International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Managing digital records within Nigeria's regulatory framework

OluGbenro Adedeji Ogundipe *

Doctorate in Business Administration, Edgewood College, USA.

International Journal of Science and Research Archive, 2024, 12(02), 2861–2868

Publication history: Received on 19 July 2024; revised on 26 August 2024; accepted on 29 August 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1603

Abstract

Nigeria has a complicated legal and regulatory environment. This complicated history brings to mind the oft-quoted Biblical phrase, *"There was no king in Israel, and every man did what was right in his own eyes." (New King James Version Bible,* 1982 Judges 17:6*)* As the technological landscape began to change, strong legislative frameworks are now required to guarantee the security, accessibility, and integrity of digital information. Since enacting the Nigeria Data Protection Regulation (NDPR) in 2019, and the subsequent passing into law of the Nigeria Data Protection Act (NDPA) 2023, and establishing the Nigeria Data Protection Commission (NDPC), Nigeria has reached landmark milestones in Nigeria's journey toward improving data protection and privacy. This paper provides a comprehensive analysis of the recent developments in Nigeria's data protection landscape and implications for digital records management in government agencies and businesses. This paper further tries to examine the implications of these developments for digital records management within Government Agencies and Businesses.

It will also provide a brief history of digital records in Nigeria. Furthermore, it will analyze key provisions of the NDPA and the NDPC's strategic priorities and identify opportunities and challenges for aligning records management practices with the new framework. The paper also reviews the relationship between records management and organizational credibility in Nigeria, discussing how proper record management is crucial for the credibility of public institutions and organizations in Nigeria.

Additionally, it attempts to show the benefit of data-driven regulatory approaches to assist organizations in navigating Nigeria's complex regulatory landscape. This paper offers recommendations for businesses, agencies, and regulators to utilize the NDPA and its strategies to enhance the adoption of digital records management. The methodology for selecting and analyzing sources involved a comprehensive literature review and policy analysis, focusing on key legal documents, academic articles, and reports from relevant agencies.

Keywords: Digital records management; Nigeria; Data protection; NDPA; Regulatory compliance; Organizational credibility

1. Introduction

Nigeria's government and business sectors depend heavily on digital record management.

Nigeria has taken decisive steps to prioritize data protection and privacy in the last few years. The signing of the Nigeria Data Protection Regulation (NDPR) in 2019 and the establishment of the Nigeria Data Protection Commission (NDPC) as the independent data protection authority signal a strong commitment to safeguarding citizens' data in the digital age (NDPC, 2023).

* Corresponding author: OluGbenro Ogundipe

The NDPA 2023, which evolved from this, is a comprehensive legal framework for data protection. It applies to the processing of personal data of over 220 million persons in Nigeria, making it one of the world's largest single-country data protection frameworks. The Act empowers the commission to supervise personal data processing and enforce compliance, a big part of the commission's role in ensuring data protection and privacy in Nigeria.

These developments have regulatory implications for digital records management within government agencies and businesses, among the largest collectors and processors of citizens' data. These Businesses and Agencies need to align their record management policies, systems, policies, and practices with those set out in the NDPR. They must also cooperate with the NDPC in its regulatory and enforcement activities.

The objectives of this paper are threefold:

- To scrutinize the key provisions of the NDPA and their implications for digital records management,
- To explore the relationship between electronic records management and organizational credibility, and
- To investigate the possibilities of data-driven regulatory compliance approaches in Nigeria's complex regulatory landscape.

Nigeria's experience with data protection offers valuable lessons for other countries facing similar regulatory challenges. By emphasizing the global significance of these developments, the paper can serve as a model for best practices in digital records management and data protection.

This paper examines the implications of the NDPR, the NDPA, and NDPC for digital records management in Nigerian Government Agencies and Businesses. It establishes the path of these recent developments within the longer history of digital records in Nigeria, identifying drivers, milestones, and challenges.

It also attempts to analyze key provisions of the law and the Commission's strategic priorities and assesses the opportunities and challenges agencies might face in implementation. It also explores the relationship between electronic records management and public organizational credibility in Nigeria and the potential of data-driven regulatory compliance approaches to assist organizations in navigating Nigeria's complex regulatory landscape. The paper offers recommendations to guide implementation.

2. Methodology

This paper employs a qualitative research approach, it combines a comprehensive literature review with relevant policy analysis. The literature review includes academic articles, reports, and case studies on digital records management and data protection both in Nigeria and globally. Specifically, the policy analysis focuses on the Nigeria Data Protection Regulation (NDPR) 2019 and the Nigeria Data Protection Act (NDPA) 2023. All the sources selected were based on their relevance, currency, and credibility. The aim of this analysis is to identify themes, challenges, and opportunities key to the evolution of Nigeria's digital records management landscape.

3. A History of Digital Record Management in Nigeria

Digital record management in Nigeria is very recent. It only dates back to the 1990s when small computers were adopted in government ministries, departments, and agencies (MDAs). Almost all early digitization efforts focused on converting paper records into digital formats for storage and retrieval, often within individual MDAs (Abdulkarim, 2019).

The expansion of internet connectivity and e-government initiatives in the 2000s accelerated the shift towards digital records and processes (Adeyemo, 2011).

The National Information Technology Development Agency (NITDA) was established in 2001 with the mandate to coordinate IT policy and promote e-government. Many MDAs adopted electronic document and records management systems (EDRMS) to automate workflows and manage born-digital records.

It is important to note here, though, that the transition to digital records was not without its challenges. Many digitization and EDRMS projects were piecemeal, without common standards or interoperability (Abdulkarim, 2019). Records management policies and practices often did not keep pace with technological change (Adeyemo, 2011). Data

privacy and security concerns grew with the explosion of personal data collection and use. These challenges began to highlight the complexity of the digital transformation process and the need for robust regulatory frameworks.

Formal regulations came into force in 2019 with the development of the Nigeria Data Protection Regulation (NDPR) by the National Information Technology Development Agency (NITDA). The NDPR established data protection principles and imposed obligations upon both public and private sector entities (NITDA, 2019). It increased awareness of data privacy concerns and was the foundation for developing a more comprehensive legislative framework.

We can trace this all the way back to 2007 with the establishment of the National Information Technology Development Agency (NITDA) Act, which tasked the agency with overseeing the country's IT development and ensuring the security and integrity of electronic data and records.

Building on this foundation, Nigeria's regulatory framework continued to evolve. The 2011 implementation of the Freedom of Information (FOI) Act mandated the accessibility of public records, including digital ones, to promote transparency and accountability. The Electronic Transactions Act provided legal recognition for digital records and stipulated their authenticity and security requirements in the same year. As Nigeria's digital transformation progressed, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 and the Data Protection Regulation of 2019 further strengthened the country's commitment to safeguarding the integrity and security of its digital information assets.

In 2011, the Freedom of Information (FOI) Act was implemented to make it easier for people to get hold of public records, even digital ones. This was done to make the government more open and accountable. That same year, the Electronic Transactions Act gave digital records legal recognition and set rules for how they should be kept safe and authentic. As Nigeria became more digital, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 and the Data Protection Regulation of 2019 made it even clearer that the country was serious about protecting its digital assets and keeping them safe.

This evolution of regulation has presented challenges and opportunities for government entities, but overall, progress has been made in establishing a framework for effectively managing Nigeria's digital records.

For instance, implementing the Treasury Single Account (TSA) in 2015 marked a major step towards digital financial records management in Nigeria to enhance transparency and accountability (Yusuf & Chiejina, 2015).

The NDPA's most recent enactment in 2023 and establishing the NDPC as a data protection authority also marked a new chapter. The Act provides a baseline that will guide digital records management in line with global standards on data protection. It presents an opportunity to address long-standing challenges and enhance trust in Nigerian data records in the digital age. The NDPA's role in shaping the future of data protection in Nigeria is major.

4. Six Key Provisions of the NDPA and Implications for Digital Records Management

The NDPA establishes principles and obligations for data processing that impact digital records management practices in businesses and government agencies significantly. These provisions represent a paradigm shift in how organizations approach data handling and storage.

The NDPA, 2023, lists these six provisions:

- The Principles of fair and lawful processing, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality (NDPA, 2023, Section 24). Businesses and Agencies must align their records management policies and practices with these principles.
- Obligations to implement technical and organizational measures to ensure data security (NDPA, 2023, Section 29). Businesses and Agencies must all upgrade systems and processes to meet security requirements.
- The Rights of data subjects, including rights to access, rectification, erasure, and portability (NDPA, 2023, Sections 34-38). Agencies will need mechanisms to facilitate the exercise of these rights.
- The Requirement for data protection impact assessments (DPIAs) for high-risk processing (NDPA, 2023, Section 28) requires agencies to conduct DPIAs for sensitive records and systems.
- Restrictions on cross-border transfers of personal data (NDPA, 2023, Sections 41-43). Businesses and Agencies that share data internationally will need to take appropriate precautions.

- The Powers of the NDPC to register data controllers, issue guidance, conduct audits, investigate complaints, and impose penalties for noncompliance (NDPC, 2023). Businesses and Agencies must proactively engage with and respond to Commission oversight.

To comply with these provisions, government agencies and businesses must develop data protection policies, implement security measures, and regularly assess their digital records management practices. This may require significant investments in technology, infrastructure, and personnel training (Adejumo et al.,2021). To illustrate, government agencies have had to upgrade their systems to align with these principles, ensuring data accuracy and confidentiality in their records management. The Nigeria Data Protection Commission (NDPC) has already imposed fines on a varied audience for data violations, demonstrating its regulatory authority; this type of proactive enforcement shows its commitment to compliance.

- Four Banks and Three Companies: The NDPC fined four banks and three other companies a total of ₦400 million for breaching citizens' data. These infractions were related to unauthorized access, misuse, or mishandling of personal information (NDPC, 2024).
- Increased Compliance: The NDPC's actions have improved compliance with the Nigeria Data Protection Act. Initially, private sector compliance was around 49%, but it has now risen to over 55%. Similarly, public sector compliance has increased from 4% to 15% (NDPC, 2024).
- Global Impact: Nigeria's data ecosystem, valued at over ₦10 billion, has gained prominence globally due to the Data Protection Act 2023. Nigeria now shares experiences with other nations like Kenya, Ghana, China, Singapore, and Malaysia. In fact, Nigeria will host the 2024 All African Data Protection Commission's event, with participation from about 30 countries (NDPC, 2024).

These examples highlight the NDPC's commitment to safeguarding citizens' data and promoting best practices. We must also pay attention to the important ethical considerations related to Data Protection and Digital records management. Issues related to privacy, security and access/use of personal data must be addressed both to ensure public trust and compliance with global standards. The NDPA also introduces ethical considerations that must be carefully addressed by organizations for implementation. These considerations include leveraging data for societal benefit and safeguarding individual privacy rights, ensuring equitable access to digital services while maintaining data security measures, guarding against biases in data collection and processing methodologies, and considering the societal impacts of data protection measures. Every organization must develop ethical frameworks that guide their implementation. These frameworks must uphold fundamental human rights and core societal values. This will help organizations ensure their data protection practices meet regulatory standards and contribute to the ethical fabric of Nigeria's ecosystem.

5. Explaining the Relationship between Electronic Records Management and Public Organizational Credibility

Proper records management, whether electronic or print, is increasingly recognized as crucial for public organizations' credibility (Sanderson &Ward, 2003). Records represent reliable and verifiable sources of evidence that can prove decisions, actions, and transactions, thereby supporting accountability (Wamukoya, 2000).

Electronic records management and organizational credibility are linked. Records management facilitates free information flow, which is essential for transparency (De Wet & Du Toit, 2000).

Well-managed records act as control systems that reinforce auditing processes and provide a track record to identify any irregularities that could undermine credibility (Palmer, 2000).

Electronic records management supports good governance and credibility in several ways:

- It provides evidence for accountability, enabling organizations to demonstrate they have met their financial, legal, social, and moral obligations (Cox & Wallace, 2002).
- It supports financial management and combats corruption by maintaining accurate financial records (World Bank, 2000).
- It enables organizations to deliver effective services and protects citizens' rights by ensuring access to reliable information (Hassan, 2007).
- It helps preserve institutional memory and continuity, enhancing operational efficiency and supporting credibility (Hase & Galt, 2010).

This basically means that government agencies and businesses must prioritize the development and implementation of effective electronic records management systems, regularly assess their performance, and continuously improve their practices to maintain public trust (Egwunyenga, 2018)

For instance, a study by Abdulkarim (2019) found that government agencies that implemented robust electronic records management systems experienced improvements in public trust and efficiency. Additionally, comparing these practices with international standards can highlight best practices and areas for improvement

In Nigeria, government agencies and businesses need to prioritize electronic records management. This is not just a good idea but a must if they want to follow the NDPA (Nigeria Data Protection Act) and build and maintain the public's trust and belief in them.

6. Data-Driven Regulatory Compliance in Nigeria

As has been highlighted already, the regulatory landscape in Nigeria is complex. Businesses face all sorts of challenges from multiple authorities, inconsistencies in regulations, bureaucracy, corruption, and infrastructure constraints (Oguejiofor et al., 2023). Against this backdrop, adopting data-driven regulatory compliance approaches offers transformative potential to assist organizations in navigating compliance hurdles more efficiently.

Data-driven compliance involves using data analytics, artificial intelligence, and advanced technologies to enhance compliance processes' efficiency, accuracy, and agility (Oguejiofor et al., 2023). By harnessing accurate and official data, organizations can make informed decisions, identify risks, and proactively address issues.

Key components of data-driven compliance include (Oguejiofor et al., 2023)

- Gathering data from diverse sources
- Employing analytical tools to extract insights and detect anomalies
- Evaluating risks based on data-driven models
- Utilizing AI and machine learning to automate compliance tasks
- Implementing real-time monitoring to track metrics and trigger alerts
- Anticipating regulatory changes and adjusting strategies proactively

Real-world case studies across sectors in Nigeria demonstrate the transformative power of data-driven solutions (Oguejiofor et al., 2023). Organizations have leveraged data to automate processes, achieve real-time monitoring, enhance compliance, reduce costs, and improve efficiency and reputation.

For data-driven compliance to succeed in Nigeria, organizations must invest in data infrastructure, automation, and ethical data practices. Collaboration with regulators, commitment to data privacy, and transparency are also key. Meanwhile, regulators should embrace RegTech solutions, foster data-sharing platforms, ensure consistency in enforcement, and adopt regulations to keep pace with technological advancements (Oguejiofor et al., 2023).

Ultimately, data-driven regulatory compliance offers a promising path for organizations to navigate Nigeria's complex regulatory terrain more efficiently, proactively manage risks, and contribute to business sustainability. It also empowers regulators to enhance oversight and enforcement, fostering a more transparent and compliant environment.

Recommendations

To seize the opportunities and navigate the challenges presented by the NDPA, Government Agencies, and Businesses should consider the following recommendations:

- Develop a strategic plan for aligning digital records management practices with NDPA requirements based on a comprehensive assessment of current gaps and risks.
- Prioritize investments in upgrading technological infrastructure and systems to meet data security and privacy requirements.
- Revise and harmonize records management policies, procedures, and metadata standards to incorporate data protection principles and obligations.
- Provide training and guidance for records management personnel on data protection responsibilities and best practices.

- Establish governance structures and processes to oversee data protection compliance, including the designation of data protection officers.
- Conduct DPIAs for high-risk records processing activities and implement risk mitigation measures.
- Develop processes to facilitate data subject rights, including access, rectification, erasure, and portability.
- Review and strengthen arrangements for secure cross-border data sharing, in line with NDPA requirements.
- Engage proactively with NDPC guidance, registration, and compliance monitoring activities.
- Foster dialogue and collaboration with internal and external stakeholders on data protection issues and solutions.

Establishing clear timelines, allocating adequate resources, and fostering a culture of continuous improvement and learning within government agencies and businesses are crucial to ensuring the effective implementation of these recommendations (Oluwole et al., 2020).

7. Conclusion

The NDPA and NDPC are a big step forward in managing and protecting digital records. The act and the new commission address long-standing challenges and align practices with global standards by providing a legal framework and independent regulatory oversight. These include the need for substantial investment in infrastructure and training, potential conflicts with existing regulations, and the risk of creating barriers for small businesses. Future research should explore these challenges in-depth and investigate practical solutions for implementation across different sectors, future research should also explore the impact of these regulations on the economy.

Government Agencies and Businesses that adopt these initiatives immediately through strategic planning, capacity building, and stakeholder engagement will enhance the integrity, security, and trust in their digital records as assets for good governance and service delivery.

When interpreting the data, it's important to consider alternative perspectives, including the potential challenges and unintended consequences of the NDPA. For example, increased compliance costs for small businesses should be considered. Furthermore, it's crucial to explore the wider implications for international data protection standards and Nigeria's position in the global data economy.

While many challenges remain, the NDPA provides a baseline to guide the management of digital records in the public interest.

Organizations can also navigate complex regulations by prioritizing data-driven regulatory compliance and building stakeholder trust. Government agencies as Regulators, too, can harness data-driven tools to enhance oversight, detect non-compliance, and create a more transparent and level playing field.

The utilization of digital records management, data protection regulations, and data-driven compliance in Nigeria presents an opportunity for change. With this kind of vision, collaboration, and commitment, organizations can fully unlock the hidden value of data while safeguarding rights and building public trust. This is important in Nigeria's march towards a transparent, accountable, and digitally driven future.

References

[1] Abdulkarim, M. (2019). Challenges of digital records management in Nigerian public sector. Records Management Journal, 29(4), 377-392. https://doi.org/10.1108/RMJ-01-2019-0004

[2] Adejumo, A. V., Ayo, C. K., & Adejumo, O. O. (2021). An appraisal of data protection regulation in Nigeria: challenges and prospects. International Journal of Law and Information Technology, 29(1), 51-72.

[3] Aderonke, A. A., & Ayo-Oyebiyi, G. T. (2019). Data-driven decision making in the Nigerian public sector: challenges and opportunities. Journal of Public Administration and Policy Research, 11(1), 1-8.

[4] Adeyemo, A. B. (2011). E-government implementation in Nigeria: An assessment of Nigeria's global e-government ranking. Journal of Internet and Information Systems, 2(1), 11-19.

[5] Akaba, T. I., Norta, A., Udokwu, C., & Draheim, D. (2020). A Framework for the Adoption of Blockchain-Based e-Procurement Systems in the Public Sector. In Lecture notes in computer science (pp. 3–14). https://doi.org/10.1007/978-3-030-44999-5_1

[6] Cox, R. J. & Wallace, D.A. (2002). Archives and the public good: Accountability and records in modern society. London: Westport.

[7] De Wet, S., & Du Toit, A. (2000). The challenges of implementing a records management system at the national electricity regulator in South Africa. Records Management Journal, 10(2), 73-86.

[8] Egwunyenga, E. J. (2018). Records management practices and public service delivery in Nigeria. IOSR Journal of Humanities and Social Science, 23(5), 46-54.

[9] Ekong, I., Chukwu, E., & Chukwu, M. (2020). COVID-19 Mobile Positioning Data Contact Tracing and Patient Privacy Regulations: Exploratory Search of Global Response Strategies and the Use of Digital Tools in Nigeria. JMIR Mhealth and Uhealth, 8(4), e19139. https://doi.org/10.2196/19139

[10] Guto, R., & Jumba, A. H. (2021). Relationship between Electronic Records Management and Public Organization Credibility: Critical Analysis of Literature Review. Journal of African Interdisciplinary Studies, 5(3), 52-67.

[11] Guto, R., & Jumba, H. (2021). Relationship between Electronic Records Management and Public Organization Credibility: Critical Analysis. . . ResearchGate. https://www.researchgate.net/publication/350707343_Relationship_between_Electronic_Records_Management_and_Public_Organization_Credibility_Critical_Analysis_of_Literature_Review

[12] Hase, S., & Galt, J. (2010). Record Management myopia: A case study. Records Management Journal, 21(1), 36-45.

[13] Hassan, K. (2007). 'Court Records Management in Malaysia. Personal Communication,' June 10, 2015.

[14] Kotoroi, G. (2023). Constraints facing African academic libraries in applying electronic security systems to protect library materials. International Journal of Librarianship, 8(1), 31–48. https://doi.org/10.23974/ijol.2023.vol8.1.272

[15] Mosweu, O., & Rakemane, D. (2020). The role of records management in ensuring good governance in Africa. S.A. Argiefblad, 53, 103–123. https://doi.org/10.4314/jsasa.v53i1.8

[16] National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation. Abuja: NITDA. https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

[17] Nigeria Data Protection Commission (NDPC). (2023). Nigeria Data Protection Act 2023. Abuja: NDPC. [URL forthcoming]

[18] The Holy Bible, New King James Version, Copyright © 1982 Thomas Nelson. All rights reserved.

[19] Nigeria Data Protection Commission (NDPC). (2023). Nigeria Data Protection Annual Report 2023. Abuja: NDPC. [URL forthcoming]

[20] Nigeria Data Protection Commission (NDPC). (2023). Nigeria Data Protection Strategic Roadmap and Action Plan 2023-2027. Abuja: NDPC. [URL forthcoming]

[21] Oguejiofor, B.B., Omotosho, A., Abioye, K.M., Alabi, A.M., Oguntoyinbo, F.N., Daraojimba, A.I., & Daraojimba, C. (2023). A Review on Data-Driven Regulatory Compliance in Nigeria. International Journal of Applied Research in Social Sciences, 5(8), 231-243.

[22] Oguejiofor, N. B. B., Omotosho, N. A., Abioye, N. K. M., Alabi, N. a. M., Oguntoyinbo, N. F. N., Daraojimba, N. a. I., & Daraojimba, N. C. (2023). A REVIEW ON DATA-DRIVEN REGULATORY COMPLIANCE IN NIGERIA. International Journal of Applied Research in Social Sciences, 5(8), 231–243. https://doi.org/10.51594/ijarss.v5i8.571

[23] Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. Computers & Security, 117, 102697. https://doi.org/10.1016/j.cose.2022.102697

[24] Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. Computers & Security, 117, 102697. https://doi.org/10.1016/j.cose.2022.102697

[25] Oluwole, O. A., Adebiyi, S. O., & Adeaga, O. (2020). Electronic records management practices in Nigerian public organizations: Issues and challenges. Records Management Journal, 30(2), 149-169.

[26] Palmer, M. (2000). Records management and accountability versus corruption, fraud, and maladministration. Records Management Journal, 10(2), 61-72.

[27] Sanderson, M. & Ward, S. (2003). Records management mission critical. Library and Information Update, 23,1-7.

[28] Ufua, D. E., Emielu, E. T., Olujobi, O. J., Lakhani, F., Borishade, T. T., Ibidunni, A. S., & Osabuohien, E. S. (2021). Digital transformation: a conceptual framing for attaining Sustainable Development Goals 4 and 9 in Nigeria. Journal of Management & Organization, 27(5), 836–849. https://doi.org/10.1017/jmo.2021.45

[29] Wamukoya, J. (2000). Records and archives as a basis for good government: implications and challenges for records managers and archivists in Africa. Records Management Journal, 10(1), 23-33.

[30] World Bank. (2000). Managing records as the basis for effective service delivery and public accountability in development: An introduction to core principles for staff of the World Bank and its partners. [Online] Available at: http://web.worldbank.org/. [Accessed: 10 Jan,2021].

[31] Yusuf, M. M., & Chiejina, N. (2015). Anti-graft war: one economy, one account. Sunday Nation, 9(8), 71-76