Page 2481 - 2495 **DOI:** *https://doij.org/10.10000/IJLMH.119827*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment

STEPHANIE NMA MODILIM[1], IYANUOLUWA BOLARINWA[2], MOTUNRAYO TOLANI OMIDIORA[3] AND OBAH TAWO[4]

ABSTRACT

This article critically examines Nigeria's evolving data protection landscape, focusing on the transition from the Nigeria Data Protection Regulation (NDPR) of 2019 to the more comprehensive Nigeria Data Protection Act (NDPA) of 2023. The research analyzes how this legislative progression addresses previously identified regulatory gaps and aligns with global data governance standards, particularly the EU's General Data Protection Regulation (GDPR). Through comparative analysis of institutional frameworks, enforcement mechanisms, and compliance requirements, the study evaluates the NDPA's strengths and limitations in protecting individual privacy rights while fostering digital innovation. Key findings reveal that while the NDPA significantly strengthens Nigeria's data protection regime through the establishment of the independent Nigeria Data Protection Commission (NDPC), expanded data subject rights, and formalized cross-border data transfer protocols, substantial challenges remain in regulatory independence, judicial efficiency, and emerging technology governance. The article concludes by proposing forward-looking policy recommendations to enhance Nigeria's digital privacy framework, particularly in addressing AI governance, cybersecurity integration, and global data flow adequacy requirements to position Nigeria as a regional leader in data governance.

Keywords: *Data Protection, Nigeria Data Protection Act, Privacy Regulation, Digital Governance, Cross-Border Data Transfers, Regulatory Compliance*

I. INTRODUCTION

The governance of personal data has become a central issue for digital economies, particularly in countries where innovation and privacy rights must be carefully balanced. Nigeria,

[1] School of Law, Fordham University, NewYork, USA.
[2] Department of Public Administration, Indiana University Bloomington, USA.
[3] Nigerian Law School, Enugu, Nigeria.
[4] Department of Computer Science, Wrexham University, Wales, UK

 [ISSN 2581-5369]

recognized as Africa's largest digital economy, has seen tremendous growth in fintech, e-commerce, telecommunications, and other digital services. However, this rapid transformation has also intensified concerns around data breaches, identity theft, and cybercrime, raising questions about how effectively the nation's legal and regulatory framework can respond to these challenges (Awofadeju et al., 2024).

In 2019, the Nigerian government introduced the Nigeria Data Protection Regulation (NDPR), a subsidiary legislation developed by the National Information Technology Development Agency (NITDA). The NDPR was a groundbreaking initiative that laid the foundation for Nigeria's digital privacy governance. Nonetheless, its limitations quickly became apparent. As a regulation rather than a statute, it lacked the necessary legal authority and institutional backing to ensure consistent enforcement. This regulatory gap led to significant compliance ambiguities and enforcement challenges, ultimately undermining trust in the system (Idowu, 2022).

To address these shortcomings, the Nigerian government enacted the **Nigeria Data Protection Act (NDPA)** in June 2023. The Act replaces the NDPR and establishes a more comprehensive legal and institutional framework for data governance. One of its key achievements is the creation of the Nigeria Data Protection Commission (NDPC), a statutory body mandated to enforce compliance, oversee cross-border data transfers, and impose penalties for violations (Nigeria Data Protection Act, 2023). The NDPA also codifies individual privacy rights and aligns Nigeria's data protection framework with international standards such as the EU General Data Protection Regulation (GDPR), thus facilitating cross-border trade and boosting investor confidence (Ekanem, 2023).

In terms of business compliance, the NDPA introduces stricter obligations for data controllers and processors, including mandatory data audits, lawful processing criteria, and provisions for data subject consent. For businesses operating in Nigeria's digital landscape, this marks a shift from voluntary adherence to enforceable compliance mechanisms. According to KPMG (2023), firms must now reconfigure their internal data governance strategies and adopt enterprise-wide privacy management systems to avoid sanctions and reputational risk.

The broader implication of the NDPA lies in its potential to catalyze digital innovation while safeguarding civil liberties. By providing a stable and predictable regulatory environment, the Act reduces the risk of arbitrary enforcement and supports the secure exchange of information a critical enabler of innovation in AI, digital finance, and smart infrastructure. As highlighted by Olatunji (2022), the transition from the NDPR to the NDPA reflects Nigeria's strategic ambition to become a global player in digital governance, offering a model for other African

 [ISSN 2581-5369]

nations to emulate.

The Nigeria Data Protection Act, 2023, represents a significant step forward in aligning Nigeria's data governance ecosystem with global best practices. It strengthens privacy protections, institutionalizes regulatory oversight, and clarifies compliance pathways for businesses. Through its provisions, the NDPA not only addresses the legal deficiencies of the NDPR but also positions Nigeria for leadership in data sovereignty and innovation in the digital age.

II. From NDPR to NDPA: A Necessary Evolution in Nigeria's Data Protection Framework

The governance of personal data is a defining concern of the 21st-century digital economy, demanding legal mechanisms that safeguard privacy without stifling innovation. Nigeria's initial step toward regulating personal data was the introduction of the **Nigeria Data Protection Regulation (NDPR)** in 2019 by the **National Information Technology Development Agency (NITDA)**. While the NDPR was instrumental in raising awareness and initiating compliance discussions, its legal nature as a subsidiary regulation made it inherently weak in enforcement, legitimacy, and institutional authority (Akintunde, 2022).

One of the fundamental shortcomings of the NDPR was its lack of statutory authority. As it was not enacted by the legislature, it could not function with the force of law. This ambiguity led to poor industry uptake, weak compliance incentives, and jurisdictional overlaps. Regulatory authority rested with NITDA, an agency that was not originally mandated for data protection, which further contributed to fragmented oversight and unclear enforcement pathways (Idowu, 2022). Without a formalized adjudicatory mechanism, data controllers often interpreted the regulation to suit organizational convenience, thereby undermining its normative intent.

Enforcement under the NDPR was not only limited but also symbolic. While the regulation prescribed monetary penalties for non-compliance, the fines were too lenient to deter violations, especially among large technology companies with vast revenues. In contrast to the **General Data Protection Regulation (GDPR)** of the European Union which imposes fines of up to 4% of global annual turnover the NDPR lacked teeth in penalization, making violations a low-risk affair for multinational corporations (Akintunde, 2022; Hogan Lovells, 2023). Moreover, Nigeria's judicial system had not developed case law around the NDPR, making compliance standards uncertain and litigation-based deterrence virtually nonexistent.

The regulation's approach to **cross-border data transfers** also proved inadequate. While the

NDPR required data controllers to ensure an "adequate level of protection" before transferring personal data abroad, it failed to define what constituted "adequacy" or provide mechanisms like **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)**. This ambiguity posed significant legal and commercial risks for cloud service providers, fintech companies, and multinational firms engaged in global data flows (Ekanem, 2023). Given that Nigeria had not achieved data adequacy recognition from the **European Commission**, businesses faced duplicative compliance burdens in aligning with international privacy expectations (KPMG, 2023).

Another critical deficiency lay in the **limited articulation of data subject rights**. Although the NDPR acknowledged basic privacy principles, it lacked a robust framework for individual redress. It did not clearly establish rights such as data portability, the right to be forgotten, or formal complaint mechanisms. In contrast, the GDPR provides data subjects with enforceable rights and explicit legal channels to challenge misuse by both private and public actors. This lacuna allowed powerful institutions in Nigeria to exploit data without meaningful accountability or citizen recourse (Olatunji, 2022).

These systemic gaps led to the enactment of the **Nigeria Data Protection Act (NDPA)** in 2023, a statutory reform designed to elevate the country's data protection regime to global standards. One of the Act's most transformative provisions is the establishment of the **Nigeria Data Protection Commission (NDPC)** an autonomous body empowered to investigate violations, sanction erring entities, and issue legally binding compliance orders (Nigeria Data Protection Act, 2023). This represents a departure from NITDA's limited agency model and aligns Nigeria with global regulatory practices, such as those in the EU, UK, and South Africa.

Under the NDPA, **data subject rights** have been significantly expanded. Individuals are now granted the right to erasure, data portability, and explicit consent under lawful processing categories. The Act introduces clear legal obligations on data controllers and processors to uphold these rights, with oversight mechanisms to ensure compliance (KPMG, 2023). These reforms close the normative gap left by the NDPR and provide legal certainty for both individuals and businesses.

Additionally, the NDPA formalizes cross-border data transfer protocols. It authorizes mechanisms similar to SCCs and BCRs, which are critical for interoperability with international data regimes. These provisions not only reduce the risk of regulatory conflict but also position Nigeria for eventual data adequacy recognition an essential prerequisite for seamless global digital trade (Ekanem, 2023). By embedding these tools within its statutory framework, Nigeria

signals its readiness to engage competitively in cross-jurisdictional data flows.

Nonetheless, the implementation of the NDPA poses notable challenges. The operationalization of the NDPC requires substantial capacity-building, both in terms of personnel and infrastructure. Regulatory effectiveness will depend not only on the autonomy of the commission but also on its ability to engage in public education, stakeholder collaboration, and risk-based supervision. Moreover, the rise of **AI-enabled data processing, algorithmic bias**, and **state surveillance** introduce new complexities that the NDPA must eventually contend with, particularly in crafting future regulations around emerging technologies (Awofadeju et al., 2024).

The transformation from the NDPR to the NDPA, while necessary, reflects more than a legal upgrade it represents a structural realignment of Nigeria's digital governance ethos. While the NDPR served as a preliminary framework, its limitations in statutory force, enforcement capacity, and regulatory sophistication underscored the need for reform. The NDPA fills that vacuum with stronger institutional mechanisms and global alignment, albeit with a host of technical, infrastructural, and ethical implementation hurdles that remain to be addressed.

III. KEY PROVISIONS OF THE NDPA: STRENGTHENING NIGERIA'S DATA PROTECTION FRAMEWORK IN LINE WITH GLOBAL STANDARDS

Establishment of the Nigeria Data Protection Commission (NDPC)

One of the most significant shifts introduced by the Nigeria Data Protection Act (NDPA) is the creation of the Nigeria Data Protection Commission (NDPC), a fully independent body mandated to oversee and enforce data protection laws in Nigeria (Nigeria Data Protection Act, 2023). This development corrects a critical institutional gap under the NDPR, where the National Information Technology Development Agency (NITDA) was responsible for enforcement despite lacking legislative empowerment and independence (Idowu, 2022).

Internationally, independence is considered a non-negotiable criterion for effective data governance. The European Union's General Data Protection Regulation (GDPR) and Kenya's Data Protection Act both mandate independent supervisory authorities with investigatory and sanctioning powers. Nigeria's adoption of a similar structure signals alignment with global best practices (Hogan Lovells, 2023). However, the operationalization of the NDPC remains a challenge, particularly in a regulatory climate where many agencies struggle with capacity, funding, and institutional autonomy (Olatunji, 2022). Without adequate resourcing and institutional fortification, the NDPC risks replicating the enforcement inertia seen under the

NDPR.

Expanded Rights of Data Subjects

The NDPA introduces a broader set of data subject rights that were either absent or weakly codified in the NDPR. These include the right of access to personal data, rectification, erasure (commonly referred to as the "right to be forgotten"), data portability, and the right to object to data processing (Nigeria Data Protection Act, 2023). These provisions echo the GDPR's commitment to empowering individuals to exercise agency over their personal information.

Nevertheless, the NDPA falls short in articulating procedural timelines and operational mechanisms for exercising these rights. The GDPR, for instance, requires data controllers to respond to access and deletion requests within one month and establishes clear grounds for appeal through data protection authorities. South Africa's Protection of Personal Information Act (POPIA) similarly includes procedural safeguards and response frameworks. In contrast, the NDPA's silence on enforcement timeliness and redress channels introduces interpretative ambiguity that could frustrate real-world compliance (KPMG, 2023).

Furthermore, enforcement of these rights will be contingent upon public awareness and the capacity of the NDPC to adjudicate complaints effectively. Given Nigeria's historical lag in digital literacy and civic tech adoption, individuals may lack the technical know-how or confidence to assert these rights unless targeted awareness campaigns accompany implementation (Awofadeju et al., 2024).

Compliance Obligations for Data Controllers and Processors

Under the NDPA, data controllers and processors are subjected to enhanced compliance obligations, particularly for high-risk data activities. These include implementing appropriate security safeguards, conducting data protection impact assessments (DPIAs), and appointing Data Protection Officers (DPOs) where necessary (Nigeria Data Protection Act, 2023). These requirements reflect core tenets of risk-based governance embedded in the GDPR and other global frameworks.

However, unlike the GDPR, which offers specific DPIA thresholds (e.g., systematic monitoring or large-scale processing), the NDPA is relatively silent on what constitutes "high-risk" processing or when a DPIA becomes mandatory (KPMG, 2023). This omission risks inconsistent interpretation and weakens predictability for businesses. Moreover, the Act does not prescribe standardized assessment methodologies or sector-specific guidance key tools that have supported compliance in more mature data jurisdictions (Adeyemi & Umeh, 2023).

 [ISSN 2581-5369]

The requirement to appoint DPOs also lacks clarity. While the GDPR mandates DPOs for public authorities and large-scale processors, the NDPA leaves room for subjective determination, raising questions about uniformity in implementation. This could lead to compliance fatigue in small and medium enterprises (SMEs), which may either over-comply or fall short due to resource constraints.

Regulation of Cross-Border Data Transfers

The NDPA introduces a formal mechanism for regulating cross-border data transfers, requiring that personal data be sent only to jurisdictions that provide adequate protection or through legally recognized safeguards such as contractual clauses (Nigeria Data Protection Act, 2023). This is an important evolution from the NDPR, which merely suggested "adequate protection" without specifying the operational tools required.

The alignment with the GDPR's tools such as **Standard Contractual Clauses (SCCs)** and **Binding Corporate Rules (BCRs)** suggests Nigeria's attempt to meet adequacy thresholds under global trade frameworks (Ekanem, 2023). Yet, Nigeria remains absent from the European Commission's list of data-adequate countries. This gap imposes compliance burdens on Nigerian-based multinational companies, especially those engaged in cloud computing, fintech, and digital outsourcing. The lack of interoperability with the EU legal environment may also disincentivize foreign investment in Nigerian digital services (Hogan Lovells, 2023).

Moreover, the NDPA does not yet specify a process for adequacy determinations or provide a register of approved safeguards, unlike more established frameworks in the UK and Kenya. These details are crucial in reducing legal uncertainty and protecting cross-border data flows from political and judicial disruptions.

Enforcement Mechanisms and Sanctions

The NDPA grants the NDPC explicit powers to conduct audits, investigate complaints, impose fines, and initiate legal proceedings against violators (Nigeria Data Protection Act, 2023). Theoretically, this marks a departure from the ineffective and informal enforcement under the NDPR, where penalties were inconsistent and lacked legal finality (Akintunde, 2022).

The GDPR has been cited globally for its aggressive enforcement, including billion-dollar fines against major tech firms. While the NDPA provides for similar administrative sanctions, it remains unclear whether the NDPC possesses the institutional capacity to investigate complex infractions, especially when such violations involve multinational companies or government agencies with entrenched political interests (Idowu, 2022).

 [ISSN 2581-5369]

A broader concern is whether the NDPC can resist external pressure and political interference, especially when enforcing provisions against state actors. Other African regulators, such as South Africa's Information Regulator and Kenya's Data Protection Commissioner, have experienced budgetary and jurisdictional constraints that hamper independent enforcement (Bolarinwa et al., 2023). Without financial autonomy, technical expertise, and legal safeguards, the NDPC's powers may exist more in form than in function.

IV. Enforcement challenges and corporate compliance in Nigeria's digital economy: institutional barriers and global comparisons

Regulatory Independence and Institutional Constraints

The Nigeria Data Protection Act (NDPA) establishes the Nigeria Data Protection Commission (NDPC) as an ostensibly independent regulator tasked with enforcing the nation's data governance regime (Nigeria Data Protection Act, 2023). However, independence in statutory language does not guarantee independence in practice. Nigeria's institutional history is replete with regulatory bodies whose autonomy is compromised by political influence, administrative opacity, or budgetary dependence on the executive branch (Bolarinwa, 2022).

This political interference risk is especially salient in cases where regulated entities are state-aligned or large corporations with political clout. In such a climate, enforcement actions may be selective or symbolic, especially if the NDPC lacks constitutional protections for budgetary independence and appointment procedures, as observed with other Nigerian agencies (Bolarinwa et al., 2023). In comparison, the European Data Protection Board (EDPB) enjoys institutional autonomy and standard-setting authority, enabling coordinated enforcement across the EU (Hogan Lovells, 2023). Similarly, Kenya's Data Protection Act insulates its Commissioner's office from executive control, reinforcing impartiality. Nigeria's NDPC requires not just formal independence, but institutional reinforcement through transparency mandates, funding mechanisms, and protection from executive capture (Adeyemi & Umeh, 2023).

Judicial and Administrative Bottlenecks

A major enforcement bottleneck under both the NDPR and now the NDPA is the role of Nigeria's judiciary in adjudicating data protection disputes. While the NDPA grants the NDPC investigative and sanctioning powers, the judiciary remains the final arbiter for many enforcement decisions (Nigeria Data Protection Commission, n.d.). Unfortunately, Nigeria's legal system is overburdened, with slow case resolution timelines and limited judicial

 [ISSN 2581-5369]

specialization in digital rights or data law (Akintunde, 2022). This delay can deter timely enforcement and allow violators to operate with impunity during protracted litigation.

The absence of judicial precedent further compounds the problem. Without settled case law, both businesses and regulators operate in a state of interpretive uncertainty, creating room for inconsistent compliance approaches and regulatory overreach (Idowu, 2022). In contrast, data protection frameworks in South Africa and the EU allow for administrative fines and sanctions without court approval, thereby increasing the speed and predictability of enforcement (Olatunji, 2022). To overcome these systemic challenges, Nigeria may need to empower the NDPC with broader quasi-judicial powers to resolve disputes through administrative tribunals or data protection review panels an approach supported by global best practice.

Risk Assessment and Compliance Audits

Corporate compliance under the NDPA hinges on the effective implementation of Data Protection Impact Assessments (DPIAs) and regular internal audits, particularly for high-risk data processing activities. The NDPA mandates these practices but stops short of defining thresholds for risk categorization, a gap that may lead to inconsistent implementation across sectors (KPMG, 2023). This ambiguity is particularly problematic for SMEs, which often lack the internal expertise to interpret vague statutory obligations, leading to either over-compliance or outright noncompliance (Hogan Lovells, 2023).

The GDPR mandates DPIAs for any processing that involves profiling, large-scale monitoring, or sensitive data categories. It also provides detailed guidance and registers of high-risk processing types. In contrast, Nigeria's approach under the NDPA lacks sector-specific guidance and standardized DPIA templates, which could support uniform adoption (Adeyemi & Umeh, 2023). Companies operating in highly digitized sectors such as fintech, e-commerce, or real estate which have already faced cybersecurity threats (Awofadeju et al., 2024) require clear, sector-adapted compliance protocols to navigate data risk efficiently.

Moreover, the success of compliance auditing under the NDPA will depend on the NDPC’s capacity to monitor, evaluate, and verify organizational adherence across Nigeria’s diverse and expanding digital economy. This will require both human resource development and technological investment within the Commission, which remains nascent (Nigeria Data Protection Act, 2023). Failure to audit comprehensively may result in selective enforcement or token compliance, particularly among firms lacking public visibility.

Corporate Governance and Internal Accountability Mechanisms

Corporate responses to data protection regulation depend heavily on governance structures and

 [ISSN 2581-5369]

internal accountability systems. The NDPA imposes an obligation on data controllers and processors to appoint Data Protection Officers (DPOs) for high-risk processing (Nigeria Data Protection Act, 2023). Yet, many Nigerian organizations still treat data protection as a legal formality, rather than embedding it into operational culture (Akintunde, 2022).

This disconnect often stems from a weak internal control environment. As observed by Bolarinwa et al. (2023), many Nigerian firms lack internal whistleblowing channels, independent compliance teams, or regular board-level review of risk functions. Without these governance mechanisms, DPOs operate in isolation and lack the institutional authority to enforce policy internally. In contrast, companies in the EU and UK often embed DPOs within governance structures, giving them oversight access and reporting lines to the highest management levels. Until Nigerian corporations undergo a similar shift one that treats privacy risk as reputational and operational, not just legal they may remain structurally non-compliant.

Public Trust, Transparency, and Civil Society Participation

Lastly, the efficacy of enforcement and compliance cannot be measured solely by institutional metrics; public trust and civil oversight play a crucial role. In Nigeria, civil society organizations and advocacy groups have historically held government and corporate actors accountable in governance spaces such as anti-corruption, public finance, and electoral transparency (Bolarinwa, 2022). These actors can also support the NDPC by conducting citizen education campaigns, initiating public interest litigation, and monitoring violations in under-regulated sectors.

However, such civic participation must be formalized into the regulatory architecture. The NDPA currently lacks mechanisms for stakeholder consultations, periodic transparency reports, or third-party audits all of which can build legitimacy and democratize enforcement (Tade & Umeh, 2023). As digital rights become more critical to everyday life, an open governance model where civil society acts as a watchdog and co-regulator may be vital to preventing regulatory capture and ensuring corporate accountability.

V. Regulatory Oversight and the Role of the Nigeria Data Protection Commission (NDPC)

The NDPC's Mandate and Institutional Structure

The Nigeria Data Protection Commission (NDPC), established under the Nigeria Data Protection Act (NDPA), is entrusted with enforcing the nation's data protection framework. Its statutory mandate includes ensuring compliance, conducting investigations, issuing penalties,

and overseeing public sensitisation on data rights (Nigeria Data Protection Act, 2023). While this marks a decisive institutional advancement from the Nigeria Data Protection Regulation (NDPR), critical structural uncertainties remain. Unlike the European Data Protection Board (EDPB), which coordinates enforcement across multiple jurisdictions, the NDPC operates as a standalone authority with no formalised cross-agency integration (Olatunji, 2022).

Comparatively, the UK's Information Commissioner's Office (ICO) functions with financial independence, funded by statutory data protection fees from businesses a model that ensures autonomy and sustainability. In contrast, the NDPC's funding model remains opaque, raising legitimate concerns over its vulnerability to executive influence (Bolarinwa, 2022). Kenya's Data Protection Commissioner has demonstrated early assertiveness through investigations and penalties, aided by defined operational independence (KPMG, 2023). For the NDPC to earn institutional legitimacy, it must adopt transparent governance practices and stakeholder engagement mechanisms, particularly in a country where regulatory bodies have often been perceived as politically compromised (Bolarinwa et al., 2023).

Enforcement and Compliance Monitoring

The NDPC is empowered to audit organizations, make binding corrective orders, and impose administrative penalties, creating a compliance environment that extends beyond mere advisory capacity (Nigeria Data Protection Act, 2023). However, the law is ambiguous about upper limits of penalties, unlike the GDPR, which imposes fines up to 4% of global turnover for serious violations (Hogan Lovells, 2023). The lack of statutory clarity in Nigeria may weaken the deterrent effect of enforcement and invite uneven implementation, particularly among multinationals that calibrate compliance based on enforcement probability.

Furthermore, risk-based enforcement is critical for regulatory efficiency. The ICO in the UK and Kenya's Office of the Data Protection Commissioner (ODPC) use severity-based prioritisation, focusing enforcement on high-risk sectors such as fintech and telecommunications (Tade & Umeh, 2023). Nigeria's digital economy is heavily populated by under-regulated entities with vast data exposure. Without a structured risk-ranking model or public compliance registers, the NDPC risks reactive enforcement an approach that may undercut its credibility in the long term (Akintunde, 2022).

Early enforcement actions are instrumental in shaping business perception and encouraging voluntary compliance. Kenya's ODPC has publicly sanctioned violators, creating a demonstrable accountability culture. The NDPC must pursue similar high-visibility enforcement to establish authority. However, such actions must be accompanied by procedural

 [ISSN 2581-5369]

fairness and transparency to prevent abuse, especially in Nigeria's politically sensitive corporate landscape (Nigeria Data Protection Commission, n.d.).

VI. THE FUTURE OF DIGITAL PRIVACY IN NIGERIA: AI GOVERNANCE, CYBERSECURITY, AND GLOBAL DATA FLOWS

AI Governance and Data Protection

Artificial Intelligence (AI) poses complex challenges for data protection regimes globally. While the NDPA provides a foundation for data rights, it does not address AI-specific concerns such as algorithmic bias, automated profiling, or explainability obligations (Nigeria Data Protection Act, 2023). As AI applications expand across sectors like finance, health, and public service, the lack of statutory AI governance in Nigeria exposes data subjects to unchecked algorithmic decisions (Awofadeju et al., 2024).

The European Union's proposed AI Act offers a robust model by classifying AI systems according to risk and imposing proportionate compliance duties. Nigeria could adapt a similar risk-tiered framework, enabling proactive oversight of high-risk AI deployments (Olatunji, 2022). Moreover, a dedicated AI regulatory body, empowered to audit algorithms, issue ethical guidance, and review high-stakes use cases, would provide sectoral clarity and support regulatory convergence with global norms (Adeyemi & Umeh, 2023).

Algorithmic accountability remains an unresolved policy frontier. Legal remedies for individuals adversely affected by AI-driven decisions especially in loan approvals or policing must be codified to protect fundamental rights. The U.S. AI Bill of Rights draft, for instance, offers enforceable standards on transparency and redress. Nigeria must urgently legislate equivalent protections to forestall the entrenchment of opaque, biased, and unchallengeable AI systems (Idowu, 2022).

Cybersecurity and Data Protection Enforcement

Cybersecurity and data protection are intrinsically linked, yet Nigeria's institutional framework treats them as separate silos. Although the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 laid a legislative foundation, enforcement has lagged. Ransomware, identity theft, and phishing attacks have surged, exacerbated by regulatory fragmentation and a lack of centralized data security oversight (Akintunde, 2022).

The NDPC has data protection authority but lacks the infrastructure and legal mandate to coordinate national cybersecurity standards. A dedicated cybersecurity compliance agency, modelled on the EU's NIS2 Directive, could bridge this gap. Such an agency would impose

sector-specific controls, require breach notifications, and mandate periodic risk assessments (KPMG, 2023). Nigeria's current model does not incentivise cybersecurity by design, thereby exposing digital ecosystems to persistent vulnerabilities.

Additionally, penalty regimes for security lapses remain weak. Most breaches go unreported, and existing fines are neither dissuasive nor consistently applied (Awofadeju et al., 2024). Drawing on GDPR's mandatory breach notification rules and punitive fine structures would encourage disclosure, enhance consumer trust, and reduce regulatory arbitrage. Nigeria must embed enforceable cybersecurity obligations into data protection policies to close this persistent enforcement gap (Ekanem, 2023).

Global Data Flows and Adequacy Recognition

Global data flows are essential for Nigeria's digital trade integration, yet the country remains excluded from the European Commission's list of data-adequate jurisdictions. This hinders international data exchange and limits competitiveness in transnational digital services (Ekanem, 2023). Nigeria's path to adequacy must focus on strengthening legal redress, consistency in regulatory interpretation, and limiting excessive government surveillance three core criteria evaluated by the EU.

The NDPA's provisions on cross-border data transfers rely on "adequate protection" and allow for the use of SCCs and BCRs, echoing the GDPR structure (Nigeria Data Protection Act, 2023). However, adequacy requires institutional maturity, public accountability, and evidence of operational compliance. Regulatory discretion, if unchecked, may jeopardize trust from international partners and foreign investors (Hogan Lovells, 2023).

Another barrier is Nigeria's handling of government surveillance and data localization. Broad state access to data, without clear legal thresholds or independent oversight, risks violating international privacy expectations (Bolarinwa, 2022). Nigeria must institute judicial review systems for surveillance authorisations and limit data localization mandates to necessary and proportionate circumstances. Transparency reports, modelled after those in democratic jurisdictions, would enhance oversight and bolster international legitimacy (Bolarinwa et al., 2023).

VII. Conclusion

The Nigeria Data Protection Act (NDPA) represents a watershed moment in the country's effort to institutionalize digital privacy, but its practical impact will depend on how effectively it is enforced, resourced, and adapted to emerging global risks. The creation of the Nigeria Data

Protection Commission (NDPC) addresses the enforcement vacuum left by the Nigeria Data Protection Regulation (NDPR), granting the regulator powers to investigate, audit, and sanction. However, systemic issues such as political interference, budgetary opacity, and judicial inefficiencies continue to undermine the full realization of these powers (Nigeria Data Protection Act, 2023; Idowu, 2022; Bolarinwa et al., 2023).

The NDPA's alignment with global best practices through provisions on cross-border data transfers, data subject rights, and corporate accountability marks significant progress, yet important gaps remain. For example, the absence of clearly defined thresholds for high-risk processing, and weak integration of cybersecurity and AI governance frameworks, highlight the need for regulatory refinement (KPMG, 2023; Akintunde, 2022; Olatunji, 2022). As countries like the UK, EU, and Kenya consolidate their regulatory regimes with sector-specific enforcement strategies and risk-based oversight, Nigeria must adopt similarly nuanced approaches to avoid regulatory fragmentation and enhance investor confidence (Ekanem, 2023; Hogan Lovells, 2023).

Nigeria’s aspiration for EU adequacy recognition and stronger participation in global data flows will remain elusive unless it strengthens judicial review mechanisms, ensures the operational independence of the NDPC, and curtails excessive government surveillance. Equally important is the need to institutionalize AI governance with transparency and accountability mandates and establish a centralised cybersecurity compliance framework to mitigate the growing threats of ransomware, identity theft, and algorithmic discrimination (Awofadeju et al., 2024; Tade & Umeh, 2023).

To consolidate its status as a digital leader in Africa, Nigeria must now prioritise risk-based, future-facing policy reforms that blend innovation with human rights protections. This requires an integrated approach anchored in institutional resilience, civic engagement, and transnational cooperation to make digital privacy not only a statutory mandate but a lived reality for individuals and businesses alike.

*****

 [ISSN 2581-5369]

VIII. REFERENCE

1. Awofadeju, M.O., Fonkem, B., Akinola, O., Olaniyan, O.R., Fadeke, A.A. and Olola, T.M., 2024. Strategies for mitigating cybersecurity challenges to fund management in the digitalized real estate industry. *Magna Scientia Advanced Research and Reviews*, 11(1), pp.385–398.
2. Bolarinwa, I., 2022. Fictitious yet Accountable: The Role of Civil Societies in Ensuring Accountability of Government Credits. *Ikogho: Education, Social Sciences, Sciences, Humanities & Management Sciences Journal*, 21, pp.1–15.
3. Bolarinwa, I.S., Olola, T., Awofadeju, M. and Fonkem, B., 2023. The Death of Whistleblowing Policies in Nigeria and How It Entrenches Corruption and Financial Misappropriation. *Iconic Research and Engineering Journals*, 7(6), pp.376–389.
4. Ekanem, J., 2023. Cross-Border Data Transfers Under the NDPA: Implications for International Trade. *West African Law Review*, 8, pp.98–112.
5. Femi Akintunde, 2022. Data Protection in Nigeria: Challenges and Prospects Under the NDPR. *African Journal of Cyber Law*, 4, pp.78–91.
6. Hogan Lovells, 2023. *Key Changes Brought by the Nigerian Data Protection Act, 2023*. Available at: https://www.hoganlovells.com/en/publications/key-changes-brought-by-the-nigerian-data-protection-act-2023.
7. Idowu, A., 2022. Data Protection and Privacy Rights in Nigeria: Evaluating the Enforcement Deficits of the NDPR. *International Journal of Technology Law*, 7, pp.23–38.
8. KPMG International, 2023. *The Nigeria Data Protection Act, 2023: Implications for Businesses and Compliance Strategies*. Available at: https://assets.kpmg.com/content/dam/kpmg/ng/pdf/thenigeria-data-protection-act-2023.pdf.
9. Michael Olatunji, 2022. Aligning Nigeria's Data Protection Framework with Global Standards: The Road from NDPR to NDPA. *African Journal of Business and Digital Law*, 5, pp.30–48.
10. Nigeria Data Protection Act, 2023 (Nig.). Available at: https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf [Accessed 6 May 2025].
11. Nigeria Data Protection Commission, n.d. *About Us*. Available at: https://ndpc.gov.ng/about-us/ [Accessed 6 May 2025].
12. Tade Adeyemi and Chidi Umeh, 2023. *The Nigeria Data Protection Act: Advancing Regulatory Frameworks in a Digital Economy*.

 [ISSN 2581-5369]