

A CRITICAL ANALYSIS OF THE NIGERIA DATA PROTECTION ACT 2023: ELEVATING STANDARDS TO GLOBAL NORMS

Patrick Chukwunonso Aloamaka¹

ABSTRACT

The Nigeria Data Protection Act (NDPA) 2023 marks a pivotal advancement in Nigeria's regulatory framework for data protection. This article critically examines the NDPA, highlighting its alignment with the European Union's General Data Protection Regulation (GDPR) and its implications for Nigeria. Employing a doctrinal research methodology, the analysis delves into the Act's provisions, including definitions, data subject rights, data controller obligations, and the establishment of the Nigeria Data Protection Commission (NDPC). Comparisons with the GDPR underscore both the strengths and potential challenges of the NDPA, particularly in areas such as extraterritoriality, independence of the regulatory authority, and enforcement mechanisms. The article also explores the socio-economic and legal contexts that influence the Act's implementation. Recommendations are provided to enhance the effectiveness of the NDPA in safeguarding privacy rights and fostering trust in Nigeria's digital economy.

Keywords: Data Protection, Nigeria Data Protection Act, GDPR, Privacy Rights, Regulatory Framework

INTRODUCTION

Nigeria's efforts to regulate data protection have advanced significantly with the enactment of the NDPA in 2023. Before this, Nigeria's inadequate and fragmented data protection policy was frequently criticized. Historically, Nigerian laws and policies governing data protection have been disorganized, inconsistent, and incomplete. The Nigeria Data Protection Regulation (NDPR), for example, was published in 2019 by the National Information Technology Development Agency (NITDA).² While this was a significant step, it did not succeed in offering a comprehensive legal framework for data protection. The

¹ Lecturer, Faculty of Law, Delta State University, Oleh Campus, Delta State, Nigeria. Email: pcaloamaka@delsu.edu.ng.

² Olumide Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 International Data Privacy Law 44.

NDPR's narrow scope and frequently criticized enforcement methods were the result of complaints from a range of parties.³

The NDPA, influenced by the EU GDPR, seeks to provide a robust legal structure for protecting personal data. The GDPR is widely regarded as the gold standard in data protection legislation globally, and its influence on the NDPA is evident in several key areas. The NDPA incorporates many of the GDPR's principles, such as transparency, accountability, and the rights of data subjects. This transplantation of legal norms aims to elevate Nigeria's data protection standards to international levels, thereby fostering trust and confidence among data subjects and enhancing Nigeria's global competitiveness in the digital economy.

The NDPA aims to address the shortcomings of previous regulations by establishing clear definitions, roles, and responsibilities for data controllers and processors. It establishes extensive safeguards for the protection of personal data, such as strict consent requirements, obligations for notifying data breaches, and the creation of the Nigeria Data Protection Commission (NDPC), which is in charge of monitoring compliance and enforcement.

This article provides a critical analysis of the NDPA, examining its provisions, strengths, and potential pitfalls. It compares the NDPA with the GDPR to highlight similarities and differences, and assesses the implications of adopting such a comprehensive data protection framework in the Nigerian context. Key areas of focus include the scope and objectives of the Act, the concept of extraterritoriality, the independence of the Nigeria Data Protection Commission, and the exemptions for personal or household data processing. The analysis also explores the challenges of enforcing the NDPA, considering Nigeria's socio-economic landscape, legal infrastructure, and the readiness of stakeholders to comply with the new regulations.

By critically evaluating the NDPA, this article aims to provide insights into the effectiveness of the Act in addressing data protection issues in Nigeria. It also offers recommendations for enhancing the NDPA's implementation and enforcement, ensuring that it not only meets international standards but also addresses the unique needs and challenges of the Nigerian environment. The ultimate objective is to contribute with the development of a strong legal

³ Patrick Chukwunonso Aloamaka, 'DATA PROTECTION and PRIVACY CHALLENGES in NIGERIA: LESSONS from OTHER JURISDICTIONS' (2023) 3 UCC Law Journal 281.

framework that protects people's right to privacy and fosters the expansion of the digital economy, as well as to contribute to the continuing conversation about data protection in Nigeria.

REGULATORY FRAMEWORK AND LEGISLATIVE TRANSPLANTATION

The influence of the GDPR is evident in the structure and content of the NDPA, reflecting a clear case of legislative transplantation.⁴ Legal transplantation, a method of comparative law, involves adopting legal frameworks from other jurisdictions and adapting them to fit the local context.⁵ The GDPR, recognized globally for its stringent data protection standards and comprehensive approach, serves as a model for the NDPA. This transplantation aims to bring Nigeria's data protection regime in line with international best practices, thereby enhancing the country's global standing in the digital economy and providing stronger protections for individuals' personal data.

Data Protection Laws in African Nations and Emerging Markets

The global surge in digital activities has underscored the critical importance of robust data protection frameworks. While the GDPR has set a high standard, various African nations and emerging markets have developed their own data protection laws, reflecting diverse approaches tailored to their unique socio-economic contexts. This analysis explores the data protection frameworks of select African countries and emerging markets, drawing lessons that could inform and enhance Nigeria's data protection regime.

Data Protection Frameworks in African Nations

Kenya

Kenya's Data Protection Act, enacted in 2019, aligns closely with the GDPR, emphasizing principles such as lawful processing, data minimization, and purpose limitation. The Act establishes the Office of the Data Protection Commissioner, an independent body tasked with overseeing compliance, handling complaints, and enforcing data protection rights.⁶ Notably, the Act

⁴ Olumide Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3 *British Journal of Cyber Criminology* 1.

⁵ George Mousourakis, 'Legal Transplants and Legal Development: A Jurisprudential and Comparative Law Approach' (2013) 54 *Acta Juridica Hungarica* 219.

⁶ Republic of Kenya, *Data Protection Act* No. 24 of 2019, s 5.

mandates Data Protection Impact Assessments (DPIAs) for high-risk processing activities and requires organizations to appoint Data Protection Officers (DPOs) under specific conditions.⁷ Kenya's experience highlights the importance of clear regulatory structures and the proactive assessment of data processing risks.

South Africa

South Africa's Protection of Personal Information Act (POPIA), fully effective since 2021, provides a comprehensive framework for data protection. It introduces conditions for lawful processing, including accountability, openness, and security safeguards.⁸ The Act establishes the Information Regulator, an independent authority responsible for monitoring and enforcing compliance.⁹ POPIA's emphasis on accountability and the establishment of an independent regulator underscore the need for autonomous oversight bodies to ensure effective enforcement.

India

India's Digital Personal Data Protection Act (DPDP) 2023 also provides insights relevant to Nigeria. Unlike the GDPR, DPDP focuses heavily on compliance-driven enforcement, requiring companies to notify regulators within strict deadlines about breaches.¹⁰ India's approach, which emphasizes a balance between innovation and regulatory compliance, could offer Nigeria additional insights into developing effective enforcement strategies without stifling economic growth.

While Kenya and South Africa offer valuable examples of data protection implementation in Africa, the Nigerian NDPA demonstrates an even closer alignment with the GDPR. The NDPA and GDPR share core tenets regarding privacy protection, data subject rights, and the responsibilities of data controllers and processors. The concepts of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity,

⁷ Rogers Alunge, 'Consolidating the Right to Data Protection in the Information Age: A Comparative Appraisal of the Adoption of the OECD (Revised) Guidelines into the EU GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019' in Jessica Thorn, Assane Gueye and Adam P Hejnowicz (eds), *Innovations and Interdisciplinary Solutions for Underserved Areas* (Springer International Publishing 2020).

⁸ Republic of South Africa, Protection of Personal Information Act 4 of 2013, s 4.

⁹ Protection of Personal Information Act 4 of 2013, s 39.

¹⁰ India, Digital Personal Data Protection Act 2023, s 8(5).

confidentiality, and accountability, for instance, are adopted by the NDPA from the GDPR. These guidelines are intended to guarantee that personal data is handled in a way that upholds people's right to privacy and fosters confidence in data processing operations.

While this approach can be beneficial, it must consider the cultural, socio-political, and economic contexts of the recipient country.¹¹ Legal transplantation is not merely a matter of copying and pasting laws from one jurisdiction to another; it requires careful adaptation to ensure that the transplanted laws are effective and relevant in the new context. In the case of the NDPA, several contextual factors must be considered to ensure its successful implementation.

Scope and Objectives of the NDPA

The NDPA aims to protect the privacy rights of individuals by regulating the processing of personal data. Unlike the GDPR, which explicitly recognizes data protection as a fundamental right, the NDPA extends the protection to all fundamental rights under the Nigerian Constitution.¹² This broad scope could lead to enforcement challenges, as it may create unrealistic expectations about the Act's applicability to various fundamental rights.

The NDPA applies to data controllers and processors domiciled, ordinarily resident, or ordinarily operating in Nigeria, as well as those processing personal data of data subjects within Nigeria.¹³ This wide-reaching application is intended to ensure comprehensive protection of Nigerian citizens' data, regardless of where the data processing occurs.

Extraterritorial Application

One of the most ambitious aspects of the NDPA is its extraterritorial reach,¹⁴ mirroring the GDPR's attempt to regulate data processing activities beyond its geographical boundaries.¹⁵ Although this provision attempts to safeguard Nigerian subjects whose data is handled wherever it is processed, it presents serious jurisdictional issues. Nigerian courts may struggle with enforcement

¹¹ Ugo Mattei, 'Efficiency in Legal Transplants: An Essay in Comparative Law and Economics' (1994) 14 *Int'l Rev L & Econ* 3.

¹² Nigeria Data Protection Act 2023, s 1.

¹³ Nigeria Data Protection Act 2023, s 2.

¹⁴ *Ibid.*

¹⁵ General Data Protection Regulation (EU) 2016/679, art 3.

issues, particularly when dealing with international data controllers and processors.

The GDPR's extraterritorial provisions have similarly faced scrutiny and challenges, particularly in enforcing compliance across different jurisdictions.¹⁶ The NDPA's extraterritorial ambitions could encounter similar difficulties, especially given the complexities of international law and differing national regulations.

Independence of the Nigeria Data Protection Commission (NDPC)

The NDPA establishes a Nigeria Data Protection Commission (NDPC) responsible for overseeing compliance and enforcement. However, the Act's provisions regarding the NDPC's independence are problematic. The appointment of NDPC officers on the recommendation of a cabinet minister and the insecure tenure of these officers undermine the Commission's independence.¹⁷ This could result in executive interference, compromising the NDPC's ability to enforce data protection regulations impartially.

Comparatively, the GDPR mandates a higher degree of independence for supervisory authorities, ensuring they operate without external influence.¹⁸ This independence is crucial for maintaining public trust and ensuring unbiased enforcement of data protection laws.

Enforcement and Compliance Trends under the NDPA

The Nigeria Data Protection Commission (NDPC) has reported a significant financial impact from data protection enforcement under the Nigeria Data Protection Act (NDPA) 2023. In 2024 alone, the government generated approximately ₦12 billion from data protection activities, a notable increase from ₦4 billion in 2021.¹⁹ This growth is largely attributed to heightened regulatory enforcement, increased corporate compliance, and the expansion of data protection services. Furthermore, compliance-related revenue surged from

¹⁶ Oskar Josef Gstrein and Andrej Janko Zwitter, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10 Internet Policy Review 1.

¹⁷ Nigeria Data Protection Act 2023, s 14.

¹⁸ General Data Protection Regulation (EU) 2016/679, art 52.

¹⁹ Sami Tunji, 'Govt Earned N12bn from Data Protection in 2024 – NDPC' *Punch Newspaper* (2024) <<https://punchng.com/govt-earned-n12bn-from-data-protection-in-2024-ndpc/>> accessed 26 January 2025.

₦24.5 million in 2021 to ₦1.5 billion in 2024.²⁰ The number of Compliance Audit Returns (CARs) filed by organizations also grew substantially, from 1,864 in 2020–2021 to 4,691 in 2023–2024, reflecting a growing culture of adherence to data protection regulations.²¹

The sector's expansion has also led to job creation, with employment in data protection roles increasing from 10,123 jobs in 2023 to 23,000 jobs in 2024.²² Additionally, the number of Verified Data Protection Officers (DPOs) rose from 362 in 2021 to 2,888 in 2024, while Data Protection Compliance Organizations (DPCOs) expanded from 103 in 2021 to 246 in 2024.²³ These figures highlight the increasing demand for specialized data protection expertise in Nigeria's digital economy.

The NDPC's regulatory enforcement has also intensified, with the Commission conducting 213 investigations into data breaches and compliance violations in 2024, up from 177 in 2023.²⁴ Many of these cases involved privacy breaches, unauthorized data sharing, and corporate non-compliance with NDPA provisions.²⁵ The NDPC has stated that stricter enforcement measures and higher penalties will be implemented in the coming years to ensure stronger compliance with the Act.²⁶

Furthermore, Nigeria has strengthened its international collaborations in data protection. The NDPC has signed Memoranda of Understanding (MoUs) with data protection authorities in Canada and Dubai, emphasizing Nigeria's commitment to global privacy standards.²⁷ The NDPC has also actively participated in international regulatory networks, such as the Global Privacy

²⁰ ITEdgeNews, 'NDPC Holds National Privacy Week, Reports N12bn Revenue' (*ITEdgeNews* 29 January 2025) <<https://www.itedenews.africa/ndpc-holds-national-privacy-week-reports-n12bn-revenue/>> accessed 29 January 2025.

²¹ *Ibid.*

²² *Ibid.*

²³ *Ibid.*

²⁴ Emmanuel Elebeke, 'How NITDA Impacted IT Industry in 2024 - Report' *Vanguard News* (19 December 2024) <<https://www.vanguardngr.com/2024/12/how-nitda-impacted-it-industry-in-2024-report/>> accessed 26 January 2025.

²⁵ *Ibid.*

²⁶ 'NDPR (Lite) Performance Report 2019–2020' (Rapporteur on Data Protection, April 2021) <https://www.rapdp.org/sites/default/files/2021-04/NDPR%20%28Lite%29%20Performance%20Report%20%202019-2020.pdf> accessed 29 January 2025.

²⁷ Sami Tunji (n 14).

Assembly and the Network of African Data Protection Authorities, further positioning Nigeria as a regional leader in data protection.²⁸

These empirical insights provide tangible evidence of the NDPA's impact on regulatory enforcement, compliance, job creation, and international cooperation. They reinforce the argument that Nigeria's adoption of global data protection norms is strengthening its digital economy and fostering trust in data governance practices.

Personal or Household Processing Exemptions

The NDPA includes exemptions for personal or household data processing, similar to the GDPR.²⁹ However, the NDPA's approach to these exemptions is inconsistent and potentially confusing. The Act exempts personal data processing for household purposes unless it violates the fundamental right to privacy.³⁰ This contradictory provision undermines the clarity and effectiveness of the exemption, as it creates a legislative loophole that complicates enforcement.

The GDPR also provides exemptions for personal or household activities but is more explicit in its definitions and conditions.³¹ This clarity helps avoid confusion and ensures that exemptions are applied consistently and fairly.

Data Protection by Design and by Default

The NDPA misses an opportunity to incorporate the concepts of data protection by design and by default, which are fundamental to the GDPR.³² Data controllers must incorporate data protection safeguards into their systems and processes from the beginning in accordance with these principles. Including these concepts in the NDPA would enhance its proactive approach to privacy risk mitigation and strengthen overall data protection practices.

The GDPR's emphasis on data protection by design and by default has been pivotal in encouraging organizations to prioritize privacy and security from the

²⁸ *IT Edge News* (n 15).

²⁹ Nigeria Data Protection Act 2023, s 3(1).

³⁰ *Ibid.*

³¹ General Data Protection Regulation (EU) 2016/679, art 2(2)(c).

³² General Data Protection Regulation (EU) 2016/679, art 25.

beginning of their operations.³³ Implementing similar requirements in the NDPA could significantly improve data protection standards in Nigeria.

Age of Consent

The NDPA sets the digital age of consent at 13 years, aligning with the lower end of the GDPR's range.³⁴ However, this provision is inconsistent with other Nigerian laws, such as the Child's Right Act, which sets the age of consent at 18 years.³⁵ This discrepancy creates confusion and undermines the protection of children's data. The NDPA needs to harmonize its age-related provisions with existing laws to provide clear and consistent guidelines.³⁶

The GDPR allows member states some flexibility in setting the age of consent between 13 and 16 years, reflecting differences in national legislation.³⁷ This flexibility has helped ensure that data protection laws align with broader legal frameworks within individual countries. For instance, if a member state chooses to set the age of consent below 16 years, it must not be lower than 13 years. This means that the minimum age for a child to consent to data processing under the GDPR is 13, and member states can set the age requirement within this range.

Consent and Automated Decision-Making

Gaining valid consent from data subjects is another vital aspect of data protection. According to the NDPA, consent must be freely given, specific, informed, and clear. Consent should be affirmative and not based on pre-selected confirmations.³⁸ This aligns with the GDPR's stringent requirements for consent, which mandate that consent be clear, distinguishable, and intelligible, using plain language.³⁹

The NDPA also prohibits automated decision-making in terms of obtaining consent, ensuring that each data subject has the right to either accept or reject the provision of consent and not be subject to decisions based solely on

³³ General Data Protection Regulation (EU) 2016/679, art 25; Sara Gustavsson, 'An Assessment of Privacy by Design as a Stipulation in GDPR' (Masters Thesis 2020) 12.

³⁴ Nigeria Data Protection Act 2023, s 31(5).

³⁵ Child's Right Act 2003, s 277.

³⁶ Olumide Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3 British Journal of Cyber Criminology 4.

³⁷ General Data Protection Regulation (EU) 2016/679, art 8(1).

³⁸ Nigeria Data Protection Act 2023, s 26.

³⁹ General Data Protection Regulation (EU) 2016/679, art 7.

automated processing.⁴⁰ This reflects similar provisions in the GDPR, which aim to protect individuals from potentially harmful automated decisions.⁴¹

However, the NDPA's prohibition on assumed consent from silence or inactivity is a clear and necessary distinction that enhances data protection.⁴² Ensuring that consent cannot be inferred from a lack of response helps protect data subjects from unintentional or coerced consent.

Data Protection Impact Assessments (DPIAs)

Data processing operations have risks that must be identified and mitigated, and this is where DPIAs come in.. The NDPA and GDPR both mandate DPIAs where processing operations are likely to result in high risks to the rights and freedoms of data subjects.⁴³ This involves systematically describing the envisaged processing and assessing its necessity and proportionality, as well as evaluating risks and outlining measures to mitigate them.⁴⁴

The GDPR provides more detailed requirements for DPIAs, including specific conditions under which they must be conducted and the need to consult supervisory authorities.⁴⁵ These requirements are outlined in Articles 35 and 36 of the GDPR. The NDPA lacks these detailed provisions, which could lead to inconsistencies in how DPIAs are performed and evaluated.⁴⁶

Data Protection Officers (DPOs)

Both the GDPR and NDPA mandate the appointment of Data Protection Officers (DPOs) for certain organizations.⁴⁷ The requirements make sure that organizations handling sensitive data or high-risk processing operations designate a DPO to monitor adherence to data protection laws and safeguard the rights of data subjects. Specifically, DPOs are in charge of managing data protection strategies and making sure that all applicable laws are followed.⁴⁸ These tasks ensure that the DPO plays a critical role in an organization's data

⁴⁰ Nigeria Data Protection Act 2023, s 37.

⁴¹ General Data Protection Regulation (EU) 2016/679, art 22.

⁴² Nigeria Data Protection Act 2023, s 26(3).

⁴³ Nigeria Data Protection Act 2023, s 28; General Data Protection Regulation (EU) 2016/679, art 35.

⁴⁴ General Data Protection Regulation (EU) 2016/679, art 35(7).

⁴⁵ General Data Protection Regulation (EU) 2016/679, art 35 and art 36.

⁴⁶ Nigeria Data Protection Act 2023, s 28.

⁴⁷ General Data Protection Regulation (EU) 2016/679, art 37 and art 39; Nigeria Data Protection Act 2023, s 32.

⁴⁸ General Data Protection Regulation (EU) 2016/679, art 39(1).

protection framework, helping to manage compliance with data protection laws and mitigate risks associated with data processing activities. The GDPR provides detailed criteria for when a DPO must be appointed, such as when an organization processes large-scale data or monitors individuals systematically.⁴⁹ By mandating the appointment of a DPO under these specific conditions, the GDPR ensures that organizations with significant data protection responsibilities have a dedicated person to oversee compliance and protect data subjects' rights

The NDPA's criteria for appointing DPOs are less specific, stating only that controllers or processors of major importance must appoint a DPO.⁵⁰ The term "data controller of major importance" is defined in the Act, but it leaves some flexibility in determining which organizations fall under this category. Essentially, the NDPA requires significant data controllers and processors to appoint a DPO but does not provide an exhaustive list of specific criteria or thresholds for this designation, focusing instead on the scale and significance of the data processing activities. This vagueness could lead to inconsistent applications and potentially inadequate data protection practices in smaller organizations.

The GDPR also allows for the appointment of a single DPO by a group of similar establishments, a provision not explicitly mentioned in the NDPA.⁵¹ This means that companies that are part of a corporate group, such as subsidiaries or affiliates, can appoint one DPO to oversee data protection compliance for the entire group. This is particularly beneficial for multinational corporations with multiple branches or subsidiaries, as it ensures a consistent. This flexibility can help smaller organizations share resources and expertise in managing data protection responsibilities.

Data Protection Compliance Experts

The NDPA and GDPR both emphasize the role of data protection compliance experts in monitoring and auditing compliance.⁵² By emphasizing these roles, the GDPR and NDPA ensures that organizations have dedicated experts to oversee and enhance their data protection compliance efforts, thereby

⁴⁹ General Data Protection Regulation (EU) 2016/679, art 37(1).

⁵⁰ Nigeria Data Protection Act 2023, s 32.

⁵¹ General Data Protection Regulation (EU) 2016/679, art 37(2).

⁵² General Data Protection Regulation (EU) 2016/679, art 37-39; Nigeria Data Protection Act 2023, s 32 and s 33.

protecting data subjects' liberties and rights. However, the NDPA requires these experts to be individuals with the necessary expertise in data protection are responsible for advising, monitoring, and auditing compliance within organizations, thereby enhancing the overall data protection framework.⁵³

In a similar vein, the GDPR requires that the appointment of DPOs be contingent upon certain requirements concerning the type and scope of data processing operations.. The DPO must be a person (or a team) with the requisite expertise and independence to oversee the organization's compliance with data protection laws .⁵⁴ The GDPR does not require that DPOs be bodies; rather, it focuses on the appointment of individuals or teams who can fulfil the DPO role effectively.

Rights of Data Subjects

The NDPA and GDPR both grant data subjects a range of rights, including the “right to access,” correct, and “erase their data.”⁵⁵ These rights ensure that data subjects can exercise significant control over their personal data, compelling data controllers and processors to maintain high standards of data protection and transparency. The GDPR provides more detailed provisions for these rights, including the requirement to inform data subjects of the recipients of their data and the obligation to take reasonable steps to notify third parties of any rectifications or erasures.⁵⁶ Under the GDPR, controllers are obliged to ensure transparency and take necessary steps to communicate any changes or actions taken regarding personal data to both the data subject and relevant third parties.

The NDPA includes similar rights but lacks some of the detailed procedural requirements found in the GDPR.⁵⁷ This could lead to inconsistencies in how data subjects' rights are implemented and enforced.

⁵³ Nigeria Data Protection Act 2023, s 32 and s 33

⁵⁴ General Data Protection Regulation (EU) 2016/679, art 37-39.

⁵⁵ General Data Protection Regulation (EU) 2016/679, art 16, art 17, art 18, art 20 & art 21; Nigeria Data Protection Act 2023, s 34.

⁵⁶ General Data Protection Regulation (EU) 2016/679, art 15, art 16, art 17(2) & art 19.

⁵⁷ Nigeria Data Protection Act 2023, s 34-38.

Sensitive Personal Data

Both the NDPA and GDPR impose restrictions on processing sensitive personal data, also referred to as "special categories of personal data."⁵⁸ These categories include information about a person's racial or ethnic background, political views, religious or philosophical convictions, trade union membership, genetic information, biometric information used to uniquely identify an individual, health information, and information about a person's sexual orientation or sex life. The GDPR includes additional provisions for processing data related to criminal convictions and offences, which are not explicitly addressed in the NDPA.⁵⁹ This omission could lead to gaps in protection for sensitive data in Nigeria.

The GDPR also requires that sensitive data be processed under the supervision of professionals bound by confidentiality obligations, a requirement not explicitly stated in the NDPA.⁶⁰ This could impact the security and confidentiality of sensitive personal data processed in Nigeria.

Data Security

Both the NDPA and the GDPR place emphasis on the necessity for data processors and controllers to put in place suitable security measures.⁶¹ However, the GDPR includes more detailed provisions for ensuring that all personnel with access to personal data are properly authorized and trained.⁶² These requirements ensure that data controllers and processors take a proactive and comprehensive approach to data security, protecting personal data from various threats and ensuring compliance. The GDPR also allows for the use of certifications to demonstrate compliance with security measures, a provision not explicitly mentioned in the NDPA.⁶³ These provisions allow organizations to use certifications to demonstrate their adherence to the GDPR's requirements, including security measures. Certification can serve as a visible

⁵⁸ General Data Protection Regulation (EU) 2016/679, art 9; Nigeria Data Protection Act 2023, s 30.

⁵⁹ General Data Protection Regulation (EU) 2016/679, art 10.

⁶⁰ General Data Protection Regulation (EU) 2016/679, art 9(3).

⁶¹ Nigeria Data Protection Act 2023, s 39; General Data Protection Regulation (EU) 2016/679, art 32.

⁶² General Data Protection Regulation (EU) 2016/679, art 32(4).

⁶³ General Data Protection Regulation (EU) 2016/679, art 42- 43.

indicator of compliance and commitment to data protection standards, which can build trust with data subjects, business partners, and regulatory authorities.

Trans-Border Data Transfer

The NDPA and GDPR both regulate the transfer of personal data to third countries.⁶⁴ The NDPA limits transfers to countries that provide an adequate level of data protection.⁶⁵ By doing this, the NDPA protects the rights and liberties of data subjects in Nigeria by ensuring that personal data can only be transferred to nations or areas that have been evaluated and found to offer a sufficient degree of data protection.

While the GDPR also includes provisions for transfers to international organizations.⁶⁶ This is to ensure that the transfer of personal data outside the European Economic Area EEA is conducted in a manner that maintains the high level of protection guaranteed by the GDPR, thereby safeguarding the rights and freedoms of data subjects. This broader scope in the GDPR provides more flexibility for international data transfers, while ensuring that adequate protections are in place.

The GDPR also mandates continuous monitoring of the recipient country's data protection practices and allows for the suspension or repeal of transfer approvals if adequate protections are no longer ensured.⁶⁷ This comprehensive approach ensures that personal data transferred outside the EEA is consistently protected in line with GDPR standards. This ongoing oversight is not explicitly required under the NDPA, potentially limiting its effectiveness in ensuring long-term data protection in international transfers.

Certification

The NDPA provides for the certification of data processing operations, but this is not mandatory, which is outlined in Section 33 under Part V – Principles and Lawful Basis Governing Processing of Personal Data.⁶⁸ While the NDPA allows for the certification and licensing of individuals or entities to provide data protection compliance services, it does not make such certification

⁶⁴ Nigeria Data Protection Act 2023, s 41- 43; General Data Protection Regulation (EU) 2016/679, art 44-50.

⁶⁵ Nigeria Data Protection Act 2023, s 42

⁶⁶ General Data Protection Regulation (EU) 2016/679, art 45, art 46, art 47 & art 49.

⁶⁷ General Data Protection Regulation (EU) 2016/679, art 45(3), art 45(5).

⁶⁸ Nigeria Data Protection Act 2023, s 33.

mandatory for all data controllers and data processors. The certification process serves as a mechanism to ensure that entities engaged in data processing comply with the standards set forth in the Act, but organizations are not obligated to undergo certification to operate.

Moreover, the GDPR also includes provisions for certification mechanisms and data protection seals, which serve as evidence of compliance with data protection laws, which are outlined in Articles 42 and 43 of the GDPR.⁶⁹ By incorporating these provisions, the GDPR hopes to raise the standard of data protection across the EU by encouraging best practices in data protection and provide a framework for organizations to demonstrate their compliance. The GDPR mandates that all certification mechanisms be publicly available, enhancing transparency and accountability.⁷⁰ This requirement is designed to ensure that both the certification process and the results are open to scrutiny, thereby fostering trust and confidence in the data protection measures adopted by organizations.

JUDICIAL APPROACH TO DATA PROTECTION IN NIGERIA

Before the enactment of the NDPA, Nigerian courts played a role in data protection through their interpretations of the right to privacy under the Nigerian Constitution. The Nigerian Constitution,⁷¹ specifically Section 37, guarantees the right to privacy. Nigerian courts have interpreted this provision to include data protection, as demonstrated in several cases.

In *Digital Rights Lawyers Initiative (DRLI) v National Identity Management Commission (NIMC)*,⁷² the court determined that a data subject's right under the NDPR is the rectification of personal data, and that this right should not involve payment. Similarly, in *Incorporated Trustees of Digital Rights Lawyers Initiative (DRLI) v Central Bank of Nigeria (CBN)*,⁷³ the court

⁶⁹ General Data Protection Regulation (EU) 2016/679, art 42 and art 43.

⁷⁰ General Data Protection Regulation (EU) 2016/679, art 42(8), art 42 (5), & art 43.

⁷¹ Constitution of the Federal Republic of Nigeria 1999, s 37.

⁷² *Digital Rights Lawyers Initiative (DRLI) v National Identity Management Commission (NIMC)*, Appeal Number CA/IB/291/2020.

⁷³ *Incorporated Trustees of Digital Rights Lawyers Initiative (DRLI) v Central Bank of Nigeria (CBN)*, Unreported Suit No. FHC/AB/CS/76/2020.

affirmed that data protection is a fundamental right covered by the Fundamental Rights Enforcement Procedure Rules and is subject to litigation.⁷⁴

In *Incorporated Trustees of Digital Rights Lawyers Initiative v L.T. Solutions & Multimedia Limited*,⁷⁵ The court ruled that the protection of a citizen's personal information is covered by their right to privacy. However, the court's decision in this case also highlighted the challenges in proving the infringement of this right.⁷⁶

In *Incorporated Trustees of Digital Rights Lawyers Initiative v Minister of Industry, Trade, and Investment & 2 Ors*,⁷⁷ the court emphasized the need for data controllers to demonstrate compliance with the NDPR, particularly in terms of data protection officer (DPO) appointments and privacy policy publications.

These cases illustrate the evolving judicial attitude towards data protection in Nigeria and the increasing recognition of data protection as a fundamental right.

CHALLENGES OF ENFORCING THE NDPA

One of the significant challenges in enforcing the NDPA is the lack of capacity-building initiatives and resources for proper implementation. A key strategy to overcome this is enhancing training programs for data controllers and processors to ensure compliance with data protection standards. Additionally, public awareness campaigns are essential to educate individuals about their data rights and responsibilities.

Another major challenge is the need for stronger international partnerships. Nigeria can benefit from collaborations with global data protection authorities, such as the European Data Protection Board and the African Union, to develop best practices and harmonize regulations. Establishing bilateral agreements with countries that have advanced data protection laws can also facilitate smoother cross-border data transfers and regulatory cooperation.

⁷⁴ Ikenga KE Oraegbunam and Tega Edema, 'EXAMINING the JUDICIAL ATTITUDE to DATA PROTECTION in NIGERIA' (2023) 4 LAW AND SOCIAL JUSTICE REVIEW 3.

⁷⁵ *Incorporated Trustees of Digital Rights Lawyers Initiative v L.T. Solutions & Multimedia Limited*, Suit No. HCT/262/2020.

⁷⁶ Ikenga KE Oraegbunam and Tega Edema, 5.

⁷⁷ *Incorporated Trustees of Digital Rights Lawyers Initiative v Minister of Industry, Trade, and Investment & 2 Ors*, Unreported Case Suit No. FHC/AWK/CS/116/2020.

Emerging technologies like AI, blockchain, and big data analytics present new challenges for data protection. AI-driven decision-making, for example, raises concerns about algorithmic bias and transparency in data processing. Blockchain, while enhancing data security through decentralization, creates challenges regarding data rectification and the right to be forgotten under the NDPA. Nigeria's regulatory framework should integrate automated compliance monitoring systems, leveraging AI to detect and prevent data breaches more effectively. The NDPA could benefit from sandbox initiatives similar to the UK and Singapore, allowing companies to test AI and blockchain-based privacy solutions within a controlled regulatory environment.

By addressing these challenges through capacity-building, international partnerships, and technological advancements, Nigeria can ensure a more effective and efficient enforcement of the NDPA, fostering a stronger data protection culture in the country.

THE ECONOMIC IMPLICATIONS OF THE NDPA

The NDPA is more than a legal framework for privacy protection; it serves as a catalyst for economic growth by fostering investor confidence, innovation, and digital inclusion. By creating a transparent and regulated data ecosystem, the Act strengthens Nigeria's global competitiveness and digital economy.

- 1) **Attracting Foreign Investment:** A robust data protection framework enhances investor confidence, making Nigeria a preferred destination for multinational corporations, tech firms, and cloud service providers. By aligning with international standards such as the GDPR, the NDPA ensures compliance with data security regulations, reducing risks in cross-border data transfers.⁷⁸ This regulatory clarity has attracted leading technology companies, such as Google, Meta, and Amazon Web Services, which require strong data protection laws before expanding into new markets.⁷⁹ Additionally, the NDPA facilitates

⁷⁸ NDPA 2023, s. 41.

⁷⁹ Prince Nwafor, Hi-Tech Editor and Adanna Nwankwo, 'How Google Injected \$1.8b in Nigeria's Economy in 2023' (*Vanguard News3* October 2024) <<https://www.vanguardngr.com/2024/10/how-google-injected-1-8b-in-nigerias-economy-in-2023/>> accessed 29 January 2025.

for digital trade.⁸⁰

- 3) Promoting Digital Inclusion and Consumer Trust: The NDPA can help by bridging Nigeria's digital divide by enhancing trust in digital services, particularly in rural and underserved areas. By ensuring secure handling of personal data, the Act encourages wider adoption of mobile banking, e-commerce, and online services. Additionally, it fosters government-private sector collaboration in digital literacy and cybersecurity awareness initiatives, empowering more Nigerians to engage safely with digital platforms. With clear privacy safeguards, the NDPA promotes financial inclusion, expands access to digital services, and strengthens Nigeria's leadership in Africa's digital economy.

RECOMMENDATIONS

To enhance the NDPA, the following recommendations are proposed:

1. Recognize Data Protection as a Fundamental Right: Explicitly recognizing data protection as a fundamental right would align the NDPA with global standards and provide a clearer legal basis for enforcement.

⁸⁰ NDPA 2023, s. 42.

⁸¹ Mercy King'ori, 'Nigeria's New Data Protection Act, Explained' ([https://fpf.org/28 June 2023](https://fpf.org/28%20June%202023)) <<https://fpf.org/blog/nigerias-new-data-protection-act-explained/>> accessed 27 January 2025.

2. Clarify the Scope of Exemptions: Simplify and clarify the exemptions for personal or household data processing to ensure they are practical and enforceable.
3. Ensure Independence of the NDPC: Strengthen the independence of the Nigeria Data Protection Commission by ensuring secure tenure for its officers and minimizing executive interference.
4. Incorporate Data Protection by Design and by Default: Integrate these principles into the NDPA to promote proactive privacy risk management.
5. Harmonize Age of Consent Provisions: Align the age of consent for data processing with other Nigerian laws to provide consistent protection for children.
6. Enhance Public Awareness and Education: Conduct extensive public awareness campaigns and educational programs to ensure that data subjects and controllers understand their rights and obligations under the NDPA.
7. Provide Detailed Guidelines for DPIAs: Include specific conditions under which DPIAs must be conducted and ensure continuous oversight by the DPA to improve risk assessment practices.
8. Expand Provisions for Sensitive Data: Include detailed requirements for processing sensitive data related to criminal convictions and ensure that such data is processed under strict confidentiality obligations.
9. Improve Data Security Measures: Mandate certifications for data security measures and ensure continuous training and authorization of personnel with access to personal data.
10. Enhance International Data Transfer Regulations: Implement continuous monitoring and oversight of recipient countries' data protection practices to ensure long-term compliance.

By addressing these issues, the NDPA can become a robust and effective legal framework that protects the privacy rights of individuals and promotes a culture of data protection in Nigeria

CONCLUSION

The Nigeria Data Protection Act (NDPA) 2023 represents a significant step towards strengthening data protection in Nigeria, aligning the country's regulatory framework with international standards. By adopting principles from the GDPR, the NDPA aims to provide a comprehensive and robust legal structure for the protection of personal data. However, successful implementation requires careful consideration of Nigeria's unique socio-economic and legal landscapes. Challenges such as enforcement, regulatory independence, and public awareness must be addressed to ensure the Act's efficacy. This article highlights the importance of these factors and offers recommendations for enhancing the NDPA's impact. Ultimately, a well-implemented NDPA can not only protect individual privacy rights but also boost Nigeria's digital economy by fostering trust and confidence in data processing activities.

REFERENCES

- Aloamaka PC, 'Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions' (2023) 3 UCC Law Journal 281
- Alunge R, 'Consolidating the Right to Data Protection in the Information Age: A Comparative Appraisal of the Adoption of the OECD (Revised) Guidelines into the EU GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019' in Jessica Thorn, Assane Gueye and Adam P Hejnowicz (eds), *Innovations and Interdisciplinary Solutions for Underserved Areas* (Springer International Publishing 2020)
- Babalola O, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 International Data Privacy Law 44
- Babalola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3 British Journal of Cyber Criminology 1
- Elebeke E, 'How NITDA Impacted IT Industry in 2024 - Report' *Vanguard News* (19 December 2024) <<https://www.vanguardngr.com/2024/12/how-nitda-impacted-it-industry-in-2024-report/>> accessed 26 January 2025
- Gstrein OJ and Zwitter AJ, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10 Internet Policy Review 1

Gustavsson S, 'An Assessment of Privacy by Design as a Stipulation in GDPR' (Masters Thesis2020) 12

ITEdgeNews, 'NDPC Holds National Privacy Week, Reports N12bn Revenue' (*ITEdgeNews*29 January 2025) <<https://www.itedgenews.africa/ndpc-holds-national-privacy-week-reports-n12bn-revenue/>> accessed 29 January 2025

King'ori M, 'Nigeria's New Data Protection Act, Explained' (<https://fpf.org/28> June 2023) <<https://fpf.org/blog/nigerias-new-data-protection-act-explained/>> accessed 27 January 2025

Mousourakis G, 'Legal Transplants and Legal Development: A Jurisprudential and Comparative Law Approach' (2013) 54 *Acta Juridica Hungarica* 219

Oraegbunam IKE and Edema T, 'EXAMINING the JUDICIAL ATTITUDE to DATA PROTECTION in NIGERIA' (2023) 4 *LAW AND SOCIAL JUSTICE REVIEW* 3

Tunji S, 'Govt Earned N12bn from Data Protection in 2024 – NDPC' *Punch Newspaper* (2024) <<https://punchng.com/govt-earned-n12bn-from-data-protection-in-2024-ndpc/>> accessed 26 January 2025

STATUTES

Child's Right Act 2003, s 277

Constitution of the Federal Republic of Nigeria 1999, s 37

General Data Protection Regulation (EU) 2016/679, arts 2(2)(c), 3, 7, 8(1), 9, 9(3), 10, 15, 16, 17, 17(2), 18, 19, 20, 21, 22, 25, 32, 32(4), 35, 35(7), 36, 37, 37(1), 37(2), 37-39, 39(1), 42, 42(8), 42(5), 43, 44-50.

India, Digital Personal Data Protection Act 2023, s 8(5), s 8(6).

Nigeria Data Protection Act 2023, ss 1, 2, 3(1), 14, 26, 26(3), 28, 30, 31(5), 32, 33, 34, 34-38, 37, 39, 41-43, 42.

Republic of Kenya, Data Protection Act No. 24 of 2019, s 5.

Republic of South Africa, Protection of Personal Information Act 4 of 2013, s 39.

CASE LAWS

Digital Rights Lawyers Initiative (DRLI) v National Identity Management Commission (NIMC), Appeal Number CA/IB/291/2020

Incorporated Trustees of Digital Rights Lawyers Initiative (DRLI) v Central Bank of Nigeria (CBN), Unreported Suit No. FHC/AB/CS/76/2020

Incorporated Trustees of Digital Rights Lawyers Initiative v L.T. Solutions & Multimedia Limited, Suit No. HCT/262/2020

Incorporated Trustees of Digital Rights Lawyers Initiative v Minister of Industry, Trade, and Investment & 2 Ors, Unreported Case Suit No. FHC/AWK/CS/116/2020