Making AI Accountable Data Protection Pathways in Nigeria's National AI Strategy

Chukwuyere Ebere Izuogu

Image credit: https://aiexpoafrica.com/nigeria-publish-draft-national-artificial-intelligence-strategy-nais/

Introduction

In September 2025, the National Center for Artificial Intelligence and Robotics (NCAIR), in collaboration with the National Information Technology Development Agency (NITDA) and the Federal Ministry of Communication, Innovation and Digital Economy (FMCIDE), released Nigeria's National Artificial Intelligence Strategy (the Strategy). The Strategy represents a timely and strategically important intervention in Nigeria's digital policy landscape. It reflects a deliberate effort by the Nigerian state to articulate a national vision for artificial intelligence that balances innovation, economic competitiveness, public sector transformation, and societal protection. The Strategy demonstrates clear awareness of global AI policy conversations and draws from international norms on ethical AI, inclusion, and development-oriented deployment. Its framing of AI as a general purpose and economy wide technology, rather than a narrow sectoral tool, is conceptually sound and consistent with contemporary global thinking.

In terms of strategic objectives, the Strategy seeks to drive economic growth and competitiveness by leveraging AI to enhance industrial productivity, create jobs, and stimulate innovation through the engagement of both local and international stakeholders. At the same time, it seeks to advance social development and inclusion by improving outcomes in critical sectors such as healthcare, agriculture, and education, addressing challenges such as poverty, inequality, and climate change, strengthening government service delivery, and ensuring that all citizens can access and benefit from AI technologies. In addition, the Strategy focuses on strengthening Nigeria's technological capacity and global leadership by building research, development, and innovation capabilities, establishing frameworks for responsible and ethical AI, and positioning Nigeria as an active and influential participant in the global AI ecosystem.

At a structural level, the Strategy is organised around five (5) strategic pillars that address building foundational AI infrastructure, fostering and sustaining a world class AI ecosystem, accelerating the adoption of AI and its transformative impact across key sectors, ensuring the responsible and ethical development and deployment of AI, and establishing a robust framework for AI governance. The Strategy's emphasis on local relevance, capacity development, and inclusive growth is particularly appropriate in the Nigerian context, where digital divides, institutional capacity gaps, and socio-economic disparities remain salient. The document also correctly identifies risks associated with AI deployment, including bias, privacy violations, security threats, labour displacement, and

misinformation, and positions governance as a central policy concern rather than an afterthought.

In this article, I examine the Strategy to assess whether it provides a structured integration of data protection and data privacy considerations under the Nigerian Data Protection Act (NDPA) and the extent to which these considerations translate into legal obligations and practical governance expectations for organisations across the AI value chain that process personal data. The review also offers concrete guidance for implementing these requirements in a manner that aligns with the realities of Nigerian institutions and their data processing activities.

Data Protection as a Foundation for Responsible AI in Nigeria

While the Strategy occupies a pivotal role in Nigeria's evolving data governance framework, the effectiveness and credibility of its implementation will increasingly depend on how clearly it addresses data protection and data privacy as essential enablers of responsible AI deployment. As artificial intelligence systems rely on large scale data collection, automated inference, and continuous learning, data is not merely an input but the infrastructure on which AI value is created, risks are amplified, and trust is either maintained or undermined. Accordingly, the Strategy must move beyond high level ethical commitments and incorporate concrete data protection principles that apply across the AI lifecycle and throughout the entire AI value chain.

At present, the Strategy acknowledges data governance in general terms, in particular, it recognises that data governance standards should align with the principles of the NDPA. However, it does not provide sufficient detail on how existing data protection obligations established by the NDPA intersect with the development, deployment, and use of artificial intelligence. This creates a material policy gap. Artificial intelligence systems raise distinct and heightened risks to privacy, autonomy, fairness, and accountability because of their capacity to infer sensitive attributes, repurpose data beyond original collection contexts, and generate decisions at scale with limited human oversight. Without explicit alignment between the Strategy and the NDPA, organisations operating across the AI value chain face uncertainty regarding compliance expectations and enforcement priorities.

A central improvement that should be reflected in the Strategy is a clear recognition that data protection is a cross-cutting obligation that applies to all actors in the AI ecosystem, including data collectors, model developers, system integrators, deployers, and downstream users. Each of these actors may qualify as a data controller or data processor depending on their functional role, level of decision-making authority, and degree of control over personal data. The Strategy should therefore explicitly adopt a role-based approach that mirrors established data protection doctrine rather than assuming a single category of AI operator.

Under the NDPA, the concepts of data controller and data processor are central to accountability. The Strategy should adopt these concepts explicitly and apply them to the AI value chain. Data controllers within the AI ecosystem include organisations that determine the purposes and means of data processing for AI training or deployment. These may include public institutions deploying AI driven decision systems, private companies offering AI enabled services, or platform operators integrating AI features into digital products. Data processors include entities that process personal data on behalf of controllers such as cloud service providers, model training

vendors, data annotation firms, and infrastructure providers.

For organisations acting as data controllers within the AI value chain, the Strategy affirms core principles of lawful processing and obligations established under the NDPA, including data minimisation, purpose limitation, data subject rights, data security, and transparency. These principles are not abstract ideals but have direct operational implications for the design of AI systems. For instance, data minimisation requires a careful assessment of whether the scale and granularity of data used for model training are proportionate to the intended outcomes, particularly when personal or sensitive data is involved. Similarly, purpose limitation requires that training data sets be clearly defined and documented in relation to specific and legitimate objectives, rather than collected indiscriminately for unspecified future use.

For data processors involved in AI development or deployment, the Strategy should emphasise contractual clarity, technical safeguards, and auditable processing practices. Processors often operate model training infrastructure, annotation services, cloud platforms, or inference engines on behalf of controllers. In these contexts, the Strategy should encourage the adoption of processor obligations that go beyond baseline security and extend to model governance, access controls, logging, and incident reporting. This is particularly important where processors may independently influence model behaviour through architectural choices, parameter tuning, or optimisation techniques.

One of the most critical data protection challenges raised by artificial intelligence is the reuse and repurposing of data for model training. The Strategy should address this explicitly. Many AI systems rely on historical data sets that were originally collected for unrelated purposes, often without any contemplation of automated decision making or large-scale inference. The Strategy should require that organisations conduct documented compatibility assessments before reusing personal data for AI training. These assessments should consider the relationship between the original collection purpose and the new AI use case, the reasonable expectations of data subjects, the nature of the data involved, and the potential impact on individual rights. Where incompatibility is identified, organisations should be required to obtain fresh lawful basis or refrain from reuse.

Closely related is the issue of consent and lawful basis. The Strategy should avoid framing consent as the default lawful basis for AI processing. Instead, it should encourage organisations to assess appropriate lawful bases under the NDPA including legal obligation, public interest, and legitimate interest. Where legitimate interest is relied upon, the Strategy should require documented balancing tests that assess necessity, proportionality, and impact on data subjects. This mirrors established data protection practice and provides defensible grounds for AI innovation. At the same time, where consent is relied upon, the Strategy should emphasise that consent must be meaningful, informed, and freely given, and that individuals should not be subjected to opaque or coercive consent mechanisms embedded within complex digital services.

Transparency is an area where the Strategy requires further strengthening from a data protection perspective. AI systems often operate as opaque black boxes, making it difficult for individuals to understand how their data is used or how decisions affecting them are made. While the Strategy recognises that principles of data processing under the NDPA, such as transparency and information provision, are

essential for protecting the fundamental rights of data subjects, these obligations need to be translated into AI-specific disclosures. The Strategy should require organisations to provide clear and accessible information about how AI systems process personal data, the logic underlying automated decision making, and the potential impacts on individuals. This is particularly important in high impact applications such as credit scoring, recruitment, healthcare, law enforcement, and public service delivery, where meaningful explanations should be provided to enable affected persons to understand and, where necessary, contest outcomes.

The Strategy should incorporate data subject rights as a core component of its AI governance pillar. Rights including access, rectification, erasure, restriction, objection, and data portability are not optional features but legally enforceable safeguards that must be operationalised within AI systems. The Strategy should encourage organisations to design AI systems that enable these rights to be exercised effectively through human review mechanisms, appeal processes, and technical tools that support data correction and model retraining where appropriate. It should also acknowledge the practical challenges of rectification and erasure in trained models, particularly in extreme cases where such challenges may necessitate measures such as AI model disgorgement. To ensure proportional and effective compliance, the Strategy should promote solutions including model retraining, parameter adjustment, suppression of outputs, or, in exceptional circumstances, disgorgement of AI models to uphold data subject rights.

Cross border data transfers represent another critical policy issue. Many AI systems rely on global data flows, cloud infrastructure, and multinational development teams. The Strategy should clarify how international data transfers for AI related purposes should be assessed and governed, including through adequacy decisions, standard contractual safeguards, and risk-based assessments. This is particularly important for Nigerian organisations partnering with foreign AI providers or participating in global AI research and development initiatives.

From an implementation perspective, effective institutional coordination is essential. The Strategy should recognise data protection authorities as key partners in AI governance and promote collaboration on the development of guidance, enforcement priorities, and capacity building. Mechanisms such as joint regulatory sandboxes and advisory opinions could support innovation while ensuring compliance with legal requirements. The Strategy should also encourage the creation of sector specific guidance that addresses the distinct data protection risks posed by AI in areas including finance, telecommunications, healthcare, education, and public administration.

Capacity building is another area where data protection considerations should be embedded. Organisations across the AI value chain require practical tools, templates, and training to operationalise compliance. The Strategy should support the development of standardised risk assessment frameworks, model documentation practices, and compliance toolkits that integrate data protection by design and by default. This will help reduce compliance fragmentation and support innovation within clear regulatory boundaries.

Finally, the Strategy should adopt a proportionate and risk-based approach to data protection in AI governance. Not all AI systems pose the same level of risk. Low risk applications may require lighter touch obligations, while high risk or systemic applications should be subject to enhanced scrutiny, documentation, and oversight. This approach aligns

with emerging global standards and supports regulatory credibility while avoiding unnecessary burdens on innovation.

Conclusion

Nigeria's National Artificial Intelligence Strategy represents a strong and timely policy foundation for harnessing the benefits of AI while managing its associated risks. However, its effectiveness will ultimately depend on how clearly and coherently data protection and data privacy considerations are integrated into its implementation architecture. As this analysis demonstrates, alignment with the NDPA is not merely complementary but essential to ensuring responsible, lawful, and trustworthy AI deployment across the AI value chain. Without clearer articulation of roles, obligations, and compliance expectations, organisations may face uncertainty that undermines both innovation and accountability.

Implementation therefore presents an important opportunity to operationalise these considerations through legislative, regulatory, and institutional reforms. Legislative reforms, whether through amendments to existing digital laws or the enactment of AI specific instruments, could clarify how data protection principles apply to AI systems, embed risk-based obligations, and provide legal grounding for measures such as enhanced transparency, enforceable data subject rights, and proportionate remedies including, in extreme cases, AI model disgorgement. Such reforms would strengthen legal certainty while ensuring that AI governance remains anchored in fundamental rights protection.

Equally important is the role of coordinated institutional action. Effective collaboration between AI policy bodies, data protection authorities, and sector regulators can translate high level strategy into practical guidance, supervisory priorities, and compliance tools tailored to Nigerian realities. This approach would support innovation within clear guardrails, reduce regulatory fragmentation, and build confidence among both domestic and international stakeholders.

Ultimately, embedding data protection as a foundational element of AI governance through thoughtful implementation and, where necessary, legislative reform will enhance the credibility, resilience, and sustainability of Nigeria's AI ecosystem. Doing so will position Nigeria not only as an adopter of global AI norms but as a jurisdiction capable of shaping responsible AI governance in a manner that reflects its legal framework, institutional capacity, and development priorities.

Disclaimer

Contact person for this article

Chukwuyere Izuogu, LL.M (Hannover), CIPP/E

chukwuyere@sskohn.com

STREAMSOWERS & KÖHN is a leading commercial law firm providing legal advisory and advocacy services from its offices in Lagos, Abuja, and Port Harcourt. The firm has extensive experience in acting for Nigerian and international companies, government, and industry regulators in the firm's various areas of practice.

Contact us at:
852b Bishop Aboyade Cole St,
Victoria Island,
Lagos
Tel: +234 1 271 2276; **Fax:** +234 1 271 2277
Email: info@sskohn.com; **Website:** www.sskohn.com