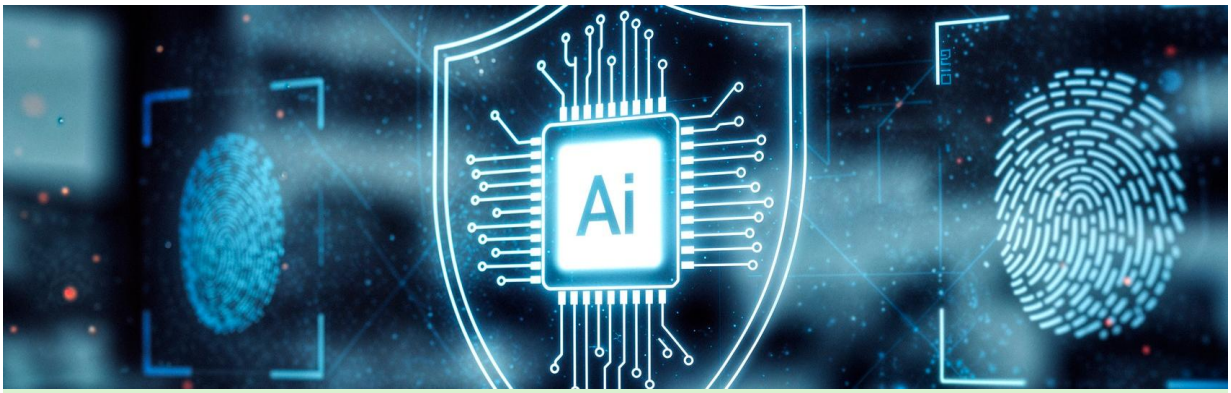
Beyond Future AI Laws: How the NDPA and GAID Already Regulate Artificial Intelligence in Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road, Lekki Phase 1, Lagos, Nigeria

16th June, 2026

Introduction



Artificial intelligence (AI) is no longer a technology of the future. Across finance, healthcare, telecommunications, education, insurance, advertising, public administration and health services, organisations are deploying credit-scoring algorithms, fraud-detection tools, automated recruitment systems, clinical decision-support models, recommendation engines, surveillance analytics and generative AI platforms as part of ordinary business operations. For technology companies, AI has moved from a product differentiator to baseline infrastructure.

As governments around the world move toward dedicated AI legislation, a common assumption within Nigeria's technology and business community is that AI remains largely unregulated in Nigeria until a standalone AI statute is enacted. That assumption is commercially and legally risky. Nigeria may not yet have a dedicated AI Act, but AI systems that process personal data, profile individuals, make or support consequential decisions, or affect the privacy rights of data subjects in Nigeria are already subject to binding obligations under Nigeria's data protection framework.

The Nigeria Data Protection Act 2023 (NDPA) and the Nigeria Data Protection Act General Application and Implementation Directive 2025 (GAID), issued by the Nigeria Data Protection Commission (NDPC), together create the current binding AI-relevant compliance framework in Nigeria. The GAID is particularly important because it expressly refers to Artificial Intelligence as an Emerging Technology where it is deployed for the processing of personal data. Upon the issuance of the GAID, the NDPC stated that it would cease to apply the Nigeria Data Protection Regulation 2019 as the legal instrument for regulating data privacy and protection, subject to transitional matters preserved under the NDPA.[1]

At the policy level, Nigeria's National Artificial Intelligence Strategy (NAIS) sets out a broader national vision for AI-led growth, competitiveness, inclusion, innovation and responsible adoption.[2] AI-specific legislative proposals, including proposals for institutional AI oversight, are also emerging. However, while those policies and legislative developments are important, the NDPA and GAID remain the binding instruments that organisations deploying AI must comply with today.

This article explains how the NDPA and GAID already regulate AI in Nigeria, the practical implications for businesses and technology stakeholders, the gaps that remain in the present framework, and why a dedicated AI law should complement rather than replace Nigeria's existing data protection-based AI governance obligations.

[1] GAID, Article 3(3); NDPA, sections 61-64.
[2] National Artificial Intelligence Strategy, September 2025: Link; Accessed 11 June 2026

Nigeria's Current AI-Relevant Regulatory Framework

Unlike the European Union, which has enacted a standalone AI Act, Nigeria currently regulates many AI risks through a combination of data protection law, sector-specific regulation, technology policy and emerging AI policy initiatives. For present compliance purposes, the NDPA and GAID are the most important binding instruments because most commercially relevant AI systems depend on the collection, use, analysis, storage, or transfer of personal data.

The NDPA applies to the processing of personal data by controllers and processors in Nigeria, and also applies to persons not domiciled, resident, or operating in Nigeria where they process personal data of data subjects in Nigeria. This is significant for foreign AI vendors, cloud providers, API providers, SaaS platforms and multinational businesses whose AI systems process personal data relating to individuals in Nigeria.[3]

The GAID goes beyond general data protection principles. Article 43 applies to data controllers and data processors that deploy or intend to deploy Emerging Technologies, including Artificial Intelligence, Internet of Things and Blockchain, for the purpose of processing personal data. It requires such organisations to consider the NDPA, public policy, the GAID and other NDPC regulatory instruments in safeguarding data subjects' privacy. Article 43 also requires technical and organisational parameters for emerging technology tools, including safeguards relating to automated decisions, erasure, sensitive personal data, children and vulnerable groups, cross-border flows, and privacy by design and default.[4] Accordingly, Nigeria does not presently have a complete AI law, but it does have binding AI-relevant rules. The practical point for businesses is straightforward: where an AI system processes personal data or affects data subjects' privacy and related rights in Nigeria, compliance obligations already exist.

[3] NDPA, section 2(2).
[4] GAID 2025, Article 43(1)-(2)

Key Areas Where the NDPA and GAID Regulate AI

a. Data Collection, Training Datasets and Lawful Processing

One of the most commercially consequential aspects of the NDPA and GAID framework is how early compliance obligations arise. AI compliance does not begin at product launch. It begins at the point of data collection, dataset acquisition, model training, testing, validation and deployment.

Under the NDPA, personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate; stored no longer than necessary; and processed securely. These principles apply to AI training pipelines, fine-tuning exercises, inference workflows, automated profiling, customer analytics and AI-driven personalisation where personal data is involved.[5]

Organisations that scrape web data, licence third-party datasets, repurpose customer information, use employee data to train internal tools, or deploy AI models against user behaviour must identify a lawful basis for each processing activity. They must also ensure that the original purpose for which the data was collected is compatible with any subsequent AI-related processing. Where the new processing is materially different, additional transparency, consent, or another lawful basis may be required.

This is particularly important for recommendation engines, behavioural advertising tools and personalisation systems. The GAID's Schedule 1 treats certain forms of behavioural matching and targeted content delivery without explicit and voluntary consent as inconsistent with the consent framework and purpose limitation principle. AI systems that personalise content, prices, advertising, or access to opportunities, therefore, require careful purpose-mapping and consent/lawful-basis analysis.

b. Automated Decision-Making and Human Oversight

Section 37 of the NDPA gives a data subject the right not to be subject to a decision based solely on automated processing of personal data, including profiling, where the decision produces legal or similarly significant effects concerning the data subject. This directly affects AI systems used for credit scoring, loan approvals, fraud blocking, recruitment filtering, insurance pricing, access control, identity verification, risk scoring and other consequential decisions.[6]

The NDPA recognises limited exceptions, including where the decision is necessary for entering into or based on the data subject's consent. However, even where an exception applies, the data subject retains important safeguards, including the right to obtain human intervention, express their point of view and contest the decision.

For businesses, this means that AI governance cannot be reduced to legal paperwork. Product design must support meaningful human review, explainable escalation pathways, contestability and records showing that a human reviewer is not merely rubber-stamping algorithmic outputs. A nominal human reviewer who simply approves an AI decision without real consideration may not provide meaningful protection.

The GAID reinforces this point by requiring emerging technology deployments to consider the right against decisions based solely on automated processes or algorithms as part of the technical and organisational parameters for the tool. In practical terms, automated decision-making governance is a legal, operational, product and engineering issue.

[5] NDPA, section 24.
[6] NDPA, section 37

c. Pre-deployment governance for AI and emerging technologies

Article 43 of the GAID is the clearest AI-facing provision in Nigeria's current data protection framework. It applies where a controller or processor deploys or intends to deploy AI for the processing of personal data. The organisation is expected to set out technical and organisational parameters for the processing and design of the tool, with particular regard to automated decisions, erasure, sensitive data, children and vulnerable groups, cross-border data flows, and privacy by design and default.[7]

Article 43 further requires assessment of emerging technology tools before deployment. The assessment must consider the suitability of sandbox or controlled-environment testing, the possibility of creating systemic bias, whether there are disparate outcomes, and whether such outcomes can be effectively addressed. Where risks cannot be mitigated, the controller or processor may be required to retool, retest or discard the tool.[8]

This is, in substance, an AI impact assessment obligation. It is not limited to traditional privacy harms. It requires organisations to consider disparate impact, vulnerable groups, data ethics and accountable use of data. For AI developers and deployers, bias testing, privacy-by-design review, rights-impact analysis and post-deployment monitoring should form part of the product development lifecycle.

Article 43(5) is also significant because it clarifies that the "suitability" or "possibility" of a safeguard or act implies an obligation to take reasonable technical and organisational measures in guaranteeing fair and accountable use of data, taking into account data ethics and regulatory audits.[9]

d. Human-rights limits on AI deployment

Article 44 of the GAID introduces a broader public-interest and human-rights dimension to AI governance. It provides that controllers and processors may benchmark with a global consensus on emerging technologies, including the United Nations Resolution on Artificial Intelligence. It further provides that controllers and processors should refrain from or cease the use of emerging technology systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights.[10]

This provision should be treated carefully. It does not transform the GAID into a full AI Act, but it does impose a meaningful compliance obligation where AI systems process personal data and create rights-related risks. Organisations deploying AI in high-impact contexts should therefore document human-rights and privacy-risk assessments, including risks of discrimination, exclusion, surveillance, manipulation, denial of opportunity, loss of access to services and lack of effective redress.

e. Data Protection Impact Assessments for High-Risk AI Systems

Data Protection Impact Assessments (DPIAs) are central to AI compliance under the NDPA and GAID. Article 28(3) of the GAID lists circumstances in which a DPIA is mandatory. The categories most relevant to AI include evaluation or scoring, automated decision-making with legal or similarly significant effects, systematic monitoring, processing of sensitive personal data, processing of data relating to vulnerable persons, use of innovative technologies posing significant privacy risk, financial services processing through digital devices, healthcare services, e-commerce, educational services, surveillance cameras in public-facing places and cross-border data transfers.[11]

Many commercially relevant AI deployments will fall within at least one of these categories. An AI tool used in a bank may involve profiling, financial services processing and automated decision-making. A hospital AI tool may involve sensitive health data and clinical decision support. A recruitment tool may involve scoring, profiling and significant effects on job applicants. A smart surveillance tool may involve systematic monitoring and public-space surveillance.

[7] GAID, Article 43(1)-(3).
[8] GAID, Article 43(4).
[9] GAID, Article 43(5).
[10] GAID, Article 44(3).
[11] GAID, Article 28(3).

The GAID provides that a DPIA should be submitted before the commencement of processing whenever required. It also provides that controllers or processors deploying software for processing sensitive personal data must conduct and submit a DPIA within four months after the issuance of the GAID, and that where processing commenced before the NDPA and GAID, a DPIA must be carried out within six months of the issuance of the GAID. On a strict reading, those transitional timelines have already elapsed.[12]

The enforcement consequence is material. The GAID provides that failure, refusal, or negligence in conducting a DPIA may, among other enforcement measures under the NDPA, result in restriction of all platforms where data subjects may have contact with the controller or processor for transactions involving personal data. For a consumer-facing AI product, that is not a nominal compliance risk; it can become an operational risk.

f. Cross-Border Data Transfers and Global AI Infrastructure

AI infrastructure is often global. Nigerian user data may be hosted in foreign cloud environments, processed through international APIs, transferred to offshore model providers, or accessed by regional teams outside Nigeria. Each of these flows may constitute a cross-border transfer of personal data from Nigeria.

Part VIII of the NDPA regulates cross-border transfers. A controller or processor must not transfer personal data from Nigeria to another country unless the recipient is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection in accordance with the NDPA, or one of the statutory derogations applies. The NDPA requires controllers or processors to record the basis for the transfer and the adequacy of protection.[13]

For AI deployers, this means that reliance on a foreign vendor's standard data processing terms will not automatically satisfy Nigerian law. Organisations should map each AI workflow, identify data flows, assess transfer mechanisms, review cloud/API/vendor terms, record the lawful basis for transfer and ensure that data subjects are provided with appropriate transparency. Section 43(2) of the NDPA also provides that no specific international or multinational cross-border data transfer code, rule, or certification mechanism shall be adopted as a Nigerian standard for the protection of data subjects or data sovereignty without approval of the National Assembly.[14]

[12] GAID, Article 28(8)-(10).
[13] NDPA, sections 41-42; GAID, Article 45 and Schedule 5.
[14] NDPA, section 43(2).

Gaps in the Existing AI Governance Framework in Nigeria

The NDPA and GAID are more significant for AI governance than many businesses realise. However, they do not eliminate the need for a dedicated AI governance framework. Their strength lies in data protection, privacy, accountability and rights-based compliance. Their limitation is that not all AI risks are data protection risks.

a. Absence of a Statutory Definition and Definitional Boundaries for Artificial Intelligence: Neither the NDPA nor the GAID provides a detailed statutory definition of Artificial Intelligence or a comprehensive classification of AI systems by risk level. The GAID identifies AI as an Emerging Technology, but it does not distinguish between low-risk, limited-risk, high-risk and prohibited AI systems. This creates uncertainty for developers, investors and users trying to determine which obligations apply to specific tools.

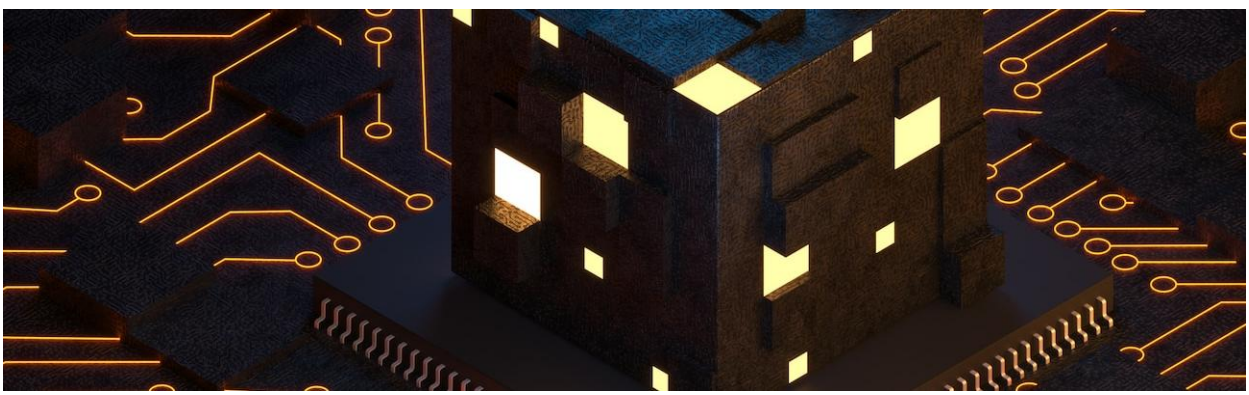
b. Risk of Circumvention Through Nominal Human Review: The NDPA focuses on decisions based solely on automated processing. This creates a possible compliance gap where a human is inserted into the process in form but not in substance. A dedicated AI law could clarify what meaningful human oversight requires, including reviewer competence, independence, access to relevant information, documentation and authority to override an AI output.

c. Lack of an AI-Specific Liability Framework: The NDPA does not resolve how liability should be allocated where an AI system causes harm through the combined actions of model developers, deployers, data providers, API providers, cloud vendors and end-user organisations. This is a major commercial issue for AI procurement, insurance, contractual allocation of risk and litigation strategy.

d. Fragmented Regulatory Jurisdiction and Oversight: Regulatory jurisdiction AI systems may fall under several regulators at once, including the NDPC, Central Bank of Nigeria, Securities and Exchange Commission, Nigerian Communications Commission, National Information Technology Development Agency, National Agency for Food and Drug Administration and Control, and sector-specific professional bodies. Without coordination, businesses may face overlapping or inconsistent expectations. A dedicated AI governance framework should therefore include a clear coordination mechanism among regulators.

e. Limited technical supervisory infrastructure

Effective AI regulation requires technical capacity. Regulators need the ability to understand model development, data engineering, algorithmic risk, privacy-enhancing technologies, cybersecurity controls, model documentation and system monitoring. The NDPC's data protection mandate gives it an important role, but the broader AI governance ecosystem will require deeper technical capacity across regulators.



Recommendations for Businesses, Regulators and Technology Stakeholders

a. Businesses should operationalise existing NDPA and GAID AI obligations

Organisations should not wait for a dedicated AI law before building AI governance controls. They should identify all AI systems that process personal data, map data flows, determine lawful bases for processing, conduct DPIAs where required, document technical and organisational parameters, review automated decision-making processes, implement human oversight, test for disparate outcomes, review vendor contracts and establish post-deployment monitoring. Inserted practical AI Compliance Checklist covering AI inventory, lawful basis, DPIAs, automated decisions, bias/disparate impact, cross-border transfers, vendor governance and monitoring.

b. Regulators should issue sector-specific AI/data protection guidance

The NDPC should work with sector regulators to issue practical guidance on how the NDPA and GAID apply to AI in finance, healthcare, telecommunications, education, advertising, employment, insurance, e-commerce and public administration. Sector-specific guidance will reduce uncertainty and improve compliance quality.

c. Nigeria should enact a dedicated AI framework that complements the NDPA and GAID

A dedicated Nigerian AI law should not duplicate the NDPA and GAID. It should complement them by introducing a statutory AI definition, risk classification, prohibited practices, conformity assessment for high-risk systems, incident reporting for serious AI failures, AI-specific liability rules, procurement standards, transparency obligations and regulatory coordination mechanisms.

d. The NDPC should build technical and sandbox capacity

Article 43 already contemplates controlled-environment testing and retesting of emerging technology tools. Nigeria should build institutional infrastructure around this by formalising AI/data protection sandbox processes, creating testing templates, encouraging responsible experimentation and publishing anonymised regulatory learnings.

e. International benchmarks should be used carefully

Nigeria should align with credible international AI governance standards where appropriate, but such alignment should be adapted to the NDPA, GAID, Nigerian constitutional values, local market realities and data sovereignty considerations.

Conclusion

Nigeria is yet to enact a standalone Artificial Intelligence Act. However, AI is not operating in a regulatory vacuum. Where AI systems process personal data or affect data subjects in Nigeria, the NDPA and GAID already impose binding obligations relating to lawful processing, transparency, purpose limitation, automated decision-making, DPIAs, emerging technology governance, cross-border transfers, data ethics, vulnerable groups, and human-rights-related risks.

The better view is not that Nigeria has no AI regulation. Rather, Nigeria currently has a binding data protection-based AI compliance framework and an emerging AI policy and legislative architecture. Businesses that understand this distinction will be better prepared for enforcement, investment due diligence, product governance and eventual AI-specific regulation.

For organisations deploying AI in Nigeria, compliance is not a future obligation. It is already present. The immediate task is to map AI systems against the NDPA and GAID, close existing compliance gaps and build governance frameworks capable of scaling with Nigeria's forthcoming AI regulatory regime.

For further enquiries, reach out to **contact@strenandblan.com**

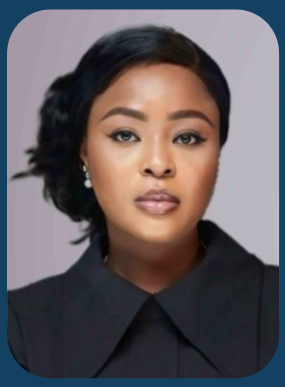
About **Stren & Blan Partners**

Stren & Blan Partners is an innovative and dynamic Law Firm with a compelling blend of experienced lawyers and energetic talents. We are focused on providing solutions to our client's business problems and adding value to their businesses and commercial endeavours. This underpins our ethos as everything we do flows from these underlying principles.

Stren & Blan Partners is a full-service commercial Law Firm that provides legal services to diverse local and multinational corporations. We have developed a clear vision for anticipating our client's business needs and surpassing their expectations, and we do this with an uncompromising commitment to Client service and legal excellence.

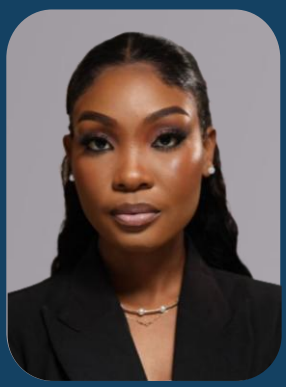
The **Authors**

Christian Aniukwu
Partner



Francisca Igboanugo
Team Lead

Linda Daramola
Associate



Eniola Alayo
Associate

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road,
Lekki Phase 1, Lagos, Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan