

**EVALUATING NIGERIA'S DATA PROTECTION ACT AND ITS EFFECTIVENESS IN
THE DIGITAL AGE**

By

Amarachi Aaron Anyanwu

300 Level Law Student @ COLLEGE OF LAW, AFE BABALOLA UNIVERSITY ||
AANYANWUWHILLZ@GMAIL.COM

ABSTRACT

With the rapid pace of digitalisation and the rise of data-driven technologies, the issue of data protection has become increasingly important, as personal data is now widely seen as a valuable asset. In response to this development, the Nigerian Data Protection Act establishes a legal framework designed to safeguard individuals' data rights. However, like many laws in Nigeria, its practical impact is limited by challenges such as weak enforcement mechanisms and gaps within the existing legal structure. This article, therefore, examines the Nigerian Data Protection Act, with a focus on assessing its effectiveness and continued relevance in the digital age. The study adopts a doctrinal research methodology.

Keywords: *Data, Data Protection, Artificial Intelligence, Digitalisation, Digital age.*

1.0 Introduction

The rapid growth in digitalization has made data protection a major concern, as data has become a form of currency. Gone are the days when organizations collected data merely for record-keeping; today, personal and non-personal data is collected to drive insights, inform decisions, and create value. Data is shaping the world on a global scale,⁹⁰ and in the coming future, it will be almost impossible to do business without data.

Digitalization is the integration of digital technologies and advancements into all aspects of business, society and life in general. It involves the use of data to create new value. This development has led to the collections of various forms of data, including biometrics, financial, health and online behaviour data. Given that data can easily be accessed, this ease can lead to data misuse, which could cause infringement of data privacy rights, Identity theft, Financial Fraud, Surveillance, legal liabilities, discrimination and loss of trust in digital systems.⁹¹

Data protection has become a major issue due to the rise of advanced digital technology and sophisticated cyber and digital threats. This has inspired a new wave of comprehensive frameworks in various countries which are aimed to protect individuals and their data. One of such frameworks is the Nigerian Data Protection Act 2023, which was enacted to protect individuals personal data, safeguard data privacy and ensure lawful measures are adopted when handling data.

2.0 Legal Framework for Data Protection in Nigeria

As discussed in previous paragraphs it has been emphasized that the rise of digitalization has increased data collection, due to this there must be laws to protect individual's personal data. As a result, there is a need for legal frameworks to protect individuals and their legal frameworks. The Nigerian Data Protection Act 2023, this is the law that governs data protection and related matters. It is the privacy legal instrument for data protection. Privacy protection is a part of the fundamental human right enjoyed by every citizen, this right extends to data protection. This section will examine the legal frameworks for Data Protection in Nigeria, especially the NDPA 2023.

2.1 Historical development

Before the enactment of the Nigerian Data Protection Act, data protection in Nigeria relied on patchwork regulations; the only regulation available that supported, regulated and promoted data

⁹⁰ Alius, "The Growing Importance of Data in the Digital Economy - Technology Org" (*Neurotechnology*, UAB, September 11, 2025) <<https://www.technology.org/2025/09/11/the-growing-importance-of-data-in-the-digital-economy/>> accessed January 5, 2026.

⁹¹ Sustainability Directory, "What Are the Implications of Data Misuse? → Question" *ESG → Sustainability Directory* (October 29, 2025) <<https://esg.sustainability-directory.com/question/what-are-the-implications-of-data-misuse/>> accessed January 6, 2026.

privacy and protection was the right to privacy stipulated in section 37 of the 1999 Constitution.⁹² In 2019 The National Information Technology Development Agency developed the Nigerian Data Protection Regulation, and it became the legally accepted framework for data privacy and protection. The need for a more elaborate codification that would be enforceable in all superior courts, hence on the 12th of June 2023, President Bola Ahmed Tinubu signed the Nigerian Data Protection Act into law.⁹³

2.2 Objectives

This section seeks to explain the aims of the NDPA2023, the goal the act seeks to achieve is regulating the processing of personal data in Nigeria and ensuring that it is enforced by organizations and businesses in Nigeria. The act provides for the objectives of the act, it states that it is to safeguard the data processing of citizens data as guaranteed by the 1999 CFRN. One of the primary objectives of the act is to provide regulations that ensure the processing of data is lawful, provide means to seek redress in the event that there is a breach of data privacy, establish a commission that oversees data protection and privacy issues and strengthen the foundation of the nation's digital economy.

Overall, the objective demonstrates the act's commitment to balancing technological advancement with the protection of individual rights in Nigeria's evolving digital economy.⁹⁴

2.3 Key provisions

In the following paragraphs we will discuss the provision of the NDPA 2023, it is important to establish that the act provides for several provisions which aim at regulating the processing of personal data and safeguarding the privacy of individuals. The second provision that would be examined are the rights of data subjects, this section emphasizes that the person who owns the data has the right to know whether the organisation is collecting or using their personal data, why it is being collected, what it is being used for, what type of data is being collected and how long it will be kept for. Individuals also have the right to get a copy of their personal data, ask for the data to be deleted, and restrict their use of data for certain information. Data controllers must delete personal data without delay when it is no longer needed or when there is no lawful reason to keep it.⁹⁵ This section of the act strengthens transparency, accountability and control by giving individuals power over how their personal data is handled, however this section has some gaps

⁹² Constitution of the Federal Republic of Nigeria 1999 (as amended) s 37.

⁹³ Ifeanyi Okonkwo, "Adeyemi Owoade, Overview of the Nigerian Data Protection Act" Jackson, Etti & Edu (Jul 11 2023) <<https://a.storyblok.com/f/302089/x/ac8dcf7542/overview-of-the-new-nigerian-data-protection-act-ndpa-2023.pdf>> accessed January 5, 2026.

⁹⁴ Nigerian Data Protection Act 2023 s1.

⁹⁵ NDPA 2023 s34

which are that “unreasonable delay” was not defined, this can give data controllers room to delay responding to request while claiming they are acting within a reasonable timeframe and there is no timeline in which a request should be fulfilled, this weakens enforcement.

The next provision is the obligation of controllers and processors, and it states in simple terms that the data controller and processors have the duty to protect the subject's data, keep personal data secure and provide necessary information to show compliance and notify the commission of the engagement of a new processor.⁹⁶ In case there is a data breach the data processor must notify the data controller and they must come together to figure out how to go about it and find a solution to the breach. In the case that the data breach will risk the individual's life the data controller has the duty to inform the commission within 72 hours.⁹⁷ When a new data processor is hired by the data controller, the duty to ensure that the processor follows the rules of the act is on the controller.⁹⁸

Finally the final provision we would be examining is the penalties where there is noncompliance of enforcement order issued in Section 47,⁹⁹ the offender may be punished with a fine or imprisonment for up to one year. The court has the discretion to impose both a fine or imprisonment.

3.0 Institutional and Enforcement Framework

The effectiveness of any regulatory framework depends largely on the enforcement. There is a formal body whose responsibility is to ensure the enforcement of the Nigeria Data Protection Act and it is the Nigerian Data Protection Commission (NDPC). The NDPC is charged with oversight and enforcement functions. This institutional framework plays a huge role in translating legal provisions into practical compliance, it promotes awareness and registers data controllers and processors for effective enforcement.¹⁰⁰

3.1 Powers of the NDPC

As mentioned in previous paragraphs the NDPC is the central enforcement body under the Nigeria Data Protection Act. The powers that the act has vested in the commission are very important because they enable real data protection in practice. The powers of the NDPC are not merely

⁹⁶ NDPA 2023 s29

⁹⁷ Ifeanyi Okonkwo, “Adeyemi Owoade, Overview of the Nigerian Data Protection Act” Jackson, Etti & Edu (Jul 11 2023) <<https://a.storyblok.com/f/302089/x/ac8dcf7542/overview-of-the-new-nigerian-data-protection-act-ndpa-2023.pdf>> accessed January 19, 2026.

⁹⁸ NDPA 2023 s40

⁹⁹ NDPA 2023 s47

¹⁰⁰ Dicer, “Elevate Your Data Protection Standards” (*Amanitrust*, May 4, 2025) <<https://amanitrust.ng/blog/the-role-of-ndpc-ensuring-data-protection-compliance-in-nigeria>> accessed January 19, 2026.

administrative but are intended to ensure compliance, accountability, and protection of citizens. In exercising its mandate, the NDPC is empowered to promote awareness and improve data understanding of data protection of personal data.¹⁰¹ Receive complaints from individuals that have had their data protection rights violated.¹⁰² Offer recommendation and advice on any matter concerning data protection.¹⁰³ Evaluate the extent to which personal data protection standard for cross border transfer is adequate.¹⁰⁴ Submit legislative proposals that could possibly strengthen data protection in Nigeria. Through the regulative powers the commission is able to identify breaches, assess the extent of data protection violations and take appropriate steps to prevent continued misuse of personal data.

3.2 Enforcement mechanisms and sanctions

The protection of personal data under the Nigerian Data Protection Act of 2023 is not only about recognising rights and obligations, it is fundamentally about ensuring that those rights can be enforced and that when breaches occur they attract meaningful consequences. In Nigeria's regulatory system, enforcement mechanisms and sanctions are essential if the law is to move beyond paper commitments to actual impact. With this in mind, the Act establishes a suite of mechanisms, including complaints procedures, investigative powers, administrative fines, corrective orders, and remedies available to data subjects which are all designed to promote compliance and protect individuals whose personal data is mishandled or misused.¹⁰⁵

Recent enforcement actions by the Nigeria Data Protection Commission (NDPC) suggest a gradual shift from a largely symbolic regulatory framework to a more assertive enforcement regime. In 2025, the NDPC imposed an administrative fine of ₦766,242,500 on MultiChoice Nigeria for violations of the Nigeria Data Protection Act, including intrusive, unnecessary and disproportionate data processing practices, as well as failure to cooperate with regulatory investigations.¹⁰⁶ This marked one of the largest data protection fines in Nigeria's history and signalled a growing willingness by the Commission to hold major corporate actors accountable. Beyond these headline case, the NDPC has repeatedly warned banks, insurance companies and

¹⁰¹ SAN FCI Arb (U K) OM Atoyebi, "An Appraisal of the Powers and Functions of the Nigeria Data Protection Commission in Data Protection in Nigeria" (*Omaplex Law Firm*, July 23, 2024) <<https://omaplex.com.ng/an-appraisal-of-the-powers-and-functions-of-the-nigeria-data-protection-commission-in-data-protection-in-nigeria/>> accessed January 19, 2026.

¹⁰² *ibid*

¹⁰³ NDPA 2023 s5(m)

¹⁰⁴ SAN FCI Arb (U K) OM Atoyebi, "An Appraisal of the Powers and Functions of the Nigeria Data Protection Commission in Data Protection in Nigeria" (*Omaplex Law Firm*, July 23, 2024) <<https://omaplex.com.ng/an-appraisal-of-the-powers-and-functions-of-the-nigeria-data-protection-commission-in-data-protection-in-nigeria/>> accessed January 19, 2026.

¹⁰⁵ NDPA 2023 s 46.

¹⁰⁶ Babatunde Bamigboye, "NIGERIA - NDPC Fines Multichoice Nigeria N766,242, 500 for Violating NDP Act" (*NADPA-RAPDP*) <<https://www.rapdp.org/index.php/en/node/222>> accessed January 20, 2026.

gaming organisations of impending sanctions for non-compliance with data protection audits, thereby indicating a broader regulatory shift towards proactive supervision rather than reactive complaint-handling. Taken together, these developments reflect an emerging enforcement culture that, while still in its early stages, suggests that the NDPA 2023 is beginning to acquire real deterrent value in practice.

Nevertheless, it remains to be seen whether such sanctions will be applied consistently across sectors and sustained over time, particularly in light of Nigeria's broader challenges relating to regulatory capacity, political interference and judicial delays.

3.3 Remedies Available to Data Subjects

Harm in this context may encompass financial loss, reputational damage, or emotional distress and harms that are increasingly recognised in data protection jurisprudence globally. The availability of these remedies affirms that personal data protection is not merely an administrative compliance issue, but one that intersects with fundamental human dignity and personal autonomy.¹⁰⁷ That being said, challenges such as the high cost of litigation, delays in court processes, and limited public awareness of legal rights may restrict the practical use of these remedies by ordinary Nigerians unless supported by legal aid structures or public education campaigns. An illustrative real-world example of consent and data processing practices in Nigeria can be observed in the context of online banking platforms such as Guaranty Trust Bank's internet banking service. When customers access certain online banking services, the platform may display a notice indicating that by continuing to use the service, the user consents to the processing of their personal data by GTBank, its holding company, and subsidiaries as detailed in the bank's privacy policy. This is a form of notice-and-consent practice that aligns with the principle that data processing must be lawful and based on an identifiable legal basis, such as the data subject's consent.

4.0 Data Protection in the Digital Age

The rapid growth of digital technologies has fundamentally transformed how personal data is generated, collected, stored, and exploited. These developments have significantly increased both the volume and sensitivity of data being processed by public and private actors. As a result, traditional data protection principles are increasingly being tested by the scale, speed, and complexity of modern data processing operations.¹⁰⁸ In Nigeria, the challenge is particularly more

¹⁰⁷ NDPA 2023 s51.

¹⁰⁸ Abiodun Amuda-Kannike SAN, Shuaib Oniye and Yusuf Amuda-Kannike, "DATA PROTECTION LAWS IN NIGERIA: THE IMPACT OF AI AND TELECOM REGULATIONS ON E-COMMERCE SECURITY" (2025) 2 LexScriptio A Journal of the Department of Jurisprudence and Public Law 158.

due to the rapid adoption of digital services across banking, telecommunications, social media, and online retail, often without a commensurate growth in regulatory capacity or public awareness. The Nigerian Data Protection Act 2023 was enacted for this particular purpose. However, the effectiveness of the Act must be assessed against emerging digital realities such as AI-driven decision-making, big data profiling, fintech expansion, and cross-border e-commerce.¹⁰⁹

4.1 AI and big data

Artificial intelligence and big data analytics have become central to modern governance, commerce, and service delivery. AI systems depend on vast datasets to train algorithms capable of recognizing patterns, predicting behaviour, and making automated decisions. Big data, in turn, refers to extremely large and complex datasets generated from digital platforms, social media interactions, financial transactions, biometric systems, and Internet-of-Things (IoT) devices.¹¹⁰

One of the primary data protection challenges posed by AI and big data is mass data harvesting and secondary use. Personal data collected for one purpose is frequently repurposed for unrelated objectives such as targeted advertising, behavioural profiling, credit scoring, or political micro-targeting without meaningful consent. This practice undermines the principles of purpose limitation and data minimisation recognised in modern privacy law.¹¹¹

In the Nigerian context, oversight of AI remains underdeveloped as Nigeria does not have a specific regulatory framework to govern the use of AI. While the NDPA 2023 provides general safeguards such as lawful processing, consent, and security obligations, it does not contain detailed rules governing algorithmic accountability, automated decision-making, or explainability of AI outcomes. This creates a regulatory gap in relation to modern data-driven technologies.¹¹²

5.0 Comparative Analysis

A comparative analysis provides a useful lens for evaluating the strengths and weaknesses of Nigeria's data protection framework under the Nigeria Data Protection Act 2023 (NDPA). By examining how other African jurisdictions regulate personal data, it becomes possible to identify best practices that Nigeria can adopt to strengthen enforcement, close regulatory gaps, and respond more effectively to emerging digital technologies. South Africa offers a particularly strong point

¹⁰⁹ Edidiong Otong, "Exploring Artificial Intelligence (AI), Data Protection, And Digital Rights in Nigeria's Regulatory Framework and Global Standard" (2024) 12 *Uniuoy Law Journal*.

¹¹⁰ Kalada DS Nonju and Benjamin Ihua-Maduenyi, "International Journal of Research and Innovation in Social Science" (2024) 5 *International Journal of Research and Innovation In Social Science*.

¹¹¹ Ifeoma Peters, "Emerging Technologies: Implications of AI, Big Data, IoT, Blockchain, and Biometrics on Privacy and Compliance – 1 - DNL Legal and Style" (*DNL Legal and Style - Blazing The Trails, Providing World Class Legal Services*, December 4, 2025) <<https://dnlegalandstyle.com/dnl/emerging-technologies-implications-of-ai-big-data-iot-blockchain-and-biometrics-on-privacy-and-compliance-1/>> accessed January 20, 2026.

¹¹² Edidiong Otong, "Exploring Artificial Intelligence (AI), Data Protection, And Digital Rights in Nigeria's Regulatory Framework and Global Standard" (2024) 12 *Uniuoy Law Journal*.

of comparison because it has one of the most comprehensive and mature data protection regimes on the continent. Its Protection of Personal Information Act 4 of 2013 (POPIA) is widely regarded as being closely aligned with international standards, particularly the EU General Data Protection Regulation (GDPR). Unlike Nigeria's relatively new statutory framework, POPIA has been in force since 2020 and has generated practical enforcement experience through regulatory actions, fines, and judicial oversight.¹¹³ This section therefore examines South Africa's POPIA as a comparator to Nigeria's NDPA, focusing on its legal framework, regulatory authority, enforcement mechanisms, and practical effectiveness, with the aim of drawing lessons relevant to Nigeria's evolving data protection regime.

5.1 Protection of Personal Information Act (POPIA), South Africa

The Protection of Personal Information Act 4 of 2013 (POPIA) is South Africa's principal data protection legislation. It was enacted to give effect to the constitutional right to privacy under section 14 of the Constitution of the Republic of South Africa and to regulate the processing of personal information by both public and private bodies.¹¹⁴ Although the Act was passed in 2013, it became fully operational on 1 July 2020 following a commencement proclamation, with a one-year grace period for compliance.¹¹⁵

POPIA is structured around eight core conditions for the lawful processing of personal information:

1. Accountability
2. Processing limitation
3. Purpose specification
4. Further processing limitation
5. Information quality
6. Openness
7. Security safeguards
8. Data subject participation.¹¹⁶

¹¹³ Protection of Personal Information Act 4 2013.

¹¹⁴ Constitution of the Republic of South Africa 1996, s 14.

¹¹⁵ Proclamation No 21 of 2020.

¹¹⁶ POPIA 2023, s4

These conditions closely mirror the data protection principles found in international instruments such as the GDPR and resemble the principles now codified under Nigeria's NDPA 2023. For example, POPIA requires that personal data be processed lawfully and in a reasonable manner, collected for a specific purpose, and not retained longer than necessary.¹¹⁷ It also imposes strict obligations on responsible parties to implement appropriate technical and organisational measures to safeguard personal information against loss, damage, unauthorised access, misuse, breach or unlawful processing.¹¹⁸

In addition, POPIA provides extensive rights for data subjects, including the right of access to personal information, the right to request correction or deletion of inaccurate data, and the right to object to the processing of personal data, particularly for purposes such as direct marketing.¹¹⁹ These rights are similar in substance to those contained in Nigeria's NDPA but are more elaborately regulated through subsidiary regulations and formal guidance issued by South Africa's supervisory authority.

5.2 Enforcement Mechanisms and Sanctions under POPIA

Where a responsible party is found to have contravened the Act, the Information Regulator may issue an enforcement notice directing the party to take specified remedial action within a stated period of time.¹²⁰ In serious cases, POPIA authorises the imposition of administrative fines of up to R 10 million and/or imprisonment for a period not exceeding ten years.¹²¹ A notable example of POPIA's enforcement strength is the Dis-Chem Pharmacies case, where the Information Regulator fined a major retail pharmacy chain for unlawfully using customer contact details for direct marketing purposes without proper consent.¹²²

Here, WhatsApp provided stronger privacy protections to users in Europe, but the consent process was flawed for users in South Africa. In addition, the policy did not explain what the collected data would be used for, and WhatsApp failed to show that it had sufficient safeguards in place to protect users' data.¹²³ This allegedly violated POPIA's transparency and consent requirements.

¹¹⁷ POPIA 2023, s11.

¹¹⁸ POPIA 2023, s 19.

¹¹⁹ POPIA 2023, s 23-25

¹²⁰ POPIA 2023, s 95 (1) (a) (b).

¹²¹ POPIA 2023, s 109

¹²² Nomzamo Zondi (Information Regulator), "ENFORCEMENT NOTICE ISSUED TO DIS-CHEM DUE TO CONTRAVENTION OF POPIA" (*Information Regulator South Africa*, September 1, 2023)

<<https://infoeregulator.org.za/wp-content/uploads/2020/07/FINAL-MEDIA-STATEMENT-ENFORCEMENT-NOTICE-ISSUED-TO-DISCHEM-PHARMACIES-LTD.pdf>> accessed January 20, 2026.

¹²³ Tayla Pinto, "WhatsApp Enforcement Action" (*Michalsons*, April 28, 2025)

<<https://www.michalsons.com/blog/whatsapp-enforcement-notice-popia-breaches/77829>> accessed January 20, 2026.

POPIA adopts a relatively strict approach to cross-border data transfers.¹²⁴

This framework is closely aligned with the GDPR's adequacy and safeguard mechanisms and serves as a useful model for Nigeria, where cross-border data flows involving fintech platforms, cloud services and multinational tech companies are rapidly increasing.

Legal commentators have noted that POPIA's international compatibility enhances South Africa's attractiveness as a digital business hub while still maintaining strong privacy protections.¹²⁵ Nigeria's NDPA similarly aspires to GDPR-level alignment, but its effectiveness in regulating cross-border data transfers will depend on the development of clear adequacy standards and enforcement practice by the NDPC.

5.3 Comparative Lessons for Nigeria

South Africa's experience under POPIA offers several important lessons for Nigeria's evolving data protection regime:

First, clear regulatory guidance enhances compliance. The Regulator's publication of codes of conduct and guidance notes under POPIA has helped businesses understand their obligations and reduced interpretative uncertainty. Nigeria would benefit from a more aggressive issuance of sector-specific guidelines, particularly for fintech, AI and big data processing.¹²⁶

Secondly, strong sanctions create real deterrence. The availability of substantial fines and criminal penalties under POPIA appears to have encouraged greater corporate compliance. Nigeria's NDPA should be enforced with similar seriousness to prevent data controllers from treating regulatory penalties as a mere cost of doing business.¹²⁷

Finally, public awareness is critical. POPIA's impact has been reinforced by sustained public education campaigns and media coverage of enforcement actions. Nigeria must invest in similar awareness strategies to ensure that citizens understand their data protection rights and are willing to assert them. Nigeria is beginning to show enforcement maturity similar to jurisdictions such as

¹²⁴ POPIA 2023, s 72.

¹²⁵ DLA Piper, "Data Protection Laws in South Africa" *Data Protection Laws of the World* (January 6, 2025) <<https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA>> accessed January 20, 2026.

¹²⁶ Michalsons, "Protection of Personal Information Act Summary" (*Michalsons*, October 20, 2023) <<https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia>> accessed January 20, 2026.

¹²⁷ Zlatko Delev, "GDPR & Data Protection Laws in Africa: A Comparison" (*GDPR Local*, November 29, 2023) <<https://gdprlocal.com/gdpr-and-data-protection-laws-in-africa-a-comparison/>> accessed January 20, 2026.

South Africa and the European Union, although it still lags behind in institutional capacity, regulatory guidance and judicial consistency

6.0 Conclusion

The enactment of the Nigeria Data Protection Act 2023 represents a major milestone in Nigeria's journey towards a robust data protection regime. By replacing the Nigeria Data Protection Regulation with a comprehensive statutory framework, the Act strengthens the legal basis for protecting personal data and establishes the Nigeria Data Protection Commission as a dedicated enforcement authority. In summary, while Nigeria has made commendable legal progress through the Nigeria Data Protection Act 2023, the challenges posed by emerging technologies and digital business models show that law alone is not enough.

7.0 Recommendations

To strengthen data protection in Nigeria and ensure that the legal framework remains effective in the digital age, the following recommendations are proposed:

Improving Public Awareness and Digital Literacy

A major weakness in Nigeria's data protection framework is low public awareness. Many Nigerians are unaware of their rights to access, rectify or erase their personal data or to lodge complaints with the NDPC. The government, in partnership with civil society organisations and technology companies, should launch nationwide public education campaigns using radio, television, social media and community outreach. These campaigns should explain data protection rights in simple language and encourage citizens to challenge unlawful data practices.

Enhancing Cross-Border Data Protection Cooperation

Nigeria should strengthen international cooperation with foreign data protection authorities and align its standards with global frameworks such as the EU General Data Protection Regulation. This would improve Nigeria's credibility as a data-secure jurisdiction and ensure better protection for Nigerians' data processed abroad. Ultimately, data protection in the digital age is not merely a technical or regulatory issue; it is a human rights issue.

REFERENCES

Constitutional Provision

Constitution of the Republic of South Africa 1996, s 14.

Statutes

Protection of Personal Information Act 4 of 2013.

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

Protection of Personal Information Act 4 of 2013, s 11.

Protection of Personal Information Act 4 of 2013, s 19.

Protection of Personal Information Act 4 of 2013, ss 23–25.

Protection of Personal Information Act 4 of 2013, s 72.

Protection of Personal Information Act 4 of 2013, s 95(1)(a)–(b).

Protection of Personal Information Act 4 of 2013, s 109.

Proclamation No 21 of 2020.

Journal Articles

Nonju KDS and Ihua-Maduenyi B, ‘International Journal of Research and Innovation in Social Science’ (2024) 5 *International Journal of Research and Innovation in Social Science*.

Otong E, ‘Exploring Artificial Intelligence (AI), Data Protection, and Digital Rights in Nigeria’s Regulatory Framework and Global Standard’ (2024) 12 *Uniuyo Law Journal*.

Online Articles / Blog Posts / Web Sources

Alius, ‘The Growing Importance of Data in the Digital Economy – Technology Org’ (Neurotechnology UAB, 11 September 2025) <https://www.technology.org/2025/09/11/the-growing-importance-of-data-in-the-digital-economy/> accessed 5 January 2026.

DLA Piper, ‘Data Protection Laws in South Africa’ *Data Protection Laws of the World* (6 January 2025) <https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA> accessed 20 January 2026.

Michalsons, ‘Protection of Personal Information Act Summary’ (20 October 2023) <https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia> accessed 20 January 2026.

Peters I, ‘Emerging Technologies: Implications of AI, Big Data, IoT, Blockchain, and Biometrics on Privacy and Compliance’ (DNL Legal and Style, 4 December 2025) <https://dnlllegalandstyle.com/dnl/emerging-technologies-implications-of-ai-big-data-iot-blockchain-and-biometrics-on-privacy-and-compliance-1/> accessed 20 January 2026.

Pinto T, ‘WhatsApp Enforcement Action’ (Michalsons, 28 April 2025) <https://www.michalsons.com/blog/whatsapp-enforcement-notice-popia-breaches/77829> accessed 20 January 2026.

Sustainability Directory, ‘What Are the Implications of Data Misuse?’ (29 October 2025) <https://esg.sustainability-directory.com/question/what-are-the-implications-of-data-misuse/> accessed 6 January 2026.

Zlatko D, ‘GDPR & Data Protection Laws in Africa: A Comparison’ (GDPR Local, 29 November 2023) <https://gdprlocal.com/gdpr-and-data-protection-laws-in-africa-a-comparison/> accessed 20 January 2026.

Zondi N (Information Regulator), ‘Enforcement Notice Issued to Dis-Chem Due to Contravention of POPIA’ (Information Regulator South Africa, 1 September 2023)

<https://inforegulator.org.za/wp-content/uploads/2020/07/FINAL-MEDIA-STATEMENT-ENFORCEMENT-NOTICE-ISSUED-TO-DISCHEM-PHARMACIES-LTD.pdf> accessed 20 January 2026.