

From Regulatory Exposure to Financial Loss:

Why Data Governance Must
Become a Boardroom Priority



Introduction

A corporate crisis does not always begin with a balance-sheet shock or setback. It may begin with a regulator asking questions that the organisation cannot confidently answer: What data does it hold? Why was it collected? Who can access it? How long is it retained? What safeguards govern its use, storage and disclosure?

As organisations increasingly rely on data for decision-making, innovation and service delivery, weaknesses in how that data is governed can expose them to regulatory scrutiny before the resulting financial, operational and reputational consequences become fully apparent. Data governance is therefore no longer solely an information technology, legal or compliance concern. It is an enterprise-risk issue requiring board-level oversight.

What Regulators Ask

- *What data does it hold?*
- *Why was it collected?*
- *Who can access it?*
- *How long is it retained?*
- *What safeguards govern its use, storage and disclosure?*

The Companies and Allied Matters Act 2020 ("CAMA") requires directors to act in the company's best interests and to exercise the care, diligence and skill expected of a reasonably prudent director. The Nigerian Code of Corporate Governance 2018 ("NCCG") further places responsibility on the board for legal compliance, risk management, internal control and information-technology governance, including the approval of the company's information-technology data-governance framework.¹ Whilst Nigeria Data Protection Act 2023 ("NDP Act or the Act") reinforces this responsibility by requiring personal data to be processed lawfully, fairly, transparently, and securely, while imposing duties of care and accountability on data controllers and processors.²

In light of the above, this article critically examines how inadequate data governance can progress from regulatory exposure to financial loss and identifies the measures boards should take to protect corporate value and strengthen organisational resilience. The article also argues for elevating data governance to a board-level responsibility, as this would help manage risk and maintain the trust of customers, regulators, and investors alike.

This article critically examines how inadequate data governance can progress from regulatory exposure to financial loss — and argues for elevating data governance to a board-level responsibility.

Why Data Is Now a Board-Level Asset and a Board-Level Risk

The legal framework reflects data's dual character. The NDP Act seeks to strengthen Nigeria's digital economy through the beneficial and trusted use of personal data, while safeguarding data subjects' rights, regulating processing and providing remedies for breaches.³

Data protection also has a constitutional foundation. Section 37 of the Constitution guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. In **Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission**⁴, the Court of Appeal held that the protection afforded by section 37 extends to personal information and personal data.⁵ This does not mean that every weakness in an organisation's data-governance framework automatically constitutes a constitutional violation. It does, however, confirm that the unlawful handling of personal data may engage both statutory obligations and constitutionally protected privacy interests.

A distinction must therefore be maintained between data governance and data protection. Data governance concerns the structures and controls through which an organisation manages its information assets. In contrast, data protection, governed by the NDP ACT, applies specifically to personal data, information relating to an identified or identifiable individual.⁶

The issue belongs at the board level because the Nigerian Code of Corporate Governance 2018 contemplates an information-technology data-governance framework designed to mitigate data risks and manage relevant assets effectively. The framework may address cyber threats, risks arising from third-party and outsourced service providers, and periodic independent assurance.⁷ The Code recommends that the relevant board committee review the framework and recommend it for board approval at least annually.⁸

A Distinction Worth Maintaining

Governance

Broader · Structures & Controls

Concerns the structures and controls through which an organisation manages its information assets.

Protection

Subset · Personal Data under the NDP Act

Applies specifically to personal data — information relating to an identified or identifiable individual.

What the NDP ACT Requires and What the Board Must Oversee

The NDP Act imposes its principal obligations on data controllers and data processors, not directly on their boards. However, when a company processes personal data, the board should ensure management has established effective compliance structures. The Act requires personal data to be processed fairly, lawfully and transparently, and obliges controllers and processors to implement appropriate safeguards, exercise a duty of care and demonstrate accountability.⁹

Compliance must also be continuous. The General Application and Implementation Directive 2025 requires organisations to identify their statutory obligations, prepare compliance schedules, conduct periodic audits, maintain semi-annual data-protection reports, monitor their data-security systems and undertake organisation-wide privacy training.¹⁰ These requirements move data protection beyond annual filings and privacy notices to an ongoing governance discipline supported by records, reporting and internal assurance.

Responsibility must be clearly allocated. A data controller of major importance must designate a Data Protection Officer with appropriate expertise. The organisation must involve the DPO in matters relating to personal data processing, provide adequate resources and access, preserve the officer's independence and ensure an appropriate reporting line to management. With the guidance of the data controller or Data processor, the DPO must also compile and submit a semi-annual report on the organisation's compliance status.¹¹

A lawful basis must support each processing activity involving personal data. Section 25 recognises consent, contractual necessity, legal obligation, vital interests, public interest or official authority, and legitimate interests subject to statutory limitations.¹² In *Araka v Ecart Internet Services Nigeria Ltd & Anor*,¹³ The Federal High Court affirmed that contractual necessity justifies processing only connected with the performance of the relevant contract. It held that personal data obtained for order fulfilment could not lawfully be repurposed for direct marketing without an applicable lawful basis.¹⁴

High-risk processing must also be assessed before deployment. Section 28 requires a Data Protection Impact Assessment where processing is likely to create a high risk to the rights and freedoms of data subjects. Boards should require management to review periodically whether the organisation qualifies as a controller or processor of major importance and is therefore subject to registration and related compliance obligations.¹⁵

High-risk processing must also be assessed before deployment. Section 28 requires a Data Protection Impact Assessment where processing is likely to create a high risk to the rights and freedoms of data subjects.

Why Checklist Compliance is not Enough

Registration, annual compliance filings and policy documents are important, but they do not establish that an organisation's data-governance framework is operating effectively. The GAID expressly provides that Registration, compliance audit returns, Data Protection Impact Assessments and approved cross-border transfer instruments may demonstrate accountability and prima facie good faith, but do not replace concrete evidence of compliance when a complaint concerns another obligation under the NDP Act.¹⁶

The same outcome-focused approach is reflected in the Nigerian Code of Corporate Governance 2018. Its "Apply and Explain" philosophy requires companies to demonstrate how their governance practices achieve the intended outcomes, rather than rely on a box-ticking exercise.¹⁷ For boards, this means requiring evidence that approved policies are implemented, data-subject requests are addressed, processing activities are reviewed, vendors are supervised, and identified risks are escalated and remediated.

The consequences of ineffective implementation extend beyond procedural non-compliance. Following an investigation, the Commission may order an organisation to remedy a violation, compensate an affected data subject or pay a penalty or remedial fee. For a controller or processor of major importance, the applicable maximum is the greater of ₦10,000,000 (Ten Million Naira) and 2% of its annual gross revenue in the preceding financial year. For other controllers and processors, it is the greater of ₦2,000,000 (Two Million Naira) and 2% of annual gross revenue.¹⁸ A data subject who suffers injury, loss or harm may also recover damages through civil proceedings.¹⁹

Statutory Penalty Tier · Maximum Exposure

Controller or Processor of Major Importance

₦10M

OR 2% of annual gross revenue

**WHICHEVER IS GREATER
PRECEDING FINANCIAL YEAR**

Other Controllers & Processors

₦2M

OR 2% of annual gross revenue

**WHICHEVER IS GREATER
PRECEDING FINANCIAL YEAR**

Beyond the Fine: How Data-Governance Failures Become Corporate Crises

Financial penalties are only one consequence of inadequate data governance. The NDP Act also requires personal data to be accurate and protected through appropriate technical and organisational measures. Poor-quality data may weaken business decisions, while inadequate security can expose the organisation to operational disruption, regulatory investigation and remedial costs.²⁰

A personal data breach can also trigger immediate legal and organisational obligations. Where a breach is likely to create a high risk to the rights and freedoms of data subjects, the data controller must notify the Commission within 72 hours of becoming aware of it.²¹ Where the risk is high, affected data subjects must be informed immediately in clear language and advised on steps to mitigate the possible effects. Controllers and processors must also maintain records of breaches and the remedial action taken. The Commission may itself make a public communication where it considers the controller's notification measures inadequate.²² Effective governance therefore requires an incident-response framework capable of identifying, assessing, escalating and responding to breaches within the statutory timelines.

Artificial intelligence creates an additional area of exposure. Section 37 of the NDP Act 2023 protects individuals against decisions based solely on automated processing that produce legal or similarly significant effects, subject to limited exceptions and safeguards, including human intervention and the right to contest the decision. GAID further requires organisations deploying artificial intelligence and other emerging technologies for personal-data processing to establish documented controls, undertake impact assessments, test for adverse outcomes and continuously monitor deployed systems.²³

Operational

Inadequate security widens the door to disruption, system compromise and the operational costs of containment.

Reputational

Public communication, customer loss and erosion of trust follow any incident the Commission considers inadequately handled.

Financial

Beyond statutory penalties, weakened decisions and remediation costs compound the original loss to the business.

What Boards Should Do Now

The board's role is not to manage day-to-day data processing, but to ensure that management has established an effective and adequately resourced governance framework. At a minimum, boards should require the following:

- 01 Establish visibility and ownership**
Management should maintain an accurate record of processing activities showing the categories of personal data held, the purposes of processing, recipients, storage locations, retention periods and applicable lawful bases. Clearly allocate executive responsibility, while the DPO retains an independent advisory and monitoring role.²⁴
- 02 Approve a documented data-governance framework:**
The framework should address data quality, access, retention, security, data-subject rights, third-party processing, incident response and the deployment of emerging technologies. Consistent with the Nigerian Code of Corporate Governance 2018, the relevant board committee should review the company's information-technology data-governance framework and recommend it for board approval at least annually.²⁵
- 03 Require regular reporting and assurance:**
Board reporting should cover material incidents, unresolved data-subject requests, compliance audits, high-risk processing, Data Protection Impact Assessments, significant vendor risks and the status of remedial actions. The DPO's semi-annual report provides a statutory foundation for this reporting process.
- 04 Strengthen third-party controls:**
Before appointing processors or technology vendors, management should undertake appropriate due diligence and ensure that written agreements address compliance, security, confidentiality, data-subject rights, breach escalation and the use of subcontractors.²⁶
- 05 Embed compliance throughout the organisation:**
Organisation-wide awareness should be supplemented by role-specific training for employees whose functions involve personal data, cybersecurity, procurement, artificial intelligence or incident response. Registration status, breach-response procedures, and business-continuity arrangements should also be reviewed periodically, not only after a regulatory complaint or incident.

Treat these measures as continuing governance disciplines — not annual compliance exercises.

Conclusion

Weak data governance can quickly move from statutory non-compliance to financial, operational, and reputational loss. The Nigerian legal and corporate-governance framework does not require directors to perform the operational functions of management, the DPO or information-technology teams. It does, however, require boards to ensure that material risks, legal obligations and internal controls are properly governed.

A credible framework therefore requires clear executive ownership, independent DPO monitoring, documented processing activities, effective vendor controls, risk-based security, timely incident response and periodic assurance to the board. Organisations that treat these measures as continuing governance disciplines, rather than annual compliance exercises, will be better placed to protect personal data, demonstrate accountability and preserve corporate value. In an increasingly data-dependent economy, board inattention to data governance is itself a material governance risk.

In an increasingly data-dependent economy, board inattention to data governance is itself a material governance risk.

Contributors



Ituah Imhanze, FCArb
Partner, Data Protection



**Muhammad Yasir
Abubakar-Sadiq, AICMC**
Associate, Data Protection



Kosisochukwu Ngwu
Associate, Data Protection

For further information on the issues discussed in this article,
contact our legal team at counsel@kennalp.com

Endnotes

1. Companies and Allied Matters Act 2020, ss 305(3) and 308(1)–(3); Nigerian Code of Corporate Governance 2018, Recommended Practices 1.3, 1.9, 1.10, 1.12 and 11.5.6.6.
2. Nigeria Data Protection Act 2023, ss 24(1)–(3).
3. Nigeria Data Protection Act 2023, s 1(1)(a)–(h).
4. (2021) LPELR-55623(CA).
5. Constitution of the Federal Republic of Nigeria 1999, s 37
6. Nigeria Data Protection Act 2023, ss 2(1) and 65.
7. Nigerian Code of Corporate Governance 2018, Principle 11 (Board Committees), Recommended Practice 11.5.6.6(b)–(c) and (e). The provision's full list also includes development of IT strategy and policy, para (a) and assessment of value delivered through IT investments, para (d).
8. Nigerian Code of Corporate Governance 2018.
9. Nigeria Data Protection Act 2023, s 24(1)–(3).
10. Nigeria Data Protection Act—General Application and Implementation Directive 2025, art 7.
11. Nigeria Data Protection Act 2023, s 32; Nigeria Data Protection Act—General Application and Implementation Directive 2025, arts 11–13.
12. Nigeria Data Protection Act 2023, s 25
13. (2025) 3 CLRN 75, 83–84.
14. Nigeria Data Protection Act 2023, s 25
15. Nigeria Data Protection Act 2023, ss 28 and 44; Nigeria Data Protection Act—General Application and Implementation Directive 2025, arts 8–10 and 28.
16. Nigeria Data Protection Act—General Application and Implementation Directive 2025, art 48(1)–(3).
17. Nigerian Code of Corporate Governance 2018, 'Code Philosophy'.
18. Nigeria Data Protection Act 2023, ss 48 (4) and (5).
19. Nigeria Data Protection Act 2023, ss 48(1)–(6) and 51.
20. Nigeria Data Protection Act 2023, ss 24(1)(e)–(f) and 39.
21. Nigeria Data Protection Act 2023, ss 40 (2)
22. *ibid* s 40(1)–(9).
23. *ibid* s 37; Nigeria Data Protection Act—General Application and Implementation Directive 2025, arts 28(3) and 43.
24. Nigeria Data Protection Act—General Application and Implementation Directive 2025, arts 7 and 13.
25. Nigerian Code of Corporate Governance 2018, Recommended Practice 11.5.6.6.
26. Nigeria Data Protection Act 2023, ss 29 and 40.



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

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner, 400211
Enugu State.

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