African Journal of Engineering and Environment Research Vol.7(2) 2025 pp 148- 162

ISSN: 2714-2264

Neeka, PraiseGod Siramene

Data Breach in Nigeria: A Case for Local Accountability

Corporate Services Division,
CEFPACS Consulting Limited,
FCT Abuja, Nigeria.
Email:praiseneeka@cefpacsconsultingltd.org.ng

The link to this publication is here

African Journal of Engineering and Environment Research Vol.7(2) 2025 pp 148- 162

ISSN: 2714-2264

DATA BREACH IN NIGERIA: A CASE FOR LOCAL ACCOUNTABILITY

Neeka, PraiseGod Siramene[1]; Neeka, Biragbara J[1]; Adat, Lilian C.[2].

[1]Corporate Services Division, CEFPACS Consulting Limited, FCT Abuja, Nigeria.
[2]Alliance Law Firm, Alliance House, 71 Ademola Street, SW Ikoyi, Lagos, Nigeria
Email:praiseneeka@cefpacsconsultingltd.org.ng
[Date received: April 2025. Date accepted: June 2025]

ABSTRACT

The rapid integration of technology into daily life has made the use and exchange of information inevitable, exposing individuals and institutions to rising risks of data breaches. In Nigeria, a nation undergoing rapid digital transformation, addressing these vulnerabilities is essential to fully realize the benefits of a burgeoning digital economy. Despite the enactment of the Nigeria Data Protection Act (NDPA) and the establishment of institutional frameworks, critical implementation deficiencies persist. These gaps, driven by corruption, underfunded agencies, and weak enforcement mechanisms, leave the nation's data ecosystem vulnerable to high-profile breaches. This article examines key incidents involving government and corporate actors and assesses the strengths and shortcomings of Nigeria's current data protection regime. It explores the broader implications for privacy, institutional trust, and national security, while emphasizing the urgent need to strengthen the Nigeria Data Protection Commission (NDPC), enforce accountability across sectors, and increase public awareness. Finally, it calls for local and international cooperation to build capacity, promote transparency, and ensure that both state and private entities adhere to best practices. Bridging the gap between legislation and enforcement is key to establishing Nigeria as a leader in data protection and digital governance in Africa.

Keywords: Cyber law, Cybersecurity, Data breaches, Data privacy, Data protection, Digital transformation.

1.0 INTRODUCTION

Data collection, particularly within the realm of big data analytics, operates at the intersection of privacy and disclosure. The immense value attached to data, whether for commercial, governmental, or illicit purposes, has intensified its acquisition and heightened vulnerabilities in data security systems globally. Nigeria presents a compelling case, reflecting both the challenges and opportunities in managing data governance within developing economies.

In the first quarter of 2023, Nigeria was ranked as the 32nd most affected country in terms of data breaches, highlighting its growing susceptibility to cyber threats. During this period, approximately 82,000 accounts were compromised, representing a significant 64 percent increase compared to the previous quarter. This sharp rise reveals systemic weaknesses in the country's data protection frameworks, further compounded by an accelerating pace of digital transformation.

This trend in Nigeria contrasts sharply with developments on the global stage during the same period. Data breaches worldwide showed a marked decline, with the number of compromised accounts reducing from 81 million in the last quarter of 2022 to 41.6 million in the first quarter of 2023. This represents a nearly 50 percent reduction and reflects advancements in cybersecurity measures and stricter enforcement of data protection laws in many regions. The disparity between global and Nigerian trends highlights the gap between countries with established safeguards and those still grappling with foundational challenges in cybersecurity.

Alarmingly, Nigeria's vulnerabilities appear to be worsening. In the first quarter of 2024, the incidents of reported data breaches more than doubled, marking a troubling increase over the previous year. This persistent rise underscores the urgent need for targeted reforms in Nigeria’s cybersecurity policies and infrastructure. Without meaningful interventions, the country risks becoming a hub for data breaches, with significant implications for individual privacy, institutional trust, and national security.

2.0 CASE STUDIES: LEARNING FROM REAL INCIDENTS

2.1 The Plaschema Data Breach (April 2022)

In April 2022, the Plateau State Contributory Health Care Management Agency (PLASCHEMA) experienced a significant data breach that exposed the personal data of over

37,000 individuals. This breach occurred due to the absence of essential security measures, such as encryption and authentication, across eleven data storage buckets. Sensitive personal information including names, dates of birth, residential details, and identification documents was left vulnerable and accessible to unauthorized parties.

The breach was detected by Website Planet researchers on April 3, 2022, who promptly reported it to the Nigeria Computer Emergency Response Team (ngCERT). Despite this intervention, the exposed repositories remained unsecured for nearly four months, until July 20, 2022. This delay in response not only underscored systemic lapses in data protection protocols, but also highlighted significant challenges in enforcing compliance under the Nigeria Data Protection Regulation (NDPR), which was the prevailing legal framework at the time.

The PLASCHEMA incident revealed critical shortcomings in Nigeria's data protection ecosystem, including insufficient oversight mechanisms and limited enforcement capacity. While the NDPR mandated security measures to safeguard personal data and outlined penalties for breaches, these requirements were inconsistently implemented, allowing such vulnerabilities to persist.

2.2 The Paradigm Initiative Discovery (June 2024)

The enactment of the Nigeria Data Protection Act (NDPA) aimed to address these deficiencies, introducing stricter compliance requirements and enforcement measures. However, even under this new framework, challenges remain. In June 2024, Paradigm Initiative discovered unauthorized websites hosting and selling Nigerians' personal and financial information for as little as ₦100.

One of such websites, AnyVerify.com.ng, displayed a disturbing array of data services, including access to National Identity Numbers (NINs), Bank Verification Numbers (BVNs), voter registration details, and even passport information. These services targeted a wide range of sensitive personal data, posing grave risks to individuals' privacy and security.

In response, Paradigm Initiative issued pre-action notices to government agencies, including the Nigerian Data Protection Commission (NDPC), National Identity Management Commission (NIMC), and Independent National Electoral Commission (INEC), and instituted legal action at the Federal High Court, seeking declaratory reliefs and orders to address the breach.

2.3 The Godfrey Nya Eneye Case (2013)

The importance of privacy rights in Nigeria's legal landscape is further illustrated by the case of Eneye v. MTN Nigeria Communication Ltd. In this case, the Plaintiff alleged that MTN disclosed his mobile phone number to third parties without his consent, resulting in frequent unsolicited messages. The Plaintiff argued that this unauthorized disclosure violated his fundamental right to privacy under Section 37 of the Nigerian Constitution. He further claimed infringements on his freedom of association and right to personal liberty.

MTN, in its defense, contended that the Plaintiff's phone number was not inherently confidential and that its exchange among acquaintances justified potential exposure. The company also argued that privacy violations typically involve more intrusive acts, such as surveillance or unauthorized physical access, none of which were alleged in this case.

The trial court dismissed MTN's arguments, ruling that the unauthorized disclosure of the Plaintiff's phone number and the resulting unsolicited messages constituted a breach of his right to privacy. The court emphasized that e-marketing practices common in the telecommunications industry do not absolve service providers of their obligation to respect individuals' privacy.

While the Plaintiff's claims regarding violations of his freedom of association and liberty were dismissed, the court issued an injunction restraining MTN from further unauthorized disclosures of the Plaintiff's phone number. Additionally, the court awarded ₦5,000,000 in exemplary damages to the Plaintiff. This judgment served as both compensation for the breach and a punitive measure to deter future misconduct by service providers.

3.0 THE NIGERIA DATA PROTECTION ACT 2023: BRIDGING LEGISLATIVE INTENT AND IMPLEMENTATION CHALLENGES

Since its enactment in June 2023, the Nigeria Data Protection Act (NDPA) has been the primary legislation providing a comprehensive legal framework for privacy and data protection in Nigeria. A series of bills were drafted in the continuous effort to establish robust legislation addressing data protection in Nigeria. The NDPA safeguards the right of data subjects and seeks to strengthen the legal foundation of the national digital economy in order that that nation can participate in regional and global economies through the beneficial and trusted use of personal data. The Act establishes the Nigeria Data Protection Commission saddled with responsibilities including the registration of data processors and data controllers of major

importance, and receiving complaints about violation of the Act or its subsidiary Act, as well as ensuring compliance with national and international personal data protection best practices and obligations.

The Act makes data controllers and processors to be saddled with the responsibility of implementing technical and organizational measures to secure personal data breach. It mandates the carrying out of a Data Privacy Impact Assessment (DPIA) before processing personal data that may result in high risk of right and freedoms of a data subject.

3.1 Key accountability provisions in the NDPA 2023

3.1.1 Data Controller and Processor of Major Importance (DCPMI) Registration

A data controller and processor shall be qualified as a DCPMI and required to register with the NDPC within six (6) months of coming into force of the NDPA, if it meets any of the following requirement: has access to a filing system and processes Personal Data of more than 200 Data Subjects in a six (6) month period; or provides commercial ICT services on any digital storage device that is owned by another party and has storage capacity; or processes Personal Data in the financial, communication, aviation, tourism, oil and gas, import and export, education, health, insurance and electric power industries. The DCPMI are categorised into three levels: Major Data Processing-Ultra High Level required to abide by global and highest attainable standards of data protection; Major Data Processing-Extra High Level mandated to abide by global best practices and Major Data Processing-Ordinary High Level to abide by global best practices.

3.1.2 Implementing Data Security Measures:

The NDPA 2023 puts an obligation on organisations to deploy adequate security measures to protect personal data from loss, misuse, alteration, damage, accidental or unlawful destruction or unauthorised access. The Act places clear duties and responsibilities on the data controllers and data processors in respect of handling data. They are to ensure that: Data Security measures are put in place; Record of data processing is kept; Risk assessment DPIA are carried out when required; Data is pseudonymised and encrypted; Access to data is quickly restored where there has been an accident whether physical or technical. Introduce and update new measures to accommodate evolving risks.

3.1.3 Data Privacy Impact Assessment

Data Controllers are mandated to conduct Data Privacy Impact Assessment (DPIA) to assess and identify any security risk associated with their data processing activities as well as safeguards to ensure adequate protection. DPIA is typically required where there is a change in processing activities involving evaluation or scoring; automated decision-making with legal or significant effects on the Data Subject rights; systematic monitoring; sensitive Personal Data; application of new technological solutions of deployment of innovative processes; processing of Personal Data in relation to vulnerable Data Subjects; healthcare; financial services; deployment of surveillance camera in public places; cross-border transfers; hospitality services and educational services. The DPIA is to be conducted regularly to ensure that processes, services and technologies are in compliance with data protection laws.

3.1.4 Designation of a Data Protection Officer

A DCPMI must appoint a Data Protection Officer (DPO) with knowledge of data protection and privacy laws who will carry out the tasks prescribed under the NDPA. The function of the DPO is to advise the data controllers and processors, monitor compliance with the Act and act as a contact point with the Commission on data processing related issues. The DPO may be an employee of the organization or engaged by a service contract.

3.1.5 Notification of Data Breach

Data Controllers must notify the NDPC within 72 hours of becoming aware of a breach of personal data which is likely to negatively impact the privacy rights of individuals. The nature of the breach, category and number of subjects and the data record affected should also be reported. Data Subjects should also be notified of such breach where it will affect their rights and freedom.

3.1.6 Annual Compliance Report

In accordance with the NDPA 2023 and its implementing legislation (General Application and Implementation Directive (GAID)), data controllers and processors are required to complete and file an annual Data Protection Compliance Audit Returns (CAR) with the NDPC. A data controller or a data processor of major importance established before the 12th day of June, 2023, shall file its CAR no later than 31st of March each year. The filing process is facilitated by approved Data Protection Compliance Organisations (DPCOs). These organisations are registered on a list maintained by the Commission and work on behalf of their clients to support them in their compliance process. This report embodies the principle of accountability, which is a fundamental principle of law that guarantees effective compliance by both the public and

private sectors involved in data processing.

3.1.7 Penalties for Non-Compliance

The NDPA provides criminalised penalties for non-compliance. Thus where the data controller or processor refuses to Remedy the breach; Pay compensation to the data subject who has suffered harm, loss or damage as a result of the breach; Account for any profits made as a result of the breach; or Pay a penalty or repair costs, such controller or processor shall be liable to penalties divided into two categories: financial and procedural or reputational. For DCPMI, the penalty is the sum of ₦10,000,000 or 2 percent of its annual gross revenue for the preceding year, whichever is greater. For Data Controllers and Processors that are not DCPMI, the penalty is the sum of ₦2,000,000 or 2 percent of its annual gross revenue for the preceding year, whichever is greater. Furthermore, violations may result in imprisonment for up to one year. Upon conviction, both fines and imprisonment can be administered either alternatively or together.

3.1.8 Vicarious Liability

Data controllers and processors of organisations can be held vicariously liable where its principal officers, agents and employees are convicted in contravention of the Act. provided that the non-compliance is in relation to the business. Notwithstanding, where the organisation can show proof that the non-compliance by its officers was committed without its knowledge, or that there was no connivance or consent and that due diligence was exercised to prevent the offence from being committed, then, they will not be held liable for such acts.

3.1.9 Data Subjects Private Right of Action

Individuals whose rights have been violated under the Act have the right to seek damages through civil proceedings. This provision empowers data subjects to hold data controllers and processors accountable for violations affecting their personal data.

4.0 WHAT ORGANISATIONS MUST DO

Every organisation's controller and processor must determine how best to apply and convey its strategy for organisational accountability and responsible data use in light of the relevant legal requirements, internal policies and objectives, and potential risks to individuals from the relevant processing operations. In order to successfully execute and exhibit accountability, every organisation needs to integrate it into its culture, brand, and reputation while keeping in mind how it wishes to be viewed by its clients, investors, employees and regulators.

Accountability can be demonstrated and implemented by organisations in the following manner:

4.1 Leadership and Supervision

Organisations should appoint suitable staff such as the DPO and data governance staff to supervise the organization's privacy and accountability program and report to senior management and the board. This will ensure proper governance of data privacy, oversight, accountability, reporting, and buy-in from mid-level and top-level management.

4.2 Risk Evaluation

It is important for organisations to evaluate its privacy program on a regular basis at the program level, taking into account changes in business models, legislation, technology, and other internal and external considerations. evaluates the possible threats to people's rights and liberties in the event of a data breach occurrence in order to reduce those risks and notify the DPA and the data subjects as necessary.

4.3 Policies and processes

Develop and maintain written data privacy policies and procedures that align with applicable laws, industry standards, and the organization’s values and objectives. These should be supported by systems that ensure their consistent implementation across the organization. The framework should also include clear guidelines to promote ethical considerations and ensure fair and transparent data processing practices.

4.4 Transparency

Using easily accessible channels (e.g., privacy notices, policies, and transparency tools like dashboards and portals), it informs people about its data privacy program, procedures, and protections, as well as the advantages and/or possible risks of data processing and information about individual rights.

4.5 Training

This ensures that employees, contractors, and other individuals who handle the organization's data receive regular training and information about the privacy program's goals and controls.

4.6 Observation and Confirmation

This creates protocols for routine self-evaluations, internal audits, and occasionally external

audits or certifications. It also keeps an eye on continuous internal compliance with the program, rules, and procedures.

4.7 Response and Enforcement

This establishes suitable protocols for handling questions, grievances, breaches of data security, and internal non-compliance. prevents internal violations of the program, regulations, and controls. collaborates on investigations and enforcement activities with Accountability Agents, third-party certification organisations, and data privacy regulators.

5.0 CHALLENGES TO EFFECTIVE DATA PROTECTION IN NIGERIA

One may argue that Nigeria has a strong system in place for protecting data. But some problems with data privacy still exist. Few of them are:

5.1 Other Legal Interference with Private Data

Nigeria has a data protection policy in place in addition to a number of laws that give some organizations—particularly the government—the legal authority to access or interfere with personal data. For example, the Nigerian Communications Act 2003 gives the Nigeria Communication Commission (NCC) the authority to permit authorised communication interception in times of public emergency or for the sake of public safety. Furthermore, the Nigerian Cybercrimes Act 2015 gives a judge the authority to order a service provider or law enforcement agent to collect, record, permit, or assist competent authorities with the collection or recording of content data and/or traffic data associated with specific communications transmitted by means of a computer system. The effectiveness of the current data protection rules is diminished by these rights of interference, which are typically quite broad and give no body any supervisory authority. This is due to the fact that rules that permit interception frequently do not apply the applicable data protection regulations.

5.2 Technological Advancement

The speed at which technology is developing presents a global data protection concern. On one hand, it is easier now than ever for data to be aggregated and kept, often without data subjects' permission. However, as criminal elements frequently come up with creative ways to circumvent government-instituted enforcement measures, the regulatory tools that oversee the topic and the industry find it difficult to stay up.

5.3 Absence of Judicial Precedents and Expertise

Judicial authorities regarding data privacy and protection are scarce. Furthermore, given that data protection is a somewhat specialised field, the judiciary may not possess sufficient knowledge in this area, which presents a hurdle.

5.4 Lack of Public Awareness

Ignorance is a major obstacle to the enforcement of Nigeria's data privacy regulations. Many of the individuals for whom the laws are intended are unaware of the definition of data privacy infringement. Even people who are aware of when their rights are being infringed upon may downplay the dangers that such violations can pose. Furthermore, many data subjects are not aware of the options available to them in the event that their data privacy rights are violated.
Furthermore, despite its lofty objectives, the implementation of the NDPA faces significant challenges that undermine its effectiveness.

5.5 Institutional Inefficiencies

One of the foremost issues is the inefficiency of institutional structures responsible for enforcement. The NDPC, though entrusted with a critical role, struggles with systemic weaknesses ranging from delayed response mechanisms to limited technical capacity. These deficiencies compromise the Commission's ability to ensure compliance with the law and protect data subjects adequately. High-profile breaches, such as those involving government databases, illustrate these shortcomings and expose the Commission's inability to act swiftly in preventing or mitigating such incidents.

5.6 Corruption

Corruption exacerbates these inefficiencies, creating an environment where cybersecurity policies are either poorly implemented or entirely ignored. In a system characterized by a lack of accountability, officials often divert resources allocated for data protection initiatives, leaving critical vulnerabilities unaddressed. This culture of impunity fosters insider threats and systemic lapses that compromise sensitive personal data. The implications of such breaches extend beyond individual rights violations, potentially jeopardizing national security and undermining public trust in governance.

5.7 Funding of NDPC

Resource constraints within the NDPC and related institutions further hinder the effective

implementation of the NDPA. Insufficient funding and poor resource allocation have left the regulatory framework ill-equipped to meet its objectives. The absence of robust technological infrastructure and skilled personnel results in a reactive approach to data breaches, rather than the proactive stance envisaged by the legislation. This limitation undermines the potential of the NDPA to create a resilient data protection regime capable of addressing the complexities of the digital age.

6.0 CONCLUSION AND RECOMMENDATIONS

Nigeria is steadily advancing toward mitigating the menace of data breaches. With the proliferation of big data, the risk of such breaches has grown exponentially, as seen in many countries within the Global North. Protecting the sacredness of personal information is critical, not only to combat internet fraud, financial crimes, identity theft, and national security threats, but also to foster trust in Nigeria's burgeoning digital economy. Addressing data breaches is, therefore, a matter of utmost urgency that transcends government efforts. It requires the concerted involvement of all stakeholders, including government agencies, private corporations, international partners, civil society organizations, the judiciary, academia, and individual citizens.

The Nigeria Data Protection Act (NDPA) 2023 marks a major legislative milestone in this regard. It establishes a comprehensive legal framework for privacy and data protection, with well-defined obligations for data controllers and processors. From the requirement for Data Protection Impact Assessments (DPIAs) and the appointment of Data Protection Officers (DPOs), to mandatory breach notifications and annual compliance audits, the Act outlines a rigorous accountability framework. The establishment of the Nigeria Data Protection Commission (NDPC) further cements Nigeria's institutional commitment to safeguarding personal data.

However, as robust as this legal architecture appears on paper, gaps between legislative intent and practical implementation remain glaring. Challenges such as institutional inefficiency, corruption, low public awareness, technological limitations, and inadequate funding continue to plague enforcement efforts. The disconnect between the NDPA's lofty provisions and the operational capacity of enforcement institutions calls for urgent reform.

To bridge this gap, the NDPC must be equipped with sufficient financial, human, and technological resources. Swift and efficient responses to data breaches, proactive audits, and

targeted oversight of high-risk sectors are critical. Combating corruption within regulatory and enforcement agencies is equally essential. Mismanagement of data protection funds and internal sabotage must attract strict penalties to restore public trust.

Public awareness must also be prioritized. Citizens need to understand their rights and the remedies available when these rights are violated. Education campaigns, school programs, and collaboration with youth and civil society groups can help foster a privacy-conscious culture.

Corporations, especially those categorized as Data Controllers and Processors of Major Importance (DCPMIs), must take their responsibilities seriously by encrypting and auditing data systems, training personnel, and reporting breaches within stipulated timelines. Compliance should not only be legal but also ethical—reflecting an organizational culture of accountability.

Finally, collaboration with international partners is indispensable. Global technology firms and digital rights organizations can support Nigeria through technical assistance, policy exchange, and funding for cybersecurity infrastructure.

Conclusively, addressing data breaches in Nigeria demands a multi-stakeholder approach built on strong legislation, institutional efficiency, ethical corporate behavior, public awareness, and international cooperation. The NDPA 2023 has laid a promising foundation, but for Nigeria to emerge as a regional leader in data governance, the commitment to bridge legislative ambition with operational capacity must be unwavering. By doing so, Nigeria can protect its citizens, bolster its digital economy, and set a compelling precedent for the Global South.

7.0 REFERENCES

Statutes

1. Constitution of the Federal Republic of Nigeria 1999 (as amended)
2. Cybercrimes (Prohibition, Prevention, Etc.) Act 2015
3. Nigerian Communications Act 2003
4. Nigerian Data Protection Act 2023

Regulations

5. Nigerian Data Protection Regulation 2019

Guidelines

6. NDPC General Application and Implementation Directive (GAID) 2025
7. NDPC Guidance Notice on Registration of DCPMI 2024

Case Laws

8. Eneye v MTN Nigeria Communication Ltd [CA/A/689/2013 (Unreported)]

Articles

9. Centre for Information Policy Leadership. (2018): The Central Role of Organisational Accountability in Data Protection–The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society. Available Online @ https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

10. Communications. (2024) Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira. Paradigm Initiative. Available Online @ https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/

11. Communications. (2024): Press Release: Paradigm Initiative Files a Public-Interest Case to Challenge Recent Data Breach that Saw Personal Data Sold for N100. Paradigm Initiative. Available Online @ https://paradigmhq.org/press-release-paradigm-initiative-files-a-public-interest-case-to-challenge-recent-data-breach-that-saw-personal-data-sold-for-n100/
12. Editorial. (2023): Nigeria Data Protection Act 2023: Spotlight On Notable Provisions. Olaniwun Ajayi. Available Online @ https://www.olaniwunajayi.net/blog/wp-content/uploads/2023/07/Newsletter-Nigeria-Data-Protection-Act-2023.pdf
13. Editorial. (2023): Nigerian Healthcare Agency Exposed Thousands of Applicants Personal Data. Website Planet Available Online @ https://www.websiteplanet.com/blog/plaschema-breach-report/
14. Effoduh, J. O. and Odeh, O. F. (2024): Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens. Policy Brief, Accountability Lab Nigeria. Pp. 13-14.

15. Oloruntade, G. (2023): Nigeria is Witnessing a Disturbing Surge in Data Breaches. TechCabal. Available Online @ https://techcabal.com/2023/05/23/nigeria-is-witnessing-a-disturbing-surge-in-data-breaches/
16. Oturu, D. (2019): An Overview of Big Data and Data Protection in Nigeria. AELEX. Available Online @ https://www.aelex.com/wp-content/uploads/2019/05/An-overview-of-Big-Data-and-data-protection-in-Nigeria-1-compressed.pdf
17. Sani, A. I. (2024): Nigeria Must Tackle Corruption to Improve Its Cyber Security. The London School of Economics and Political Science. Available Online @ https://blogs.lse.ac.uk/africaatlse/2024/10/09/nigeria-must-tackle-corruption-to-improve-its-cyber-security/#:~:text=Weak%20accountability&text=In%20June%202024%2C%20Nigerian%20citizens,held%20responsible%20for%20the%20breach