DATA PROTECTION: HOW COMPLIANCE BUILDS CUSTOMER TRUST AND BUSINESS CREDIBILITY

Exploring how strong data governance enhances brand reputation, customer confidence and long-term growth.



Oladiran Falore
Managing Partner



Adaora Obi-Dike
Associate Counsel

SYNTEGRAL LP
March 2026

Abstract

As Nigeria's digital economy matures, data protection compliance is increasingly becoming a trust issue as much as a legal one. The Nigeria Data Protection Act 2023 ("NDPA" or "the Act") and the General Application and Implementation Directive 2025 (GAID) are designed not only to protect privacy rights, but also to promote the trusted use of data in a sustainable digital economy. That shift matters because customers, regulators, investors and commercial partners now read poor data governance as a sign of broader organisational weakness. Strong data governance, by contrast, signals seriousness, reliability and respect for people. This article argues that data protection compliance should no longer be treated as a narrow legal exercise. Properly understood, it is a business discipline that strengthens brand reputation, improves customer confidence, supports operational resilience and positions organisations for long-term growth.

Introduction

In 2025, what should have been an ordinary government support process became a quiet lesson in how easily public trust can be lost. Journalists reported that spreadsheets hosted on the Edo State Government's website had exposed the personal details of nearly 200 MSME loan applicants, including names, home addresses, phone numbers, bank account details, NINs and BVNs. There was no dramatic ransomware note and no sophisticated cyberattack scene. The data was simply there, in plain sight, on a public-facing government platform. For citizens, that kind of exposure cuts deeper than technical failure. It raises a more troubling question: if the institutions entrusted with public records cannot securely handle the most basic personal information, what confidence can the public reasonably place in the wider digital state?

The Nigerian framework reflects that reality. The Nigeria Data Protection Commission ("NDPC" or "Commission") describes its mission in terms that go beyond enforcement alone, emphasising fairness, integrity, accountability and transparency, and presenting data privacy as a cornerstone of a sustainable digital economy.

The GAID adopts the same orientation by expressly linking implementation of the Act to the trusted use of data. Taken together, those instruments show that Nigerian data protection law is not merely concerned with avoiding harm. It is also concerned with building confidence in the responsible use of information.

1. Compliance as a trust architecture

Many organisations still approach compliance with a defensive mindset. The goal is to avoid fines, satisfy auditors, and produce the required documentation. But that narrow view misses the wider commercial significance of privacy governance. Data protection rules shape how customers experience power, control and fairness in their interactions with a business. When an organisation is clear about what it collects, why it collects it, how long it keeps it, and who it shares it with, it signals maturity and discipline. When it is vague, evasive or careless, it signals disorder.

Consumer research reinforces this reality. PwC's 2024 Voice of the Consumer Survey reports that 83 per cent of respondents consider the protection of personal data one of the most important factors in earning their trust, while 80 per cent expect firm assurances that their information will remain private. A separate 2024 trust survey reached similar conclusions: consumers place high value on businesses that protect their data, respond promptly to concerns, and deliver a consistent, reliable experience. These findings matter commercially because they show that data protection has moved beyond a compliance checkbox. It has become a core determinant of trust.

The NDPA reflects the same logic. The Act is built on principles of lawful, fair and transparent processing, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, all anchored by accountability. It also grants data subjects practical rights: access, rectification, erasure, objection and portability. As these rights become real in the marketplace, privacy stops being an invisible backoffice function and becomes part of how customers decide whether a business deserves their confidence.

2. Why strong data governance enhances brand reputation

Brand reputation, an intangible asset is often spoken about in terms of advertising, public relations, and visual identity. Yet in reality, reputation is shaped just as much by the quiet, unseen habits within an organisation: how information is handled, how staff conduct themselves, how vendors are supervised, and how swiftly concerns are taken seriously.

A company that treats personal data with discipline tends to project discipline more broadly. Conversely, an organisation that appears careless with private information soon begins to look careless with its products, its service quality, and its internal controls.

The GAID underscores the reputational weight of governance. It expects organisations to maintain internal privacy strategies, stafffacing checklists, structured training programmes, ongoing awareness initiatives, and semiannual reporting by the Data Protection Officer to senior management. The DPO is expected to be actively engaged in dataprocessing matters, properly resourced, and positioned to report directly within the organisation. These expectations matter because they transform privacy from a passive policy into a visible management function.

For brands, the practical implication is clear. Trust grows when customers can see that privacy is governed by structure rather than slogans. An accessible privacy notice, a responsible point of contact, a prompt response to a rights request, and a clear explanation of how data is used often do more for a company's reputation than any polished marketing campaign. They communicate respect and customers recognise respect even when they do not speak in legal terms.

3. Customer confidence, loyalty and the economics of credibility

Customer confidence is not built solely by promising safety. It is built by creating an environment in which customers feel they retain dignity and control over their personal information. That is why over-collection of data, bundled consents, obscure retention practices and unexplained sharing arrangements can damage confidence even where no breach has occurred. The suspicion begins earlier: if a business asks for too much and explains too little, customers begin to question motive.

There is also an internal business case. Cisco's 2024 Data Privacy Benchmark Study found that privacy reporting has moved decisively into board oversight, with 98 per cent of respondents reporting at least one privacy metric to the board. Many of the most reported metrics, including audit results, data breaches, data subject requests and incident response, were closely tied to issues of customer trust. That is telling. Businesses increasingly understand that privacy performance is a proxy for credibility.

From a growth perspective, credibility lowers friction. It can improve onboarding completion, make customers more comfortable with digital self-service, reduce complaints, and support repeat transactions. It can also strengthen the confidence of investors, commercial counterparties and procurement teams, all of whom increasingly read privacy maturity as a sign of broader operational seriousness. In that sense, compliance is not only a cost centre. It is part of commercial enablement.

4. Long-term growth depends on privacy maturity

Long-term growth is far more sustainable when an organisation can scale without dragging hidden governance weaknesses into new products, new markets, or new partnerships.

This is precisely where data protection compliance becomes strategically valuable. A business that understands its data flows, classifies information by sensitivity, manages retention properly, tests its incidentresponse capability, and exercises real oversight over its processors is far better positioned to expand without inviting avoidable crises.

The NDPC's privacy by design white paper captures the broader policy point succinctly: robust data privacy standards form the bedrock of trusted and secure innovation. That framing matters. It rejects the false narrative that innovation and regulation sit in opposition. Well designed privacy controls do not stifle growth; they reduce the likelihood that growth will later be derailed by customer distrust, vendor failures, architectural weaknesses, or regulatory intervention.

Put more plainly, organisations that invest early in sound data governance spend far less time firefighting later. They respond to incidents with greater confidence, address customer concerns more effectively, and engage regulators from a position of preparedness rather than panic. In markets where trust is fragile and slow to rebuild, that level of readiness becomes a genuine competitive advantage.

5. Practical governance measures that build trust

If organisations wish to turn compliance into confidence, a few governance disciplines deserve special attention. First, data should be classified by sensitivity so that identity records, financial information, health information, biometric data and children's data attract higher levels of oversight. Secondly, collection practices should be revisited to ensure that only data that is genuinely necessary is requested at each stage of the customer journey.

- Publish clear, accessible privacy notices and ensure that channels for enquiries or rights requests are easy to locate and use.
- Empower the Data Protection Officer and embed structured privacy reporting within management and board oversight.
- Test breach response procedures through periodic tabletop exercises to expose gaps before they become liabilities.
- Apply rigorous due diligence and maintain strong contractual controls over processors and vendors.
- Monitor, review and refresh privacy and security controls continuously, rather than treating compliance as a oneoff project.

These measures matter because they move data protection away from ceremonial compliance and towards operational capability. The NDPA requires appropriate technical and organisational measures, while the GAID pushes organisations towards training, routine internal checks, monitoring and structured privacy governance. When these measures are taken seriously, customers tend to experience the organisation as clearer, safer and more dependable.

Conclusion

The most forward thinking organisations increasingly recognise that data protection is not merely a shield against regulatory trouble; it is a foundation for trust. The Nigerian framework makes that direction unmistakable, linking privacy to accountability, transparency, responsible innovation, and the trustworthy use of data within a sustainable digital economy. Global consumer research reinforces the point: people care deeply about how their information is handled, and they reward the brands that demonstrate respect for their data.

Ultimately, strong data governance delivers three outcomes simultaneously. It protects individual rights. It protects organisational reputation. And it protects commercial growth. For businesses operating in Nigeria's rapidly expanding digital landscape, this is not an abstract theory. It is a practical commercial truth. In a market where trust is hard won and easily lost, good privacy practice is no longer a peripheral compliance matter. It has become part of the brand itself.

Bibliography

➢ Nigeria Data Protection Act 2023

➢ General Application and Implementation Directive 2025.

➢ Nigeria Data Protection Commission, 'About Us' <https://ndpc.gov.ng/about-us/> accessed 21 March 2026

➢ Nigeria Data Protection Commission and Digital Africa Initiative Learning, 'Privacy by Design in Early-Stage Innovation' (2025) <https://ndpc.gov.ng/wp-content/uploads/2025/11/NDPC_DIAL-White-Paper-Privacy-by-Design-in-Early-Stage-Innovation-.pdf> accessed 21 March 2026.

➢ Cisco, '2024 Data Privacy Benchmark Study' (2024) <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf> accessed 21 March 2026.

➢ PwC, 'Trust in US Business Survey' (2024) <https://www.pwc.com/us/en/library/trust-in-business-survey.html> accessed 21 March 2026.

➢ PwC, 'Voice of the Consumer Survey 2024' <https://www.pwc.com/gx/en/issues/c-suite-insights/voice-of-the-consumer-survey/2024.html> accessed 21 March 2026.

Disclaimer:

The information provided in this publication does not, and is not intended to constitute legal advice. It is intended for general informational purposes only. Please contact us for further information.

Lagos Office: No 13, Mustapha Street, Off Olanrewaju Street, Billingsway, Oregun, Ikeja, Lagos.
Abuja Office: No. 16, Nkwere Street, Area 11, Garki, Abuja, FCT.
Email: info@syntegrallp.com
Telephones: 08025754547, 08023007172, 07015694060

© Copyright 2026 - Syntegral Legal Practice