
NDPC's 2025 CRACKDOWN: THE HIDDEN COSTS OF DATA PROTECTION NON-COMPLIANCE

Data Protection Insight

The background image shows a person's hands typing on a laptop keyboard. Overlaid on the screen is a large, semi-transparent red warning triangle with a white exclamation mark inside. Surrounding the triangle are several red padlock icons, some of which are open. The overall theme is data security and the consequences of non-compliance.

November 2025



P a g e s	C O N T E N T
2	Introduction
2	Legal Framework for Compliance and Enforcement
3	The 2025 NDPC List of Entities Under Investigation
4	Legal Implications of Being Listed
6	Business Implications
7	Reputational Implications
8	Other key NDPC Enforcement Cases
9	Compliance / Risk Mitigation Strategies
10	Conclusion

1. Introduction

On Monday, August 25, 2025, the Nigeria Data Protection Commission (NDPC) published in BusinessDay Newspaper, a list of entities (“the 2025 List”) under investigation across various sectors for non-compliance with mandatory obligations under the Nigeria Data Protection Act (NDP Act) 2023, including the registration of data controllers and processors of major importance, the appointment of Data Protection Officers (DPOs), and filing of Data Protection Compliance Audit (CAR) reports. This action marks a watershed moment in Nigeria's data protection enforcement landscape, demonstrating that the NDPC is now employing a dual strategy of administrative sanctions (fines, investigations, compliance directives) and public enforcement tools (naming and shaming) to ensure compliance with data protection laws by relevant entities. Against this backdrop, this article examines the NDPC's enforcement architecture, the legal implications of being listed, and the related business and reputational risks. It also reviews precedent cases, such as the NDPC fine on Fidelity Bank and the investigation and fine imposed on Meta by the FCCPC and NDPC and offers practical compliance strategies for Nigerian entities.

2. Legal Framework for Compliance and Enforcement

The Nigeria Data Protection Act 2023 (NDP Act) codified Nigeria's commitment to international data-protection standards by establishing the Nigeria Data Protection Commission (NDPC) with enforcement powers that include investigation, issuance of compliance directives, and imposition of administrative sanctions². On March 20, 2025, the NDP Act General Application and Implementation Directive (GAID) 2025³ was issued by NDPC to provide implementation directives for the NDP Act, providing clarity and context to its provisions. While the early years of Nigerian data-protection enforcement were dominated by regulations, especially under the now-defunct Nigerian Data Protection Regulations (2019), the NDPC's 2025 public listing marks a new era, where compliance obligations now carry visible and multi-dimensional consequences.

¹ Nigeria Data Protection Act 2023, Section 4

² Nigeria Data Protection Act 2023, Section 6

³ The 2025 NDP Act General Application and Implementation Directive (GAID) was issued by NDPC on March 20, 2025. The GAID seeks to enhance the understanding, implementation and effectiveness of the NDP ACT and is divided into 52 Articles and 10 Schedules.

For the NDPC's enforcement actions and the 2025 publication of entities under investigation to be fully appreciated, it is essential to first understand the categories of organisations that fall within the scope of the Nigeria Data Protection Act (NDP Act) 2023 and the nature of compliance obligations imposed on them.

The NDP Act applies broadly to all natural and legal persons who process personal data in Nigeria, as well as those outside Nigeria that process the data of Nigerian residents⁴. Within this broad framework, the Act distinguishes between Data Controllers and Data Processors. Data Controllers are those who determine the purposes and means of processing personal data, while Data Processors act on behalf of Controllers⁵. Both categories have respective obligations under the Act.

3. The 2025 NDPC List of Entities Under Investigation

Under the Act, the NDPC is empowered to investigate complaints or suspected violations, issue compliance orders and corrective measures, impose fines linked to annual gross revenue (Section 53 NDP ACT), publicly name entities under investigation or in breach, among other powers.

The 2025 List was made pursuant to Section 6(e)-(f) of the NDP Act, 2023 and the investigation is done pursuant to the powers conferred on the Commission under the NDP Act⁶. Each of the organisations listed in the 2025 List were required to provide the following:

- i. Evidence of filing NDP Act Compliance Audit Returns for-2024. S. 6(d) of the NDP Act.
- ii. Evidence of Designation or Appointment of a Data Protection Officer (including name and contact details) - S.32 of NDP Act
- iii. Summary of Technical and Organisational measures for data protection within the organisation - S.39 of NDP Act.
- iv. Evidence of Registration as a Data Controller or Processor of Major Importance - S. 44 of NDP Act.

⁴ Nigeria Data Protection Act 2023, Section 2

⁵ *Ibid.*, Section 65

⁶ The Nigeria Data Protection Act, 2023, S.5(i), 6(a), 6(c), 46(3) and 47(1) & (2) (a-b)

NDPC's notice further stated that the above-mentioned information is to be provided within twenty-one (21) days of the issuance of the Notice and warned that failure to comply with the Compliance Notice may result in the issuance of an Enforcement Order, imposition of administrative fines, and/or criminal prosecution in accordance with the NDP Act, 2023.

This publication did not merely catalogue regulatory gaps; it placed organisations in the public domain as potential violators of Nigeria's data-protection laws. For the first time, legal non-compliance directly translated into reputational exposure.

4. Legal Implications of Being Listed

The publication of the 2025 List by the NDPC raises profound legal consequences for the organisations named. Although the Commission carefully frames the list as entities “under investigation” rather than confirmed defaulters, the legal weight of such publication cannot be understated. Inclusion on the list as an entity being investigated under the NDP Act 2023 places an organisation within the formal regulatory spotlight and activates a chain of potential liabilities that extend far beyond administrative compliance.

The first and most immediate implication is the presumption of breach and regulatory escalation. While the presumption is not, strictly speaking, one of legal guilt, the very fact of being listed suggests a *prima facie* failure to comply with mandatory obligations such as the filing of Data Protection Compliance Audit (DPCA) reports, registration as a controller or processor of major importance, or the appointment of a Data Protection Officer. Once an organisation is under investigation, the NDPC possesses statutory powers under Sections 46 to 53 of the NDP Act⁷ to enforce, conduct inquiries, demand remedial action, and, if non-compliance persists, escalate to administrative sanctions. These sanctions can include hefty fines calculated as a percentage of annual gross revenue, temporary suspension of data processing operations, or binding compliance directives.

7 The NDP Act, Sections 46 - 53

Beyond regulatory enforcement, there is the risk of civil liability. Section 37 of the 1999 Constitution guarantees the right to privacy⁸, while Sections 34 – 38 of the NDP Act codify data subjects' rights to access, rectification, erasure, objection, and portability⁹. Being publicly flagged as non-compliant can serve as a catalyst for litigation, as affected individuals may seek redress for infringements of their privacy rights. Nigerian courts, in cases such as *Araka Akosa v. ECART Internet Services Nigeria Ltd & Anor.*¹⁰ and *Tokunbo Olatokun v. Polaris Bank*¹¹, have demonstrated increasing willingness to enforce both statutory and constitutional privacy protection provisions. Thus, the NDPC's listing operates as a signal to potential litigants, lowering the evidential threshold for claims of negligence or unlawful processing.

A further layer of legal implication arises from cross-regulatory scrutiny. In Nigeria's complex regulatory ecosystem, the NDPC does not operate in isolation. Sector-specific regulators such as the Central Bank of Nigeria (CBN), the Nigerian Communications Commission (NCC), and the Federal Competition and Consumer Protection Commission (FCCPC) often exercise concurrent jurisdiction over data-related matters. Once the NDPC identifies an organisation under investigation, it is not uncommon for other regulators to initiate parallel inquiries, thereby multiplying legal exposure. The recent example of Meta¹², where the FCCPC imposed Two Hundred and Twenty Million Naira (N220,000,000.00) fine for privacy and consumer-protection breaches with NDPC's involvement, illustrates how inter-agency collaboration can result in compounded penalties and judicially sustained sanctions.

Finally, the legal implications extend into the domain of commercial law and contractual obligations. Many commercial contracts, particularly in banking, fintech, and multinational supply chains, contain compliance warranties and indemnity clauses tied to data-protection obligations. Public listing by the NDPC may be deemed a likely breach of such warranties, triggering contractual remedies that range from indemnification claims to outright termination of agreements. This

8 Constitution of the Federal Republic of Nigeria, (1999 As amended) Section 37

9 The NDP Act, Sections 34 - 38

10 *Araka v E-Cart Services Ltd. & Anor.* Unreported: Suit No. FHC/ABJ/CS/195/202461

11 *Tokunbo Olatokun v Polaris Bank Limited* Unreported: Suit No. LD/17392MFHR/2024 61,

12 Federal Competition and Consumer Protection Commission ("FCCPC"), Violations: Tribunal Upholds FCCPC's \$220 Million Fine Against Meta/WhatsApp, Available at <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> Accessed September 1, 2025

contractual liability, though private in nature, is often more immediately disruptive than regulatory fines, as it directly affects business continuity and financial stability.

In a nutshell, the legal implications of being listed by the NDPC are both direct and collateral. Directly, it exposes an organisation to investigations, fines, and corrective directives under the NDP Act. Collaterally, it invites civil claims from data subjects, scrutiny from sectoral regulators, and contractual liabilities from counterparties. While the NDPC's publication does not amount to a judicial finding of guilt, it functions as a powerful legal signal that can trigger a cascade of consequences. For organisations, therefore, the act of being listed is not a mere reputational embarrassment but a substantive legal risk that must be managed with urgency, transparency, and compliance-oriented reforms.

5. Business Implications

The inclusion of an organisation on the 2025 List has far-reaching business consequences that extend well beyond regulatory scrutiny. At its core, the listing undermines market confidence. In sectors where consumer trust is paramount, such as finance, health, and telecommunications and others, the perception of weak data governance can deter both existing and prospective clients.¹³ A bank, for instance, that is publicly associated with non-compliance may struggle to convince customers that their sensitive financial information is secure, thereby eroding its competitive standing.

The consequences are equally acute in investment and financing. Data protection compliance is increasingly embedded within environmental, social, and governance (ESG) benchmarks¹⁴. Investors and lenders view non-compliance as a proxy for weak corporate governance and heightened legal risk¹⁵. Being named by the NDPC can therefore translate into delayed funding rounds, renegotiated credit terms, or outright withdrawal of investor interest.

13 Databricks, What Is Data Governance? A Comprehensive Guide, available at <https://www.databricks.com/discover/data-governance#:~:text=Data%20governance%20mitigates%20security%20and,trust%20and%20transparency%20with%20stakeholders>. Accessed September 1, 2025

14 Paolo Balboni, Kate Elizabeth Francis, 'Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future', *Journal of Responsible Technology*, Volume 22, 2025, Available at <https://doi.org/10.1016/j.jrt.2024.100099> Accessed September 1, 2025

15 Ibid

Beyond capital markets, the effect is also felt in commercial relationships: procurement contracts, especially with government agencies and multinationals, now demand demonstrable compliance with data-protection obligations. For organisations under investigation, the NDPC's listing may operate as a red flag that may trigger termination clauses, contract suspensions, or disqualification from future bids. In this sense, the financial cost of reputational and operational disruption may outweigh even the largest administrative fines.

6. Reputational Implications

The reputational damage associated with the 2025 List is both immediate and enduring. The Commission, by naming organisations in a national newspaper, ensures that allegations of non-compliance are publicly visible and easily amplified across prints, digital and social media platforms. For many stakeholders, the nuance that an organisation is merely “under investigation” rather than conclusively guilty is quickly lost. The reputational stain attaches instantly and reversing that perception is an uphill task.

Reputation, once compromised, exposes organisations to lasting disadvantages.¹⁶ Research has shown that up to a third of customers in retail, finance and healthcare will stop doing business with organisations that have been breached data before.¹⁷ Additionally, 85% will tell others about their experience, and 33.5% will take to social media to vent their anger.¹⁸ Competitors can capitalise on the situation by projecting themselves as compliant and trustworthy, subtly contrasting their practices with those of listed entities. This comparative disadvantage gradually weakens brand equity, pushing customers and clients to migrate towards organisations that embody transparency and accountability.

Furthermore, reputational damage is notoriously persistent because even after an organisation has remediated its compliance gaps and been delisted, the historical fact of investigation remains in the public domain,

16 L. Noonan, '5 damaging consequences of a data breach: Protect your assets. MetaCompliance, (2020, February 25). Available at <https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-databreach#:~:text=The%20reputational%20damage%20resulting%20from,accounts%20or%20making%20unauthorised%20purchases> Accessed September 1, 2025

17 Ibid

18 Ibid

searchable online and embedded in corporate memory. Such lingering reputational scars not only erode consumer loyalty but also complicate efforts at corporate rebranding, strategic partnerships, and international expansion.

7. Other key NDPC Enforcement Cases

7.1. *NDPC's Fine on Fidelity Bank*

In 2024, the NDPC imposed a Five Hundred and Fifty-Five Million, Eight Hundred Thousand Naira (N555,800,000.00) fine on Fidelity Bank¹⁹ on the grounds that the bank processed personal data without proper lawful basis and used non-compliant third-party tools. The NDPC's assessment highlighted the bank's failure to cooperate effectively and its inability to present a satisfactory remediation plan, which exacerbated the penalty. The fine, one of the largest to date, shows how revenue-linked sanctions and prolonged non-cooperation can produce substantial financial exposure.

7.2. *FCCPC & NDPC fine Meta Platforms*

The FCCPC issued a Two Hundred and Twenty Million United States Dollars (US\$220,000,000.00) order against Meta Platforms relating to WhatsApp's data-sharing policy, concluding that the company's integrated data practices deprived users of meaningful control and disadvantaged Nigerian users compared to those in stricter jurisdictions.²⁰ The enforcement action was taken in conjunction with NDPC. The case was appealed, and the tribunal upheld the fine. However, the process itself highlighted the efficacy of coordinated enforcement and the potential for very large penalties when systemic platform practices affect broad user populations.

19 Channels Television, 'Fidelity Bank fined N555.8m by NDPC for data breach' (2024, August 21). Available at <https://www.channelstv.com/2024/08/21/fidelity-bank-fined-n555-8m-by-ndpc-for-data-breach/> Accessed on September 2, 2025,

20 Federal Competition and Consumer Protection Commission ("FCCPC"), Violations: Tribunal Upholds FCCPC's \$220 Million Fine Against Meta/WhatsApp, Available at <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> Accessed September 1, 2025

8. Compliance / Risk Mitigation Strategies

To mitigate regulatory, legal, business, and reputational risks under the *Nigeria Data Protection Act (NDP ACT) 2023* and in line with the NDPC's 2025 List, organisations should implement a proactive, multi-layered compliance framework. Key strategies include:

- i. *Data Protection Compliance Audit:* Conducting a rapid compliance gap assessment to identify outstanding obligations such as Data Protection Compliance Audit (DPCA) filings, registration of controllers/processors of major importance, and appointment of Data Protection Officers (DPOs) and prioritising remediation of “high-risk” gaps, those that directly trigger NDPC investigations or fines.
- ii. *Proactively engaging with the NDPC once deficiencies are identified:* Cooperative posture often leads to reduced penalties or leniency. Entities should notify the Commission of remedial steps taken, and maintain records of correspondence to demonstrate good faith compliance.
- iii. *Appointing qualified Data Protection Officers:* As required under Section 32 NDP Act, entities should establish an internal data-protection team with representation from legal, IT, compliance, and business units. It is also essential for entities to integrate data protection into their board-level governance and ESG reporting.
- iv. *Updating Contracts and Vendor Management systems:* There is a need to review and update Data Processing Agreements (DPAs) with vendors and partners to ensure compliance with NDP Act standards. Audit and indemnity clauses should be included to manage third-party risks, particularly when sensitive customer data is processed externally.
- v. *Embedding Data Subject Rights Protocols:* Entities should develop streamlined internal processes for handling rights requests (access, rectification, erasure, objection, portability) and ensure opt-out

21 *Araka v E-Cart Services Ltd. & Anor.* Unreported: Suit No. FHC/ABJ/CS/195/202461

22 *Tokunbo Olatokun v Polaris Bank Limited* Unreported: Suit No. LD/17392MFHR/2024 61.

mechanisms for direct marketing are functional and effective, as demonstrated by litigation outcomes in *Akosa v. ECART* and *Tokunbo Olatokun v. Polaris Bank*.

- vi. *Independent Audits and Assurance:* Entities should commission annual external audits by Data Protection Compliance Organizations in accordance with Section 33 of the NDP Act to validate compliance. There is also a need to publish compliance statements for instance the NDPC Audit Complaint Badge (where appropriate) to reassure customers, partners, and investors of transparency.
 - vii. *Incident Response and Crisis Management:* Entities should develop and test a data-breach response plan in accordance with Section 40 of the NDP Act, establish clear communication protocols for informing regulators, customers, and stakeholders in case of breaches and prepare crisis communication strategies to mitigate reputational fallout from public investigations.
 - viii. *Capacity Building and Awareness:* In accordance with Article 46 of the NDP Act GAID, entities should regularly train employees on data protection principles and sector-specific compliance risks, and integrate data protection awareness into onboarding processes and performance assessments.
-

9. Conclusion

The NDPC's 2025 List of Entities Under Investigation underscores that compliance with data protection obligations under the NDP Act 2023 is not optional, particularly for Controllers and Processors of Major Importance such as banks, telecommunications companies, health institutions, and other entities that process sensitive or large-scale data. While the scope and depth of compliance requirements may differ across sectors and organisational sizes, the implications of non-compliance remain undesirable. For organisations named by the NDPC, the consequences manifest legally in the form of sanctions and potential litigation, commercially through the loss of contracts, investors, and customers, and reputationally through diminished trust and heightened public scrutiny. This reality makes it imperative for Nigerian organisations to treat data protection not as a mere box-ticking exercise but as a strategic component of governance and risk management. Organisations can not only avoid regulatory sanctions but also build resilience and credibility in Nigeria's growing data-driven economy by embedding proactivity, transparency, and accountability into their compliance programmes.

AUTHORS



Chidera Ezenwanne
Data Protection Practice Unit



Michael Arinze
Data Protection Practice Unit



Contact

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way, Oniru
PO Box 73002, Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285, Abuja

ENUGU

3 Emmanuel Ngwu Street,
Thinkers' Corner,
Enugu, 400001

+234 811 395 1052, +234 811 395 1053
counsel@kennalp.com

