

NAVIGATING GAID 2025: KEY SHIFTS IN NIGERIA'S DATA PROTECTION FRAMEWORK



INTRODUCTION

The Nigeria Data Protection Act (NDP Act) 2023, augmented by the Nigeria Data Protection Act General Application and Implementation Directive (GAID) 2025, represents a significant stride in safeguarding the fundamental right to privacy and fostering a trusted digital economy in Nigeria. The GAID, issued pursuant to Section 37 of the 1999 Constitution of the Federal Republic of Nigeria and Sections 1(a), 6(c), 61 & 62 of the Nigeria Data Protection Act 2023 by the Nigeria Data Protection Commission (the Commission), serves as a crucial guide for the implementation of the NDP Act, particularly amidst the evolving landscape of disruptive technologies and personal information processing.

Notably, the GAID is set to take effect from the **19th of September 2025**, replacing the Nigeria Data Protection Regulation (NDPR) 2019 and the NDPR 2019: Implementation Framework 2020. As a result, this review highlights some of the key provisions under the GAID and their implications for businesses.

SCOPE AND APPLICATION OF THE NDP ACT AND GAID

The NDP Act, and by extension the GAID, applies to the processing of personal data, whether automated or not, where the data controller or data processor is domiciled in, resident in, or operating in Nigeria. It also applies if the data controller or processor is not domiciled or resident in Nigeria but processes the personal data of a data subject in Nigeria or targets data subjects in Nigeria. This broad territorial scope underscores Nigeria's commitment to protecting its citizens' data globally.

KEY PROVISIONS OF THE GAID

General NDP Act Compliance Measures (Article 7)

Under the NDP Act, data controllers and processors must adopt a range of compliance measures. These include registering with the Commission as a Data Controller or Data Processor of Major Importance (DCPMI), conducting annual compliance audits, and filing Compliance Audit Returns. DCPMIs must also prepare semi-annual data protection reports and designate a Data Protection Officer (DPO). Organizations are further required to maintain robust data security systems, conduct internal training on data privacy, and develop clear privacy policies and cookie notices.

Designation and Registration of DCPMI (Articles 8-9)

A Data Controller or Processor of Major Importance (DCPMI) is designated based on the scale, sensitivity, and significance of data processing in relation to Nigeria's economy, society, or security. Factors include the number of data subjects, risks to rights, data sovereignty, sensitivity, financial assets handled, reliance on third-party servers, and extent of cross-border flows. The GAID classifies DCPMIs into three levels: Ultra-High Level (UHL) for strategic sectors such as banking, telecoms, insurance, oil and gas, fintech, and payment gateways; Extra-High Level (EHL) and Ordinary-High Level (OHL) which covers government bodies, banks and schools, small industries respectively.

UHLs and EHLs are to register once and file annual Compliance Audit Returns, while OHLs must renew yearly but are exempt from annual CAR filing. The Commission maintains a public register of DCPMIs, with exemptions granted to groups such as faith-based bodies, community associations, embassies, judicial entities, and multigovernmental organizations.

Data Privacy Impact Assessment (DPIA) (Article 28)

A DPIA is mandatory when data processing is likely to result in a high risk to data subjects' rights and freedoms, especially with new technologies, large-scale processing of sensitive data, systematic monitoring, or automated decision-making with significant effects. DPIAs

must detail the processing, its purpose, necessity, proportionality, risks to data subjects, and measures to address those risks. The outcome of a DPIA forms part of the NDP Act Compliance Audit Returns (CAR). Failure to conduct a DPIA can lead to restrictions on data processing platforms.

Cross-Border Data Transfer (Article 45)

Personal data may only be transferred outside Nigeria if the recipient country ensures an adequate level of protection, meaning principles substantially aligned with the NDP Act. Adequacy is determined by factors such as enforceability of rights, legal instruments like mutual assistance treaties, limits on public authority access, effective data protection laws, an independent regulator, and international commitments. Where no adequacy decision exists, transfers may still occur under specific conditions such as informed consent of the data subject, necessity for a contract, benefit to the data subject with implied consent, important public interest grounds, legal claims, or protection of vital interests where consent is impossible.



Data Protection Officer (DPO) (Articles 11-14)

DCPMI are mandated to designate a DPO with expert knowledge of data protection law and practices. The DPO can be an employee or a consultant. Their responsibilities include advising, monitoring compliance, and acting as the contact point for the Commission. DPOs must report directly to management, operate without coercion, and not be penalized for their duties. They are required to submit internal semi-annual data protection reports to management. The Commission also conducts an Annual Credential Assessment (ACA) of

DPOs to ensure professionalism and continuous professional development.

Data Subject Rights and Redress (Articles 34–40)

The NDP Act and GAID grant individuals a wide range of rights over their personal data. These include the right to confirmation and access, rectification of inaccurate or incomplete data, erasure where processing is no longer justified, and restriction of processing in certain cases. Data subjects may also object to processing, particularly for direct marketing or profiling, and exercise data portability by receiving their information in a structured, machine-readable format to transfer elsewhere. Importantly, individuals have the right not to be subject to decisions based solely on automated processing that produce legal or significant effects, except where such processing is necessary for a contract, backed by law with safeguards, or based on valid consent.



To support enforcement of these rights, the GAID introduces the Standard Notice to Address Grievance (SNAG), which is a template enabling data subjects to seek internal remedies from organizations before escalating issues. While the SNAG encourages structured engagement, it is not mandatory for filing a complaint with the Commission, ensuring that data subjects retain direct access to regulatory redress when needed.

Consideration of Time-Bound and Non-Time-Bound Obligations (Article 49)

The overriding standard in determining whether a data controller or processor has fulfilled any obligation within a reasonable time is the protection of the data subject's constitutional rights and freedoms under Section 37 of the 1999 Constitution. Where the NDP Act or regulatory instruments do not expressly fix a timeline, obligations must still be discharged promptly, considering the urgency required to safeguard the data subject's rights and interests. For storage limitation, where no legal timeframe is specified, personal data must not be retained for more than six months after the original purpose of processing has been achieved. However, controllers may retain data beyond this period, subject to the principles of Section 24 of the NDP Act, if adequate technical and organizational safeguards are applied for purposes such as defending legal claims or conducting due diligence.

Enforcement Procedures (Articles 39-40)

The Commission is empowered to investigate complaints, issue compliance orders (warnings, requirements to comply, cease and desist orders), and enforcement orders (remedy

violation, compensation, account for profits, penalties). Penalties for major importance data controllers/processors can be up to N10,000,000 or 2% of annual gross revenue, whichever is higher, while for others, it is N2,000,000 or 2% of annual gross revenue.

Personal data breaches must be notified to the Commission within 72 hours of awareness if likely to result in high risk to data subjects, and to affected data subjects immediately.

Implications of the GAID In Nigeria

The GAID has profound implications for Nigeria's data protection landscape and its broader digital economy. By replacing the NDPR 2019 and providing detailed explanations and procedures, it introduces enhanced legal certainty and coherence to the regulatory environment. This clarity reduces ambiguity for businesses and individuals, ensuring more predictable obligations and fostering confidence in compliance practices. Central to the framework is the strengthening of data subject rights, with comprehensive provisions on rectification, portability, erasure, and the novel inclusion of SNAG. These mechanisms empower individuals with greater control over their personal data, aligning with the constitutional right to privacy and reinforcing trust in the system.

The GAID also seeks to foster a trusted digital economy by embedding accountability, security, and ethical standards into data processing. This foundation of trust is crucial for accelerating Nigeria's digital transformation and enabling its active participation in regional and global economies. Secure and reliable data flows will support vital areas such as security, migration, finance, and trade, while also opening new opportunities for digital innovation and cross-border transactions. However, the framework introduces an increased compliance burden for organizations, particularly data controllers and processors of major importance (DCPMIs). The requirements for registration, annual audits, designation of DPOs, data protection impact assessments (DPIAs), and tiered obligations for different levels of processing (UHL, EHL, OHL) will necessitate significant investment in infrastructure, expertise, and training.

At the international level, GAID's emphasis on "interoperable data privacy measures" and the assessment of adequacy in foreign jurisdictions positions Nigeria for smoother and more secure cross-border data transfers. This alignment strengthens Nigeria's global standing and could facilitate enhanced trade and collaboration with international partners. Yet, the success of GAID will hinge on effective implementation, widespread awareness, and the Commission's ability to enforce provisions across diverse sectors. Building capacity, particularly for SMEs, will be essential, while the emergence of data protection compliance organizations (DPCOs) and DPOs as key enablers presents significant opportunities for professional growth within the compliance ecosystem.

Final Thoughts

Overall, the GAID is a landmark directive that operationalizes the NDP Act, providing comprehensive guidelines for data protection in Nigeria. Evidently, its detailed provisions aim to create a secure and trustworthy environment for personal data.

Author



Kelechi Okparaocha

Kelechi@wtsblackwoodstone.com

About WTS Blackwoodstone

WTS Blackwoodstone is an international business law firm that provides innovative business solutions for clients with diverse needs. The Firm's core practice areas include Corporate and Commercial law, Tax Advisory & Compliance and Transactional Services to resident and non-resident companies doing business in Nigeria. Our practice is based in Lagos and Abuja and is strategically placed to offer hands on legal services to our clients in the major economic hubs of Nigeria and the rest of Africa.

Our clients include locally headquartered multinationals, medium and small local and international clients, family-owned businesses, government agencies and high net worth individuals.

WTS Blackwoodstone is the Nigerian network partner of WTS Global. With representation in over 100 countries, WTS Global has grown to a leadership position as a global tax practice offering the full range of tax services and aspires to become the preeminent non-audit tax practice worldwide. WTS Global embodies the core values which we as a firm base our daily actions upon – innovation, excellence, reliability, and a global mindset – thereby further strengthening our firm's offering to multi-national clients.

About WTS Global

With representation in over 100 countries, WTS Global has already grown to a leadership position as a global tax practice offering the full range of tax services and aspires to become the preeminent non-audit tax practice worldwide. WTS Global deliberately refrains from conducting

annual audits in order to avoid any conflicts of interest and to be the long-term trusted advisor for its international clients. Clients of WTS Global include multinational companies, international mid-size companies as well as private clients and family offices.

The member firms of WTS Global are carefully selected through stringent quality reviews. They are strong local players in their home market who are united by the ambition of building a truly global practice that develops the tax leaders of the future and anticipates the new digital tax world.

WTS Global effectively combines senior tax expertise from different cultures and backgrounds and offers world-class skills in advisory, in-house, regulatory and digital, coupled with the ability to think like experienced businesspeople in a constantly changing world.

For more information please see: wts.com

Imprint

WTS Blackwoodstone

Unit 12, No 8 Office Apartments, Plot 8, Rasheed Alaba Williams, Lekki, Lagos
Nigeria

T: +234 9033 501 613

www.wtsblackwoodstone.com |
info@wtsblackwoodstone.com

[Disclaimer e.g.: The above information is intended to provide general guidance with respect to the subject matter. This general guidance should not be relied on as a basis for undertaking any transaction or business decision, but rather the advice of a qualified tax consultant should be obtained based on a taxpayer's individual circumstances. Although our articles are carefully reviewed, we accept no responsibility in the event of any inaccuracy or omission. For further information please refer to the author.]

