


# WRITTEN POLICY, BROKEN PRACTICE: THE DATA PROTECTION GAP

SYNTEGRAL LEGAL PRACTICE

April 2026




Oladiran Falore
*Managing Partner*



Salama Jidda
*Associate Counsel*


Nigeria's digital economy is expanding at a remarkable pace. By February 2025, there were over 430 fintech companies operating in the country, and the Nigeria Inter-Bank Settlement System Plc(NIBSS) processed ₦600 trillion in electronic payments, reflecting a 55% year-on-year increase. As digital activity rises, so does exposure to data risks, bringing with it, legal responsibilities that organisations can no longer ignore or downplay.

The introduction of the Nigeria Data Protection Act 2023 marks a major shift in the country's data governance landscape, building on the earlier Nigeria Data Protection Regulation of 2019. The Act establishes a comprehensive statutory framework, backed by an independent Commission with powers to investigate, impose fines, and enforce compliance. It also reinforces data subject rights anchored in Sections 37 and 45 of the 1999 Constitution of the Federal Republic of Nigeria. Enforcement has become more tangible, with significant penalties already issued, including a ₦766.2 million fine against Multichoice Nigeria and a US$220 million action against Meta Platforms. Despite this, many organisations, across both private and public sectors, still struggle to translate policy into practice.

Yet the familiar paradox of data protection compliance persists in Nigeria as it does globally: most organisations that fail to protect personal data do not lack policies. They lack implementation. Policies are drafted for auditors. Privacy notices populate websites without being read or operationalised. Data Protection Officers are appointed by title without authority or resources. Annual compliance filings are submitted to the NDPC while operational data handling practices remain unchanged. This article explores why this gap persists in Nigeria and what organisations need to do to address it effectively.

## UNDERSTANDING NIGERIA'S OBLIGATIONS

Nigeria's data protection landscape underwent a fundamental shift with the enactment of the Nigeria Data Protection Act 2023("Act"), which replaced the Nigeria Data Protection Regulation 2019 ("NDPR") as the country's principal data protection statute. The NDPR's most glaring weakness was its lack of a dedicated enforcement authority. It had relied on National Information Technology Development Agency (NITDA), primarily a technology development agency, to police compliance. The Act corrected this by establishing the Nigeria Data Protection Commission (NDPC) as an independent regulatory body equipped with broad investigative powers, authority to impose administrative fines, issue corrective orders, suspend processing activities, and approve mechanisms for cross-border data transfers.

Complementing the Act is the General Application and Implementation Directive (GAID), issued by the NDPC on 20 March 2025 and effective from 19 September 2025. From that date, the NDPR 2019 and its 2020 Implementation Framework ceased to have effect as operative instruments, with regulatory position not defined by the Act read alongside the GAID. For organisations that built their compliance programmes around the NDPR, this marks a material shift, requiring a reassessment of existing frameworks, while also providing an opportunity to strengthen them on a clearer statutory footing.

Under the Act, personal data may only be processed on one of six lawful bases: consent, contract, legal obligation, vital interests, public interest, or legitimate interests. Organisations that process the personal data of more than 200 data subjects within six months, operate in strategically significant sectors, or provide commercial technology services are required to register with the NDPC as Data Controllers or Processors of Major Importance (DCPMIs). Such entities are subject to enhanced obligations including the mandatory appointment of a Data Protection Officer.

In addition to registration, the Act introduces a range of operational compliance requirements. Data controllers must notify the NDPC of any breach likely to pose a high risk to individuals' rights and freedoms within 72 hours of becoming aware of it, aligning with international standards and reinforced by the 2024 amendment to the Cybercrimes Act. High-risk processing activities, including the handling of sensitive personal data or children's data, require the conduct of Data Protection Impact Assessments (DPIAs). DCPMIs are also required to file annual Compliance Audit Returns (CARs) with the NDPC by 31 March each year, cross-border transfer of personel are permitted only where the receiving jurisdiction ensures a level of protection consistent with the standards prescribed in the Act.

The consequences of non-compliance are substantial. The Act introduces a tiered penalty regime under which DCPMIs face fines of up to ₦10 million or 2% of annual gross, while other organisations face fines of up to ₦2 million or 2% of annual gross revenue. Non-compliance with NDPC orders may further result in imprisonment of up to one year. These sanctions signal a decisive shift from the relatively toothless enforcement environment that characterised the NDPR era.

Compliance is further complicated by Nigeria's multi-regulator structure, in which sector-specific authorities retain concurrent jurisdiction alongside the NDPC. The Central Bank of Nigeria governs data handling in financial institutions and fintechs; the Nigerian Communications Commission oversees telecoms; and the National Health Insurance Authority applies sector rules in healthcare. For organisations operating across sectors, managing these overlapping and sometimes inconsistent obligations simultaneously presents a serious practical challenge. This tension is most acute for fintech companies, which must navigate CBN requirements on Customer Due Diligence, KYC, payment integration, and Anti-Money Laundering, each generating significant data activity that is simultaneously subject to statutory principles on consent, purpose limitation, and data minimisation.

**THE IMPLEMENTATION GAP IN NIGERIA: STRUCTURAL CAUSES**

Filing a Compliance Audit Return or registering as a DCPMI creates an administrative record of engagement with the regulatory framework, but it does not indicate that personal data is being handled with the care the Act demands. The NDPC's phased, capacity-building-oriented approach to enforcement has inadvertently created space for organisations to treat early-stage compliance activities as the destination rather than the starting point of a longer journey.

A foundational challenge underlying these gaps is low awareness of data protection rights and obligations across all levels of Nigerian society. A study found that widespread ignorance of the Act's provisions continues to undermine the framework's effectiveness as many citizens remain unaware of their data. Within organisations, the awareness gap is sharpest among small and medium-sized enterprises, where limited knowledge compounds the challenge of limited resources. The costs associated with compliance audits, Data Protection Officer services, and security implementation can feel prohibitive to businesses already contending with macroeconomic pressures including high inflation and a volatile exchange rate environment.

A structural problem that cuts across organisations of all sizes is the isolation of data protection responsibility. Where data protection is treated as the exclusive domain of a legal or IT department, the reality that it intersects with procurement, human resources, marketing, product development, and customer service goes unaddressed. Vendor agreements, employee data handling, consent mechanisms, privacy-by-design decisions, and the management of data subject requests all require coordinated governance. Where functions do not communicate, policy documents remain precisely that: documents, disconnected from the daily realities of how personal data flows through the organisation.

This disconnect is most visible in the fintech sector, where the pace of product development frequently outstrips compliance integration. Product teams build interfaces that collect extensive personal data to support onboarding and credit scoring. Legal teams draft privacy notices. Security teams manage technical controls. Yet without a governance structure that aligns all three functions around a shared understanding of what the Act requires at each stage of the data lifecycle, compliance remains notional, a set of parallel activities rather than an integrated practice.

The implementation environment has been further complicated by active legal uncertainty. In *Frank Ijege v. NDPC*, the Kaduna Division of the Federal High Court ruled that several provisions of the NDPC's notice on DCPMIs exceeded the mission's statutory authority under the Act. This ruling created legitimate uncertainty for organisations attempting to determine whether they were subject to enhanced obligations, and illustrated a broader structural challenge: a regulatory framework in active legal development cannot be navigated confidently through static policy documents alone. Organisations require governance structures capable of tracking and responding to regulatory evolution in near real-time, treating compliance not as a fixed state to be achieved but as a dynamic process to be continuously managed.

**COMMON COMPLIANCE GAPS**

A foundational operational failure across many Nigerian organisations is the absence of accurate, current inventories of the personal data they hold, where it is stored, and who can access it. Without this baseline knowledge, meaningful compliance with the Act's principles of data minimisation, purpose limitation, and storage limitation is practically impossible. Data Protection Impact Assessments cannot be conducted without clarity on what data is being processed, and subject access requests cannot be fulfilled without knowing where that data resides. This is not merely a technical shortcoming, it reflects a deeper organisational culture in which data has historically been treated as an operational asset rather than a regulated resource carrying legal obligations to identifiable individuals. The GAID's requirement for periodic compliance audits provides a useful prompt, but an audit mechanism alone cannot resolve the underlying problem of organisations that do not continuously manage their data holdings.

Nigeria's predominantly mobile digital economy creates particular complications for consent management under the Act. A significant proportion of Nigerians access financial services, health information, and e-government portals via mobile applications, often under conditions of variable connectivity and limited time. The Act requires consent to be freely given, specific, informed, and unambiguous, yet cookie banners and privacy notices that function adequately on a desktop browser may be effectively inaccessible on a feature phone or in a low-bandwidth environment. Article 19 of the GAID now mandates opt-in consent before websites and applications deploy cookies or tracking tools beyond those strictly necessary, requiring clear and visible consent interfaces without pre-ticked boxes or implied acceptance. For the substantial portion of Nigerian digital businesses whose user interfaces were never designed with granular consent management in mind, this requirement raises serious implementation questions that cannot be resolved through policy drafting alone.

The 72-hour breach notification requirement, ranks among the most operationally demanding obligations in Nigeria's data protection framework. Complying with it requires organisations to maintain a functioning breach detection system, clear internal escalation pathways, a pre-agreed protocol for assessing whether a breach crosses the notification threshold, and a reliable mechanism for communicating with the NDPC within the prescribed window. The scale of the underlying threat is significant: Nigeria has witnessed a 468% rise in digital fraud cases in recent years.

Despite this threat landscape, the gap between breach detection and formal notification remains wide across much of the Nigerian market. Many organisations have only recently adopted formal incident response plans, and the absence of regular simulation exercises means that the 72-hour window is routinely missed, not through bad faith, but through structural unpreparedness. Having a breach notification policy on paper is meaningless without the rehearsed internal capability to execute it under pressure and within tight time constraints.

Third-party and vendor risk represents another significant compliance gap. The Act places primary liability for data protection on the data controller regardless of whether processing is carried out by an external vendor, cloud service provider, or outsourced platform. Yet many Nigerian organisations use locally-hosted or offshore cloud services, outsourced customer service platforms, and data analytics providers without conducting structured due diligence or entering into Act-compliant data processing agreements. The Act's extraterritorial scope makes things more difficult: although foreign companies that serve people in Nigeria or track their activities are meant to comply with the Act, many do not, and Nigerian data controllers often fail to require this in their contracts, creating a gap between what the law says and what happens in practice.

The requirement to appoint a Data Protection Officer reflects a broader pattern where formal compliance often hides real gaps in practice. While DCPMIs are required to designate a DPO, and this applies to most major Nigerian organisations, these appointments are often only on paper, with individuals lacking the time, training, or authority to carry out the role effectively. For SMEs that cannot afford a full-time DPO, the GAID provides for the use of NDPC-licensed Data Protection Compliance Organisations, but this practical solution remains largely underused despite its potential to bridge the implementation gap.

**MOVING BEYOND PAPERWORK**

For Nigerian organisations seeking to close the data protection implementation gap, the priority is not better documentation but effective, real governance, with clear ownership at senior management level, an empowered DPO with access to decision-making, and cross-functional collaboration across legal, IT, HR, procurement, and operations. This governance framework must also be agile, capable of responding to the NDPC's evolving guidance rather than relying on static, annual policy reviews. Building on this, organisations should undertake a structured privacy gap analysis to assess their compliance with the Act and GAID, particularly where existing programmes were designed around the NDPR, and where internal expertise is limited, this process should be supported by licensed Data Protection Compliance Organisations.

Equally important is investing in employee training that goes beyond basic awareness to drive real behavioural change. In the Nigerian context, this means delivering accessible, role-specific training, grounded in practical scenarios and refreshed regularly, with particular emphasis on phishing and digital fraud risks, which remain a major source of data breaches. For fintechs, health-tech companies, and other digital platforms, embedding privacy by design into products from the outset is both a legal requirement

and a cost-effective strategy, while conducting data protection impact assessments early in the product lifecycle helps identify and mitigate risks before they become regulatory issues.

At the operational level, organisations should leverage regulatory technology tools to support compliance activities such as data mapping, consent management, breach tracking, and audit preparation, particularly where dedicated compliance resources are limited. At the same time, vendor and third-party risk management must be treated as a core compliance obligation, not a contractual formality, with proper due diligence, enforceable data processing agreements, and continuous monitoring. This is especially critical for cross-border data transfers, where the Act imposes strict requirements, and organisations must ensure that appropriate safeguards are in place, as ultimate responsibility for compliance failures within the data ecosystem rests with the data controller.

**CONCLUSION**

Nigeria's data protection landscape has advanced considerably since the introduction of the NDPR in 2019. With the Nigeria Data Protection Act 2023 and the GAID, the country now operates within a more structured and enforceable framework that aligns with global standards and strengthens its position in the international data economy. The willingness of the NDPC to impose significant penalties on both multinational and local organisations signals a clear shift from viewing compliance as a formality to treating it as a serious legal and operational obligation.

For businesses, this shift is not just a regulatory pressure point, it is a strategic opportunity. In a market where digital trust remains fragile, scrutiny is increasing, and investors and partners expect clear evidence of compliance, organisations that take data protection seriously can differentiate themselves.

However, real progress depends on more than policies and filings. It requires intentional investment in governance structures, skilled people, and the right technology, supported by a culture that integrates data protection into everyday decision-making and operations. Tools such as Compliance Audit Returns should be seen as a starting point, not the end of the process.

Ultimately, protecting personal data is not just about meeting regulatory requirements. It is central to building trust, strengthening credibility, and supporting sustainable growth in Nigeria's evolving digital economy.

© Copyright 2026 - Syntegral Legal Practice