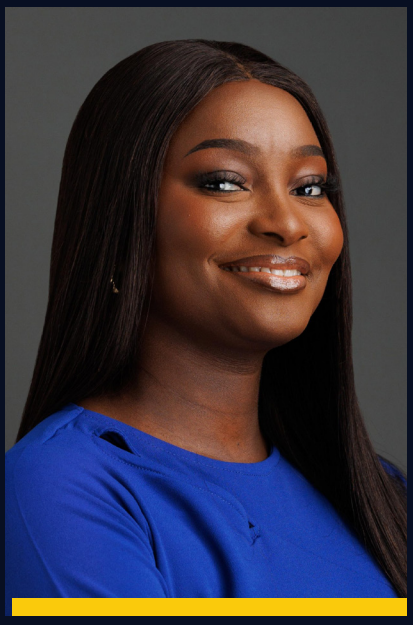
Articles 15–40 of the GAID transform the NDPA's principles into concrete, day-to-day compliance duties for data controllers and processors. They outline how organisations must manage personal data, uphold individual rights, and maintain demonstrable accountability through lawful processing, breach response, and grievance procedures. Overall, these operational rules set the practical benchmark for accountability and enforcement in Nigeria's data protection landscape. The next series will examine how the GAID governs ethics, emerging technologies, and enforcement, ensuring long-term trust and regulatory stability.

Authors

Chika Oke
Senior Associate



Jeffrey Nwalima
Associate



Kafilat Olorundare
Associate

LAGOS

Plot 1B, Block 129,
Jide Sawyerr Drive,
Lekki Phase I
Lagos State, Nigeria

ABUJA

1st Floor,
AP Plaza 100,
Adetokunbo Ademola Crescent,
Wuse 2
FCT, Nigeria

Tel.: 0700 DOALAW (0700 362529)
Email: info@doa-law.com
www.doa-law.com

DUALE, OVIA & ALEX-ADEDIPE