AUN JOURNAL OF LAW
https://journals.aun.edu.ng/index.php/aunijl

DATA PRIVACY AND CONSUMER PROTECTION IN NIGERIA'S DIGITAL ECONOMY: A LEGAL EXAMINATION OF THE NIGERIA DATA PROTECTION ACT, 2023

A.I. Uwadinma,
[a]Admiralty University of Nigeria
[a] Department, of Jurisprudence and International Law, Faculty of Law, Admiralty University of Nigeria, Delta State

[a*]*Corresponding author email*: alex.uwadinma-law@adun.edu.ng

ABSTRACT

This article critically examines the Nigeria Data Protection Act (NDPA), 2023 as a legislative response to growing concerns about data privacy and consumer protection within Nigeria's rapidly evolving digital economy. Against the backdrop of increasing reliance on digital platforms and personal data, the study explores how the NDPA addresses systemic risks to consumer rights, such as data breaches, unauthorized processing, and identity theft. Adopting a doctrinal research methodology, the article analyzes the Act's legislative and regulatory framework, highlights its key provisions—such as lawful basis for data processing, rights of data subjects, cross-border data transfer rules, and the establishment of the Nigeria Data Protection Commission (NDPC)—and evaluates their impact on consumer protection. The paper further provides a comparative assessment of the NDPA against global data protection benchmarks, particularly the European Union's General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). Key challenges identified include institutional limitations, lack of public awareness, inadequate cybersecurity infrastructure, and regulatory gaps regarding emerging technologies. To enhance the NDPA's effectiveness, this article recommends strategic reforms, such as strengthening the NDPC, expanding public education, refining legal provisions on data subject rights, and fostering regional and international collaboration. This study concludes that while the NDPA marks a significant milestone in Nigeria's data governance landscape, sustained implementation efforts are necessary to protect consumer rights and build a trustworthy digital ecosystem.

Keywords*:* Consumer Rights, Data Privacy, Digital Economy, Nigeria Data Protection Act 2023, Regulatory Compliance/Enforcement.

1. INTRODUCTION AND CONTEXTUAL BACKGROUND

Nigeria's digital economy has expanded rapidly in recent years, driven by fintech, e-commerce, social media, and a booming mobile market. The country now has Africa's largest mobile subscriber base (over 219 million) and more than 163 million internet users, illustrating the vast scale of personal data in circulation.[1]

[1] A Agbeyangi, A Makinde and I Odun-Ayo**,** 'Nigeria's ICT and Economic Sustainability in the Digital Age' (2024) <https://arxiv.org/abs/2401.03996> accessed 15 April 2025.

This growth has transformed data into a valuable commodity but also heightened risks of data breaches, identity theft, and misuse of consumer information. Historically, Nigeria lacked a comprehensive data protection law, leaving consumers vulnerable to unauthorized data collection and cybercrimes. While the 1999 Constitution guarantees a right to privacy, detailed legislation was lacking, and earlier initiatives like the Nigeria Data Protection Regulation (NDPR), 2019, were limited in scope.[2] In response to mounting concerns and to build trust in the digital marketplace, the Nigeria Data Protection Act, 2023 (NDPA) was enacted in June 2023.[3]The NDPA represents Nigeria's first comprehensive data privacy framework, aiming to safeguard individuals' data and align the country's regulations with global standards such as the General Data Protection Regulation (GDPR) of the European Union (EU).[4]Enshrining this framework marked a significant milestone in protecting consumer rights in Nigeria's digital economy, but questions remain about the Act's effectiveness and implementation.

2. LEGISLATIVE AND REGULATORY FRAMEWORK

2.1. Evolution of Data Protection Law in Nigeria: Before 2023, Nigeria's data protection administration consisted of piecemeal regulations and policies. The NDPR (2019) issued by the National Information Technology Development Agency (NITDA) was an important step towards formalizing data privacy rules, and the Nigeria Data Protection Bureau (NDPB) was created in 2022 to begin oversight.[5] However, these measures lacked comprehensive legislation and enforceability. Stakeholders advocated a stronger legal foundation to address emerging privacy challenges in the digital economy.[6] The NDPA, 2023 was formulated on 14 June 2023 and signed into law to provide a statutory basis for data protection. Crucially, the Act established the Nigeria Data Protection Commission (NDPC), replacing the interim NDPB, as the dedicated

[2] D Agboola, 'Data Privacy and Protection in Nigeria – Legal Developments' (2025) <https://ssrn.com/abstract=5191489> accessed 15 April 2025.

[3] O Babalola**,** 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' *British Journal of Cyber Criminology* (2024) 3(1) 106.

[4] B Anifowoshe**,** 'Data Privacy Laws in Nigeria: A Comprehensive Guide to NDPA 2023' (2024) <https://justunsecure.com/data-privacy-laws-in-nigeria-a-comprehensive-guide/> accessed 15 April 2025.

[5] Olaniwun Ajayi LP**,** 'Doing Business in Nigeria: 2023 Annual Report' (2023) <https://2023annualreports.olaniwunajayi.net/> accessed 15 April 2025.

[6] AT Oyewole and others**,** 'Data Privacy Laws and Their Impact on Financial Technology Companies: A Review'*Computer Science & IT Research Journal* (2024) 5(3)628–650.

regulator to enforce data protection laws.[7] The NDPA is structured into twelve parts, covering the establishment and powers of the Commission, data protection principles, the obligations of data controllers/processors, rights of data subjects, registration requirements, enforcement mechanisms, and remedies.[8] It explicitly supersedes inconsistent provisions of prior laws or guidelines, ensuring that the NDPA is now the primary authority on data privacy in Nigeria. With proposed regulations and guidelines under the Act, this legislative framework is intended to strengthen the legal foundations of Nigeria's digital economy and uphold citizens' constitutional privacy rights.[9]

3. KEY PRINCIPLES AND PROVISIONS OF THE NDPA, 2023

3.1. Principles-Based Approach: The NDPA adopts a principles-based approach to personal data processing, emphasizing fundamental ideals of transparency, lawfulness, and accountability.[10] Data must be collected for specified, legitimate purposes and processed in a fair and responsible manner consistent with those purposes. These principles echo international norms, reflecting the influence of frameworks, like the GDPR, in shaping the Act's core tenets.

3.2. Rights of Data Subjects: The Act grants individuals (data subjects) a suite of enforceable rights over their data. Key rights include the right to access personal information held by data controllers, to rectify inaccuracies, and to erase data that are no longer necessary or were unlawfully obtained.[11] Data subjects must give consent for data processing and have the right to withdraw consent at any time. They can also object to certain forms of data processing and are protected from adverse decisions made solely on automated processing of their data.[12] These provisions empower consumers by giving them greater control

[7] JO Effoduh and OF Odeh**,** *Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens* (2024) https://accountabilitylab.org/wp-content/uploads/2024/01/Strengthening-Data-Protection.pdf>.

[8] G Akhihiero, E Okhiai and O Elesho, 'Blockchain and Data Protection by Design: An Examination of the NDPA's Provisions and Best Practices' (2024) <https://ssrn.com/abstract=4931988> accessed 15 April 2025.

[9] DLA Piper, 'Data Protection Laws of the World: Nigeria' (2025) <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law> accessed 15 April 2025.

[10] IS Nwankwo, 'Strengthening Nigeria's Cyber Frontier: Building Cybersecurity Resilience through Legal Innovation' *The Commonwealth Cyber Journal*, (2025) 27.

[11] The Firma Advisory, 'The Rights of Data Subjects under the Nigeria Data Protection Act: Empowering Individuals in the Digital Age' (2024) https://thefirmaadvisory.com/new-blog/2024/1/29/the-rights-of-data-subjects-under-the-nigeria-data-protection-act-empowering-individuals-in-the-digital-age accessed 15 April 2025.

[12] *Ibid.*

and autonomy over how their personal information is used, mirroring many of the protections found in the GDPR.

3.3. Obligations of Data Controllers and Processors: The NDPA imposes strict duties on entities that collect or handle personal data. Controllers and processors must obtain explicit, informed consent from individuals before using their data, and processing must have a lawful basis.[13] They are required to implement robust security measures to prevent unauthorized access, breaches, or misuse of personal data. For high-risk data activities, organizations should conduct Data Protection Impact Assessments (DPIAs) to evaluate and mitigate potential privacy risks.[14] There is also an emphasis on data minimization and purpose limitation; only necessary data should be collected and used, and only for the purposes communicated to the data subject. Importantly, controllers bear accountability for compliance and can be held liable for the actions of processors acting on their behalf.

3.4. Cross-Border Data Transfers: In an era of cloud computing and global data flows, the NDPA regulates international transfers of personal data. The Act restricts the transfer of personal data to foreign jurisdictions unless the destination country or international organization ensures an "adequate" level of data protection comparable to Nigeria's.[15] This provision aimsto protect Nigerian consumers' data when it is transmitted overseas and address concerns over data sovereignty and exposure to weaker privacy regimes. However, the Act does not clearly define what constitutes "adequate" protection in a foreign jurisdiction, leaving this determination to the regulator's assessment or future regulations. Companies engaging in cross-border data processing must therefore carefully evaluate the legal standards of recipient countries or use safeguard mechanisms (such as contracts or international agreements) to comply with this requirement.[16]

3.5. Enforcement and Sanctions: The NDPA introduces penalties for violations to incentivize compliance. Organizations that breach data protection obligations or individuals' rights under the Act can face administrative fines and other sanctions. The NDPC is empowered to investigate complaints and infractions, and to impose corrective measures or monetary penalties on erring data controllers and

[13] R Walters**,** *Controller, Consent, Processing* in *Cybersecurity and Data Laws of the Commonwealth: International Trade, Investment and Arbitration* (Singapore, Springer Nature Singapore 2023) 119–146.

[14] H JPandit**,** 'A Semantic Specification for Data Protection Impact Assessments (DPIA)' in *Towards a Knowledge-Aware AI* (IOS Press, 2022) 36–50.

[15] PC Aloamaka**,** 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms' *UCC Law Journal* (2025) 4(2) 242–263.

[16] MI Khan, 'Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices' *American Journal of Scholarly Research and Innovation* (2025) 4(1)138–174.

processors.[17]

While the Act provides for punitive fines, they are *relatively* modest compared to the GDPR's penalty regime (which can reach up to €20 million or 4% of global annual turnover).[18] Nonetheless, the introduction of fines and legal liability in Nigeria is expected to deter negligent data practices and encourage businesses to prioritize data protection compliance.

4. CONSUMER PROTECTION DIMENSIONS

At its core, the NDPA, 2023 is a consumer protection statute tailored for the digital age. It seeks to ensure that individuals as consumers of digital services are not powerless over their personal information. By legally requiring organizations to respect privacy rights, the Act boosts consumer confidence in digital transactions.[19] One key dimension is empowerment: consumers now have enforceable rights to access and correct their data, to be informed about how their data is used, and to demand the deletion or withdrawal of consent, thus putting meaningful control back in users.[20] These rights, coupled with requirements for transparency (e.g., clear privacy notices and obtaining informed consent), mean consumers should no longer be kept in the dark about data practices.

Another critical consumer protection aspect is the remedy and redress framework. The NDPA provides avenues for individuals to lodge complaints with the NDPC and seek redress if their data is misused or their privacy is violated.[21] The Act's objective explicitly includes providing means of recourse and remedies if an individual's data right is breached. The inclusion is a significant development in a jurisdiction where, previously, victims of data abuse had little practical recourse. Under the new law, a consumer whose personal data is exposed or mishandled can report the incident, triggering a regulatory investigation and potential sanctions against the offending party, as well as compensation for harm suffered where appropriate.[22]

The NDPA's provisions also aim to foster trust in Nigeria's digital economy. When consumers know that robust legal safeguards exist and that businesses are accountable for protecting personal data, they are more

[17] O Babalola**,** 'Data Protection Compliance Organizations (DPCO) Under the NDPR, and Monitoring Bodies Under the GDPR: Two Sides of the Same Compliance Coin?' *Global Privacy Law Review* (2022) 3(2).

[18] NDPA 2023, s 51.

[19] Nigeria Data Protection Act 2023, ss 25–27.

[20] Nigeria Data Protection Act 2023, ss 34–38.

[21] JA Nwobike**,** 'Unresolved Tensions in the Intersections of Corporate Insolvency, Data Protection and Conflict of Laws under the Nigerian Legal Framework' *Beijing Law Review* (2025) 16(1)1–28.

[22] JA Nwobike, *ibid.*

likely to engage with online services and digital commerce.[23] This increased trust can have broader economic benefits, encouraging innovation and investment. In this sense, data protection is not viewed in isolation but as a catalyst for consumer confidence and market growth. However, the impact on consumer protection will ultimately depend on effective enforcement and public awareness. Many Nigerians are still unaware of their new rights under the Act, and enforcement mechanisms will need to be visible and effective to truly change corporate behavior and protect consumers.[24] Thus, while the NDPA establishes a strong legal foundation for consumer data privacy, continuous efforts on implementation are required to translate these legal protections into real-world consumer benefits.

5. INSTITUTIONAL AND ENFORCEMENT MECHANISMS

A cornerstone of the NDPA, 2023 is the creation of a dedicated regulatory authority to oversee data protection. The Act establishes the Nigeria Data Protection Commission (NDPC) as the supervisory and enforcement body;[25]this Commission effectively replaces the interim NDPB and inherits its duties.[26] The NDPC is empowered to monitor compliance, issue regulations and guidelines, verify that organizations adhere to the Act's provisions, and sanction those who do not. It has the authority to conduct investigations, either proactively or in response to complaints, and can order data controllers to take corrective actions or cease operations that violate the law. Critically, the Commission can impose administrative fines for non-compliance, adding financial consequences to legal breaches.[27]

5.1. Enforcement Procedures: Under the Act, data controllers and processors may be required to register with the NDPC, particularly those of "major importance" (e.g., large-scale data processors), to facilitate oversight.[28] The Commission can audit organizations' data processing activities and require periodic compliance reports.[29] In cases of data breaches, the NDPA mandates notification. Organizations must report

[23] OP Olebara, E Okpara and KG Onyegbule**,** 'Data Protection and Consumer Rights in Electronic Commerce in Nigeria: A Legal Appraisal' *African Journal of Law and Human Rights*(2025) 9(1).

[24] AA Aliyu**,** 'Corporate Responsibility and Data Privacy in Nigeria: Legal Obligations and Best Practices' (2024) <https://ssrn.com/abstract=5004000> accessed 15 April 2025.

[25] Nigeria Data Protection Act 2023, s 4.

[26] Nigeria Data Protection Act 2023, s 64.

[27] Nigeria Data Protection Act 2023, ss 6, 48, 49, and 62.

[28] Nigeria Data Protection Act 2023, ss 44 and 65.

[29] Nigeria Data Protection Act 2023, ss 48 and 49.

serious

personal data breaches to the NDPC and, in certain cases, inform affected individuals, ensuring that consumers are made aware of incidents that could impact their privacy or security.[30] The NDPC also serves as the arbiter of data complaints. If an individual files a complaint about a company's data handling, the Commission will investigate and can adjudicate the matter, providing an accessible form of justice outside the court system.[31]

5.2. Challenges for the Regulator: While the NDPC's establishment is pivotal, its effectiveness hinges on capacity and resources. Ensuring the Commission's independence and adequate funding is essential. Without sufficient budget, staffing, and technical expertise, the NDPC may struggle to perform nationwide monitoring or penalize large corporations that violate the law.[32] Moreover, unlike the GDPR's ecosystem where each EU member state has a well-resourced Data Protection Authority, Nigeria's NDPC is a single national body that must oversee a vast economy with millions of data processing entities. The Act grants NDPC broad powers, but building institutional strength will be a gradual process.[33] Another enforcement mechanism, as noted, is the penalty regime. The NDPA authorizes fines for violators, which signals to businesses that non-compliance has tangible consequences. However, if fines are too low or enforcement actions infrequent, they may not be a strong deterrent.[34] Comparatively, the GDPR's success has been aided by high-profile fines and strict enforcement by authorities across Europe, a benchmark Nigeria will need to approach by empowering its Commission.[35]

In summary, the NDPA's institutional and enforcement framework is designed to operationalize the law through the NDPC's oversight and sanctions. It is a significant improvement over the past, where enforcement was weak or ad hoc. The focus now will be on ensuring that this framework is robust in practice, that the Commission can actively police compliance, that organizations take their new obligations seriously, and that consumers begin to see enforcement outcomes that vindicate their rights.

[30] Nigeria Data Protection Act 2023, s 40.

[31] Nigeria Data Protection Act 2023, s 46.

[32] AP Uwemedimo**,** *An Analysis of the Legal and Ethical Issues on the Use of Biometric Data in Contemporary Nigerian Society* (PhD Thesis, Faculty of Law, University of Uyo 2024).

[33] AL Gray and F Suleman**,** 'Unpacking the Process of Developing South Africa's National Drug Policy – Lessons for Universal Health Coverage' *Journal of Pharmaceutical Policy and Practice* (2024) 17(1)2376349.

[34] Nigeria Data Protection Act 2023, ss 48 and 49.

[35] MNI Khan**,** *op cit.*

6. COMPARATIVE PERSPECTIVE: GDPR AND POPIA

Nigeria's NDPA, 2023 draws inspiration from international data protection regimes, most notably the EU's General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). A comparative look at these frameworks highlights both the NDPA's alignment with global best practices and the areas where it falls short.

6.1. Comparison with the GDPR: Since the enforcement of GDPR in 2018, it is often regarded as the gold standard for data protection law, and the NDPA mirrors many of its features. For instance, the NDPA has an extraterritorial scope similar to the GDPR – it applies not only to Nigerian-based entities but also to foreign organizations processing data of individuals in Nigeria, which is analogous to the GDPR's reach beyond Europe.[36] Both laws anchor personal data processing in core principles like transparency, purpose limitation, and data minimization, and both grant fundamental rights to data subjects (access, correction, erasure, etc.). However, the NDPA omits or only partially covers some rights present in the GDPR. Notably, it does not explicitly include a right to data portability, the ability for individuals to obtain and reuse their data across different services which the GDPR guarantees.[37] The NDPA also lacks a clear equivalent to the GDPR's right to object to automated decision-making and profiling, though it does state that individuals should not be subject to decisions based solely on automated processing in certain circumstances.[38] In terms of enforcement mechanisms, both laws establish independent regulators (the NDPC in Nigeria and Data Protection Authorities in EU states) to oversee implementation. However, the GDPR's enforcement framework is more developed. Itfeatures cooperation among EU regulators and the European Data Protection Board and authorizes much heavier penalties. The GDPR allows fines up to 4% of a company's global turnover or €20 million, far exceeding the fines enshrined in the NDPA.[39] This stark difference in sanction severity means the GDPR exerts stronger pressure on companies to ensure compliance. Additionally, the GDPR mandates proactive measures, like appointing Data Protection Officers in certain cases and performing DPIAs for high-risk processing, areas where the NDPA's requirements are less explicit or

[36] JO Effoduh**,** *Towards the Implementation of Data Protection Measures to Safeguard Against Surveillance Abuse in Nigeria* (2024) <https://accountabilitylab.org/wp-content/uploads/2024/01/Towards-the-implementation-of-Data-Protection-Measures-to-Safeguard-Against-Surveillance-Abuse-in-Nigeria.pdf> accessed 15 April 2025.

[37] O Babalola**,** *op cit.*

[38] E Salami and I Nwankwo**,** 'Regulating the Privacy Aspects of Artificial Intelligence Systems in Nigeria: A Primer' *African Journal on Privacy and Data Protection* (2024) (1) 220–247.

[39] CU Agbedo**,** 'Protecting Nigerians from Data Breaches' *Business Day* (2025) <https://businessday.ng/opinion/article/protecting-nigerians-from-data-breaches/> accessed 15 April 2025.

comprehensive

.[40] Overall, although the NDPA aligns broadly with the GDPR, it is narrower in scope on some consumer rights and less enforceable, reflecting the nascent state of Nigeria's data protection regime.

6.2. Comparison with South Africa's Protection of Personal Information Act (POPIA): South Africa's POPIA (effective 2021) offers a regional point of comparison, sharing similarities with Nigeria's law but also some instructive differences. Like the NDPA, POPIA is principles-based, emphasizing accountability, transparency, and lawful processing of personal data by those who collect and use it.[41] Both laws restrict cross-border data transfers to countries with adequate protection and seek to uphold data subject rights in their respective jurisdictions. A key area of divergence is the level of detail and guidance. POPIA provides more explicit rules on certain issues. For example, it contains detailed provisions on processing children's data and on handling special categories of sensitive data (such as biometric and health information), including requiring authorization or additional safeguards for such processing.[42] The NDPA, by contrast, is comparatively vague on these points; it defines some categories of sensitive data but does not stipulate distinct handling requirements beyond the general obligations, potentially leaving gaps in protection for especially sensitive information.[43] In terms of institutional enforcement, POPIA established an information regulator as an independent authority with clear powers to enforce compliance and penalize offenders (similar to Nigeria's NDPC).[44] One practical difference is that the South African regulator has been active in conducting public awareness and campaigns mandated by law to ensure that citizens understand their data protection rights. POPIA explicitly emphasizes outreach and literacy, whereas Nigeria's NDPA does not contain strong provisions for public awareness[45]. This lacuna is significant given Nigeria's context, where digital literacy is uneven. The lack of a statutory mandate for educating campaigns under NDPA could slow down public uptake of the new rights. Additionally, POPIA requires a written contract when

[40] PC Aloamaka, *op cit.*

[41] MNI Khan, *op cit.*

[42] C Staunton and others, 'Protection of Personal Information Act 2013 and Data Protection for Health Research in South Africa' *International Data Privacy Law*, (2020) 10(2) 160–179.

[43] CI Ewulum**,** *The Legal Regime for Cross-Border Data Transfer in Africa: A Critical Analysis* (2023) <https://ssrn.com/abstract=4546964> accessed 25 May 2025.

[44] JO Effoduh and OF Odeh, *Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens* (2024) <https://accountabilitylab.org/wp-content/uploads/2024/01/Strengthening-Data-Protection.pdf> accessed 26 May 2025.

[45] D Eke and others, *Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs* (2022) Centre for the Study of African Economies (CSEA) <https://cseaafrica.org/images/posts/8194277452151253.pdf> accessed 26 May 2025.

transferring

personal data to third parties in other countries to ensure continued protection.[46] The NDPA's cross-border transfer rule, while conceptually similar, does not provide such specific guidance (e.g., it does not expressly require contractual guarantees for foreign transfers), which could lead to uncertainty in application.

6.3. Lessons and Best Practices: The comparative analysis suggests several lessons for Nigeria. From the GDPR, Nigeria can consider incorporating additional consumer rights (like data portability and stronger rights regarding automated profiling) to enhance individuals' control over their data. From both GDPR and POPIA, Nigeria could adopt more rigorous enforcement measures, for instance, increasing the maximum fines or granting the NDPC more autonomy and resources, to more closely match the deterrent effect seen in the EU.[47] POPIA's example highlights the importance of public awareness initiatives and clearer operational guidelines, embedding requirements for the regulator to educate businesses and consumers, and clarifying ambiguous areas such as cross-border transfer procedures, would strengthen the NDPA's effectiveness. In essence, while the NDPA is largely aligned with international norms, fine-tuning it by learning from these other frameworks could close the gaps and improve its implementation.

7. CHALLENGES AND GAPS IN THE NDPA 2023

Despite the laudable step of enacting the NDPA, there are significant challenges and gaps that may hinder its effectiveness in practice. These issues span institutional capacity, public awareness, technological coverage, and legal clarity:

7.1 Institutional Capacity and Enforcement: The Nigeria Data Protection Commission faces resource and capacity constraints that could undermine enforcement. The NDPC is a new agency and is currently underfunded and understaffed relative to its broad mandate.[48] This raises concerns about its ability to conduct nationwide monitoring and enforce compliance across Nigeria's vast digital landscape. Ensuring the Commission's independence from political influence is another challenge, sustained autonomy is needed for impartial enforcement, yet there are questions about how insulated the NDPC is, given that it succeeds a bureau that was under a federal ministry. Additionally, enforcement reach is limited, unlike the EU which has a network of regulators, Nigeria has a single centralized authority, and it may struggle to oversee data

[46] J Coetzee**,** 'Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision'*Potchefstroom Electronic Law Journal* (2024) 27 1–29. <https://perjournal.co.za/article/view/15234> accessed 26 May 2025.

[47] OJ Effoduh and OF Odeh**,** *op cit.*

[48] Nigeria Data Protection Commission**,** 'NDPC Presents 2024 Performance, 2025 Plans to Ministerial Task Team' (25 March 2025) <https://ndpc.gov.ng/2025/03/25/ndpc-presents-2024-performance-2025-plans-to-ministerial-task-team/> accessed 26 May 2025.

practices in all sectors and regions. Without decentralized offices or significant expansion, there's a risk of patchy enforcement, especially in remote or rural areas.

7.2 Public Awareness and Compliance Culture: A foundational challenge is the low level of awareness about data protection rights and obligations in Nigeria. Many consumers are not informed of their rights under the NDPA; for example, large segments of the population (particularly in rural communities) do not know that they can request access to their data or demand its deletion.[49] This awareness gap means the rights established on paper may not be exercised in practice, limiting the Act's impact. On the business side, many organizations (especially small and medium-sized enterprises) are either unaware of the new law or view compliance as a low priority and an extra cost. The concept of corporate data responsibility is still nascent; without efforts to educate and incentivize companies, compliance may remain superficial. Furthermore, Nigeria's socio-economic context plays a role, pressing economic concerns can overshadow data privacy issues, both for individuals (who may prioritize basic needs over privacy) and for policymakers.

7.3 Technological and Infrastructural Barriers: Nigeria's digital and cybersecurity infrastructure is still developing, which complicates the implementation of data protection measures. Cybersecurity weaknesses mean that even with legal requirements in place, many organizations might lack the technical capacity to secure personal data against breaches. There is also a regulatory gap regarding emerging technologies. The NDPA does not comprehensively address new data-driven technologies such as artificial intelligence (AI), machine learning, and blockchain. These technologies pose novel privacy challenges – for instance, automated decision-making systems can profile consumers in ways not anticipated by older laws.[50] The Act's silence or ambiguity on these issues could leave consumers unprotected against harms from AI-driven services. While Section 37 of the Act[51] provides that individuals should not be subject to purely automated decisions that significantly affect them, the NDPA offers limited guidance on how this right is applied or enforced. Overall, the law's treatment of cutting-edge technologies is seen as underdeveloped. Likewise, the criteria for cross-border data transfer adequacy are not clearly defined, creating uncertainty for companies engaged in global data flows. Without detailed regulations or agreements in place, determining

[49] G Akhihiero, E Okhiai and O Elesho**,** *Blockchain and Data Protection by Design: An Examination of the NDPA's Provisions and Best Practices* (30 May 2024) <https://ssrn.com/abstract=4931988> accessed 26 May 2025.

[50] H Ijaiya**,** 'Harnessing AI for Data Privacy: Examining Risks, Opportunities and Strategic Future Directions' *International Journal of Science and Research Archive* 2878–2892. (2024) 13(2) <https://ijsra.net/sites/default/files/IJSRA-2024-2510.pdf> accessed 26 May 2025.

[51]National Data Protection Act, 2023.

which

countries are "safe" for Nigerian data is a challenge, potentially hindering international business or leading to inconsistent decisions.[52]

7.4 Judicial and Legal Framework Challenges: As a newly minted law, the NDPA has yet to be tested in Nigerian courts. There is a lack of judicial precedents interpreting its provisions, which means uncertainty looms over how certain clauses will be applied in practice. It will take time for case law to develop clarifying the Act's scope and the balance of rights (e.g., how will courts handle conflicts between data protection and freedom of expression or national security exceptions?). Additionally, the Nigerian judiciary faces well-known issues of slow adjudication and case backlogs. Data protection disputes, if routed through the courts, could take years to resolve, which would discourage individuals from seeking legal redress and weaken enforcement.[53] Another legal gap is the limited technical expertise among judges and legal practitioners regarding data privacy and technology. Capacity-building in the judiciary is needed so that judges can competently handle complex data protection cases; without it, enforcement via the courts may be ineffective or inconsistent.

7.5 Gaps in the Legislation's Substance: Several substantive gaps in the NDPA itself have been identified by commentators. One is the absence of certain rights. For example, the Act does not explicitly provide the right to data portability that would allow consumers to easily transfer their data between service providers, a right standard in the GDPR. Another gap is in addressing automated decision-making, while, as noted, the Act acknowledges the issue, it stops short of detailed regulation or explicit rights to human review of automated decisions, potentially leaving consumers vulnerable to opaque algorithmic practices. The Act also does not differentiate strongly between sensitive and non-sensitive personal data in terms of protections. It defines some categories of sensitive data (such as data on health, genetics, ethnicity, etc.), but unlike some jurisdictions that impose stricter rules or higher consent standards for sensitive data, the NDPA's provisions remain largely uniform for all personal data.[54] This could be problematic given the greater harm that can result from misuse of sensitive information. Moreover, certain obligations and enforcement procedures in the Act lack clarity; for instance, how the NDPC should practically enforce fines, especially against large

[52] IS Nwankwo, 'Cross-Border Health Data Transfers from Nigeria: Navigating the Legal and Ethical Landscape' in M Corrales Compagnucci and M Fenwick (eds), *International Transfers of Health Data: A Global Perspective* (Springer Nature Singapore 2024) 195–218. <https://doi.org/10.1007/978-981-97-9983-1_10> accessed 26 May 2025.

[53] MB Adisa**,** 'An Overview of Legal Recourse for Data Privacy Violations in Nigeria' (21 August 2024) *The Trusted Advisors*<https://trustedadvisorslaw.com/an-overview-of-legal-recourse-for-data-privacy-violations-in-nigeria/> accessed 26 May 2025.

[54] AE Adaji**,** 'Reconciling the Ideals of Open Science with Data Privacy in the Context of Health Research in Nigeria: A Legal Analysis' *Research Square* (2023) rs.3.rs-3293485 <https://doi.org/10.21203/rs.3.rs-3293485/v1> accessed 26 May 2025.

multinational

tech companies, or how quickly organizations must respond to data subject requests, are areas that would benefit from more detailed regulations. The NDPA will likely require subsidiary legislation (regulations, guidelines) to fill in these details, but until those are developed, ambiguity exists.[55] In summary, while the NDPA lays a solid foundation, these challenges and gaps must be addressed to ensure the law truly safeguards consumers as intended.

8. RECOMMENDATIONS FOR EFFECTIVE IMPLEMENTATION

To strengthen Nigeria's data protection regime and address the challenges identified, a number of strategic steps are recommended:

8.1 Strengthen the Nigeria Data Protection Commission (NDPC): Provide the NDPC with substantially greater funding, skilled human resources, and technical tools. A well-resourced NDPC will be better equipped to conduct investigations and audits and guide organizations in compliance. Measures should be taken to guarantee the Commission's independence (for example, fixed-term appointments for its leadership and financial autonomy) to insulate it from political influence.[56] Establishing regional offices or liaison units across Nigeria could extend the NDPC's reach, enabling more effective oversight in various states and localities.

8.2 Enhance Public Awareness and Education: Launch nationwide education and awareness campaigns about data protection rights and obligations. Government agencies, in partnership with civil society and industry stakeholders, should organize workshops, media outreach, and community programs to inform citizens about their rights under the NDPA and how to exercise them. Integrating digital privacy and data protection into school curricula and vocational training can foster a culture of privacy from the ground up. Likewise, targeted outreach to businesses (especially SMEs and startups) is critical, providing toolkits or seminars on NDPA compliance will help inculcate a compliance culture. Emulating POPIA's approach, the NDPC should have an explicit mandate (and resources) to promote public awareness as part of its regulatory function.[57]

---

[55] E Adeoti, 'A New Era of Data Protection and Privacy: Unveiling Innovations & Identifying Gaps in the Nigeria Data Protection Act of 2023' (24 July 2023) <https://ssrn.com/abstract=4520238> accessed 26 May 2025.

[56] LA Abdulrauf and H Dube (eds)**,** 'Independence of Data Protection' in *Data Privacy Law in Africa: Emerging Perspectives* (Pretoria University Law Press 2024) 355.

[57] S Victor**,** 'Data Protection and Compliance in Nigeria: Challenges and Opportunities' (30 April 2025) <https://ssrn.com/abstract=5236705> accessed 26 May 2025.

8.3 Impro

ve Cybersecurity Infrastructure and Support Compliance: Data protection law cannot be effective without secure systems. The government should invest in strengthening national cybersecurity infrastructure, such as supporting the development of security operations centres and encouraging adoption of international security standards (ISO 27001, etc.) among Nigerian companies. Initiatives to assist small and medium enterprises in enhancing their cyber defences are also needed for example, subsidies or grants for cybersecurity tools, or creating a pool of certified Data Protection Compliance Organisations to help businesses audit and improve their practices.[58] By reducing technical vulnerabilities, these steps will make it easier for organizations to comply with NDPA requirements for data security and breach prevention.

8.4 Regularly Update the NDPA and Fill Legal Gaps: Treat the NDPA as a living framework that will evolve with technology. The legislature and the NDPC (through its regulation-making powers) should periodically review and update the law to address emerging issues.

8.5 Regulating AI and Automated Decisions: Future amendments or regulations should provide clear rules on the use of AI, algorithms, and profiling. This could include requiring algorithmic transparency for decisions that significantly affect individuals and giving data subjects the right to human review of automated decisions, aligning with best practices in the GDPR.

8.6 Sensitive Data Protections: The law should incorporate stricter conditions for processing sensitive personal data – for instance, requiring explicit consent or authorization for processing health, genetic, biometric, or other highly sensitive data, and mandating enhanced security measures for such data.

8.7 Clarify Cross-Border Transfer Requirements: The NDPC should issue detailed guidelines that define what constitutes an "adequate" level of protection for foreign countries. This might include a whitelisting mechanism of approved countries, model contractual clauses for data transfers, or treaties with key trading partners. By clarifying these points, businesses can confidently engage in international data flows without running afoul of the law. Additionally, Nigeria should consider incorporating additional rights like data portability and the right to object to processing into its legal framework to fully empower consumers, as these have become part of global data protection norms.[59]

8.8 Build Judicial Capacity and Fast-Track Enforcement: Strengthen the capacity of the judiciary to handle data protection cases efficiently. This can be achieved by conducting training programs for judges and

[58] L Qudus**,** 'Cybersecurity Governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges' *International Journal of Science and Research Archive* (2025) 14(1) 1146–1163. <https://doi.org/10.30574/ijsra.2025.14.1.0225> accessed 26 May 2025.

[59] AO Ezema and MVC Ozioko**,** 'The Importance of Data Governance in Safeguarding Privacy and Security in Nigeria's Technology Industry: A Legal Review' *Nnamdi Azikiwe University Journal of Private and Property Law*, (2024) 1(1) 138–151. <https://journals.unizik.edu.ng/naujppl/article/view/4073> accessed 26 May 2025.

lawyers on technology law and data privacy issues, so that they are familiar with concepts like digital evidence, forensic data audits, and the technical nuances of privacy breaches. The judicial system could designate certain courts or judges to specialize in NDPA cases, or establish fast-track procedures for data protection complaints (akin to small-claims or fast-track commercial courts) to ensure timely resolution.[60] By improving the speed and expertise with which courts deal with privacy disputes, the law's deterrent effect will be enhanced, and consumers will have greater confidence in seeking redress. Moreover, publishing guiding judgments and interpretations will help build a body of case law that clarifies the NDPA's provisions over time.

8.9 Regional and International Collaboration: Data protection today transcends national borders. Nigeria should actively participate in regional initiatives to harmonize data protection standards across Africa. Adopting frameworks like the African Union's Malabo Convention on Cyber Security and Personal Data Protection as a benchmark can facilitate interoperability of laws and easier cross-border data exchange.[61] Collaboration with other countries' data protection authorities (for instance, through information-sharing agreements or mutual assistance in enforcement) can help Nigeria learn from established regulators and tackle transnational data breaches. Engaging with global best practices, perhaps through observer roles in international bodies or partnerships with European regulators, will keep Nigeria's approach up-to-date. Such collaboration will also signal to multinational companies that Nigeria is serious about data protection, aligning enforcement efforts with international expectations.

8.10 Promote Accountability and Transparency in Compliance: Encourage a culture of accountability among data controllers and processors. The NDPC should consider implementing periodic compliance audits or assessments for organizations processing large volumes of personal data.[62] Public sector institutions, in particular, should be exemplars in compliance, given that government data breaches or misuse can be especially damaging. Whistleblower protection mechanisms are also vital, employees who report data protection violations in their organizations should be shielded from retaliation, as their disclosures can help

[60] SN Modilim and others, 'Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment' *International Journal of Law Management & Humanities*, (2024) 7(6) 2481–2505. <https://www.researchgate.net/publication/391672110_Reforming_Data_Governance_in_Nigeria_A_Critical_Analysis_of_the_Nigeria_Data_Protection_Act_Regulatory_Enforcement_and_Global_Alignment> accessed 26 May 2025.

[61] A Mukuki and A Assenga**,** *Comparative Study of Data Protection Legislation Frameworks across the East African Community* (2024) D4D Hub <https://www.d4daccess.eu/sites/default/files/2024-05/COMPARATIVE%20STUDY%20OF%20THE%20DATA%20PROTECTION%20LEGISLATION%20FRAMEWORKS%20ACROSS%20THE%20EAC%20.pdf>accessed 26 May 2025.

[62] T Akinkunmi**,** 'Navigating Nigeria's NDPA: A Guide for Organizations to Build Trust and Mitigate Risk' (13 February 2025) <https://ssrn.com/abstract=5136591> accessed 26 May 2025.

uncover non-compliance that might otherwise go unnoticed.[63] Finally, the NDPC itself should operate transparently by publishing annual reports detailing its enforcement activities, number of complaints received, fines imposed, and any data breach statistics. Such transparency will build public trust in the regulatory regime and highlight areas for improvement each year.

By implementing these recommendations, Nigeria can significantly bolster the efficacy of the NDPA, 2023. The goal is to create not just a robust law on paper, but an actionable, enforceable, and respected data protection ecosystem. This will ensure that the promise of the NDPA protecting consumers and their data in the digital economy is fully realized.

9. Conclusion

The Nigeria Data Protection Act, 2023 is a landmark law that has ushered in a new era for data privacy and consumer protection in Nigeria's digital economy. It establishes a much-needed comprehensive framework aligned with global standards, granting individuals important rights over their personal data and mandating accountability from businesses and government agencies that process such data. The NDPA's enactment signals Nigeria's commitment to safeguarding citizens' information in an increasingly data-driven world, and it lays the foundation for building trust in online services and digital transactions.

However, as with any major new legislation, the true measure of success lies in implementation. The Act's effectiveness in protecting consumer rights will depend on addressing the challenges identified, from empowering the regulatory Commission with the necessary tools, to educating the populace, to refining the law in response to technological change. Comparisons with regimes like the GDPR and POPIA illustrate that while Nigeria has made substantial progress, there remain opportunities for improvement, such as broadening the scope of rights and strengthening enforcement mechanisms to match international best practices. The NDPA should not be seen as a static solution but as the beginning of an evolving process to achieve a high standard of data protection.

In the final analysis, the NDPA 2023 represents a commendable step forward for Nigeria. If the government, regulators, businesses, and civil society work collaboratively to implement the Act effectively i.e investing in institutions, raising awareness, and continually updating legal provisions, Nigeria can develop a robust data protection regime that both secures consumer rights and supports innovation in the digital economy. By doing so, Nigeria will not only protect its citizens in the digital realm but also position itself as a trustworthy

[63] R Skiba**,** *Leading and Influencing Ethical Practice* (After Midnight Publishing 2024).

player in the global digital marketplace, where strong data protection is increasingly a prerequisite for economic partnerships and growth. The ongoing commitment to strengthen data privacy safeguards will be essential in ensuring that the benefits of Nigeria's digital economy are realized without compromising the fundamentalrights and interests of its people.