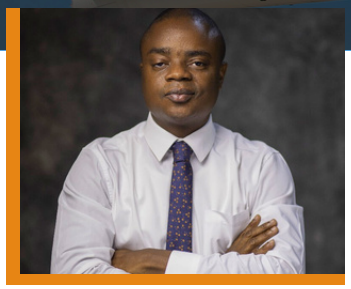
SYNTEGRAL
LEGAL PRACTICE

THE COST OF NON-COMPLIANCE: LEGAL, FINANCIAL, AND REPUTATIONAL RISKS – WHAT ORGANISATIONS STAND TO LOSE WHEN DATA PROTECTION IS TREATED LIGHTLY IN NIGERIA

March, 2026



Oladiran Falore
Managing Partner



Unwana Obioh
Associate Counsel

OVERVIEW

This article looks at the real consequences organisations face when data protection is not taken seriously. It breaks the risks down into four connected areas. First, the legal impact, showing how routine data handling can quickly lead significant liability. Second, the financial impact. Third, reputational consequences; and finally, it highlights operational and governance challenges, demonstrating how weak processes, poor oversight, and inadequate compliance structures magnify risks across legal, financial, and reputational domains. The discussion highlights how regulatory enforcement, litigation exposure, and operational failures can compound organisational vulnerability. Ultimately, this article makes a clear point: managing personal data properly is not just about meeting legal requirements. It is a fundamental responsibility that supports long-term stability and success.

1. INTRODUCTION

In Nigeria today, personal data sits at the centre of almost every organisational activity. From financial institutions tracking transactions and maintaining customer records, to telecom companies managing subscriptions and usage patterns, to e-commerce platforms storing payment details and behavioural insights, the collection, storage, and use of personal information is routine. Even internal processes such as employee onboarding, payroll administration, health records, and vendor management generate significant volumes of personal data. Each of these interactions carries a potential risk if handled without proper oversight or legal compliance.

A simple but telling example illustrates this. A mid-sized digital lending company experienced a surge in customer complaints over a short period. Borrowers began reporting that they were being contacted by individuals posing as company agents, urging them to take loans and immediately transfer the disbursed funds to "secure" their accounts. Investigations later revealed that these fraudsters had obtained fragments of customer information, including names and application statuses, which made their approach appear credible. While the initial breach point was not immediately clear, what became evident was that internal data handling controls were weak. Customer data was accessible across multiple teams without strict role-based restrictions, audit trails were limited, and third-party integrations had not been properly assessed. What started as a few isolated incidents quickly escalated. Customers lost money, trust eroded, regulators were notified, and the company was forced to suspend parts of its operations while responding to the incident. Legal exposure followed, alongside the cost of remediation, customer communication, and system overhaul. The reputational damage proved even harder to contain, as the narrative shifted from fraud by external actors to questions about the company's own data governance.

The Nigeria Data Protection Act (NDPA) 2023 provides a framework for managing such risks, setting out clear obligations for the lawful processing, storage, and sharing of personal data. Compliance is not something reserved for crisis moments; it is embedded in everyday decisions, from how data is collected and consent is obtained, to how systems are configured, access is controlled, and third parties are engaged. Where these controls are weak or overlooked, the consequences rarely remain isolated.

This article examines what organisations stand to lose when data protection is treated lightly, structured around four key dimensions. It first considers the legal risks that arise under the NDPA, including regulatory enforcement and potential civil liability. It then explores financial exposure, covering both direct penalties and the wider cost of operational disruption and remediation. The discussion moves to reputational impact, showing how quickly trust can be undermined when personal data is mishandled. Finally, it looks at the operational and governance weaknesses that often sit beneath these failures, drawing out practical lessons for organisations seeking to build more resilient and compliant data practices.

2. LEGAL RISKS: THE IMMEDIATE AND ESCALATING CONSEQUENCES

Legal risk under the NDPA is ever-present in the way organisations handle personal data, attaching consequences to both routine and exceptional processes. The law does not wait for major breaches to trigger liability; even seemingly minor lapses in consent, record-keeping, or data sharing can expose an organisation to complaints, regulatory investigation, or enforcement action. Under the NDPA, this includes potential fines, directives to cease or alter processing, restrictions on data handling, and, in some circumstances, criminal liability. Civil claims by affected data subjects may run in parallel, creating overlapping channels of legal exposure.

Everyday business processes also contribute to this risk. Onboarding forms, cookies on websites, employee records, and vendor data exchanges all create touchpoints where non-compliance can occur. For instance, unclear privacy notices or inadequate consent mechanisms may be interpreted as unlawful processing. Similarly, weak security or insufficient access controls can trigger regulatory attention even in the absence of an actual data breach. Because the NDPA obliges organisations to maintain accountability and demonstrate adherence to principles of lawful, fair, and transparent processing, minor gaps often escalate quickly once identified.

Criminal liability remains relatively rare but is still possible. Certain deliberate or reckless failures, such as unauthorised disclosure of sensitive personal data, carry criminal liability. More commonly, though, organisations confront civil and regulatory consequences, which tend to amplify as investigations probe the adequacy of underlying systems and governance. Exposure rarely remains contained; regulatory or claim scrutiny often extends beyond the incident itself, examining patterns of decision-making, contractual arrangements, and internal processes. Organisations that treat compliance lightly may find that what begins as a modest issue soon escalates into multifaceted legal challenges that affect both operations and reputation.

3. FINANCIAL RISKS: DIRECT COSTS AND HIDDEN LOSSES

Irrespective of how a data protection issue first presents itself, it rarely stops at the initial penalty. The financial implications extend well beyond any immediate fine, touching both the operational and strategic dimensions of an organisation. Direct costs are the first to emerge: regulatory fines under the NDPA can be substantial, legal fees for defending investigations add up quickly, and incident response, such as forensic analysis, remediation, and communication, requires dedicated resources. In 2023, Multichoice Nigeria was fined ₦766.24 million after regulators found deficiencies in how it obtained and managed customer consent. Similarly, Fidelity Bank was penalised ₦555.8 million for inadequate safeguards around customer data, exposing weaknesses in internal controls. These costs are often unavoidable and immediate, forming the initial layer of financial exposure.

Non-compliance carries real, immediate costs that organisations must factor into operational and financial planning. System downtime during incident response or enforcement proceedings disrupts routine business activity, leading to delays in service delivery and diversion of internal teams from core functions. For sectors like banking, fintech, and telecommunications, even brief interruptions can cascade into broader operational challenges, affecting customer transactions and internal workflows. The cumulative effect of these disruptions can surpass the initial regulatory penalty, demonstrating that financial risk is both direct and operationally embedded.

Indirect financial consequences, though less immediately visible, can be even more damaging over time. Loss of customers due to diminished trust, reduced subscriptions or engagement, and strained business partnershipfs all erode revenue streams.

Reputational effects feed back into commercial performance: clients may defer investment decisions, partners may impose stricter contractual conditions, and market confidence can waned. The impact is not uniform, but in sectors handling large volumes of personal data, the ripple effects of a single misstep can multiply quickly.
Ultimately, what weighs most heavily on the organisation is not the point-of-enforcement penalty alone but the accumulated disruption, recovery costs, and diminished commercial activity that tend to follow. Financial risk under the NDPA, therefore, is dynamic and ongoing, extending from immediate fines to long-term erosion of economic viability if not properly mitigated through proactive governance and operational resilience.

4. REPUTATIONAL RISKS: LOSS OF TRUST AND MARKET CONFIDENCE

Once a data protection failure becomes known, whether through a breach, a complaint, or regulatory action, it immediately affects how customers, partners, and the broader public perceive the organisation. Unlike legal or financial consequences, reputational harm is often less predictable but can be far more enduring. Stakeholders respond not only to the incident itself but to the organisation's apparent competence and commitment to safeguarding personal data. In practice, a single misstep can quickly reshape perceptions and influence behaviour across multiple stakeholder groups.

Customers are often the first to signal disapproval. Hesitation to engage, reduced usage of services, or outright churn can follow even minor data mishandling, particularly when privacy concerns are amplified online. Partners, suppliers, and investors also reassess their risk exposure, adjusting contractual terms or delaying collaborations. Public narratives form rapidly, especially in this day and age where social media amplifies criticism and shapes opinion almost in real time. Reputational damage tends to follow legal or regulatory exposure but can exceed it in severity, particularly when stakeholders perceive systemic neglect or lack of accountability.

Trust, once eroded, is difficult to rebuild. Business outcomes such as client retention, market expansion, and strategic partnerships are directly affected, with long-term consequences for growth and competitiveness. Organisations may find that even after operational normalcy is restored, the lingering perception of risk limits market opportunities and constrains the confidence of both existing and potential stakeholders.

In practice, reputational impact operates alongside legal and financial exposure, reinforcing the urgency of proactive data protection measures. The visibility and persistence of stakeholder perception ensure that reputational harm is not merely an ancillary consequence but a central risk that can amplify the effects of any breach or regulatory intervention. Organisations that underestimate it may find that the cost of regaining trust far outweighs any initial fines or operational disruptions.

5. OPERATIONAL AND GOVERNANCE IMPERATIVES: WHERE THINGS GO WRONG

Most data protection failures can be traced back to day-to-day operational practices rather than isolated errors. How an organisation collects, stores, and shares personal information in routine processes shapes the likelihood and severity of legal, financial, and reputational risks. Data that is gathered without clear purpose, maintained in incomplete or outdated records, or accessed without proper controls creates exposure before any external complaint or regulatory inquiry arises. Similarly, unchecked sharing with vendors or third parties compounds that risk, especially when contractual safeguards and monitoring mechanisms are absent.

Non-compliance is often a systemic issue. Lack of a privacy policy, inconsistent consent mechanisms, or fragmented record-keeping are rarely accidental; they reflect gaps in governance, oversight, and accountability. When responsibilities for data protection are unclear or unevenly distributed across an organisation, policies remain unimplemented and internal checks fail. Such governance lapses magnify the impact of even minor operational errors, allowing small mistakes to escalate into legal disputes, financial liabilities, or reputational damage.

Operational controls, therefore, are as critical as formal compliance measures. The establishment of clear policies, structured audits, employee training, and the appointment of a Data Protection Officer (DPO) are practical responses that mitigate risk, but only if integrated into daily practice. Organisations that treat compliance as an abstract obligation often lack these structures, leaving their systems vulnerable and reactive rather than proactive. Where operational and governance gaps exist, issues tend to surface late –and frequently, only after they have already caused measurable harm. This delayed visibility makes recovery more complex and costly, as legal, financial, and reputational consequences converge. Embedding strong operational controls and robust governance is therefore not an operational luxury; it is the frontline defence against the cascade of risks that emerge when personal data is handled carelessly.

6. CONCLUSION

Organisations that approach data protection as a box-ticking exercise or a distant regulatory concern risk far more than administrative inconvenience. The cumulative effect of legal, financial, and reputational exposure is rarely linear; a single misstep can ripple across systems, finances, and stakeholder trust, magnifying consequences that initially appear contained. Regulatory scrutiny under the NDPA does not operate in isolation, complaints, investigations, and enforcement actions expose not only the immediate incident but the broader organisational practices that enabled it, revealing gaps in governance, oversight, and operational discipline. Financially, penalties are often just the beginning; incident response, service disruptions, and the erosion of commercial relationships can generate cascading costs that outstrip initial fines. Equally potent is reputational impact: customers, partners, and the public respond to perceived neglect of personal data with hesitation, disengagement, and amplified criticism.

The lesson is clear: effective data protection is inseparable from robust operational and governance practices. Policies, audits, staff training, and clearly defined responsibilities are not merely compliance instruments, they are essential shields against escalating risk. Organizations that embed data protection into their decision-making processes not only mitigate potential liabilities but also signal reliability and accountability in a competitive, trust-driven market. In practical terms, treating personal data with diligence is not just a legal or ethical obligation; it is a strategic imperative whose neglect carries costs no organisation can afford to ignore.

REFERENCES

1. Nigeria Data Protection Act (NDPA) 2023
2. Adewale Ajayi & John Anyanwu, “The Nigeria Data Protection Act, 2023” KPMG [Online] https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023/ Accessed on 22nd March 2026.
3. Dotun Bhadmus, “Understanding Sanctions under the Nigeria Data Protection Act 2023 (Compliance Orders, Enforcement Orders, Criminal Sanctions) and the Legal Options Available to Data Subjects” Available at SSRN [Online]https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4539103Accessed on 22nd March 2026.
4. Folake Balogun, “NDPC fines MultiChoice N766m for Privacy Violation” BusinessdayNG [Online] https://businessday.ng/technology/article/ndpc-fines-multichoice-n766m-for-privacy-violation/ Accessed on 22ndMarch 2026.
5. Samuel Nwite, “Nigeria Data Protection Commission Fines Fidelity Bank ₦555.8m for Data Privacy Violations” Tekedia[Online] https://www.tekedia.com/nigeria-data-protection-commission-ndpc-fines-fidelity-bank-n555-8m-for-data-privacy-violations/ Accessed on 22nd March 2026.