

Insights & Outcomes Report

KENNA Data Protection
Executive Dialogue

Theme:

“From Policy to Practice:
Navigating Data Protection Compliance
in a Digitally Evolving Nigeria”

Data Protection Insight

January 2026

Executive Overview

01 Event Context & Objectives

Timely convergence of regulators, CEOs, and legal practitioners on September 18, 2025—the eve of GAID 2025 effectiveness.

 Unveiling Legal and Regulatory Aspects of Data Protection in Nigeria publication.

02 Board Governance & Fiduciary Duties

Professor Fabian Ajogwu's framework on data protection as a strategic governance pillar requiring board-level oversight.

 Three fiduciary duties: Care, Loyalty, and Good Faith .

03 Regulatory Perspective & Compliance

NDPC's guidance on building an 'economy of trust' and the transition from awareness to full enforcement mode.

 Over 1,000 companies under investigation across key sectors.

04 Panel Dialogue: Policy to Practice

Multi-sector perspectives on the compliance journey: MTN's in-house approach, legal advisory challenges, and academic insights.

 Consensus: Nigeria is "policy rich, practice evolving, fast" .

05 Key Outcomes & Next Steps

Strategic imperatives: board-level leadership, compliance as competitive advantage, and ecosystem strengthening.

Event Context & Timely Significance

Venue & Purpose

The Data Protection Executive Dialogue convened at **Black Diamond Hotel (Onyx Hall), Lagos**, bringing together the regulator, CEOs, board members, legal practitioners, compliance professionals, academics, and stakeholders across key economic sectors.

The event served a dual purpose: interrogating practical realities of data protection compliance under Nigeria's evolving regulatory framework, and unveiling the comprehensive intellectual resource, "**Legal and Regulatory Aspects of Data Protection in Nigeria**".

Critical Timing

The dialogue occurred on the eve of GAID 2025 effectiveness (September 19, 2025), creating unprecedented urgency for organizations to transition from policy awareness to practical implementation.

Nigeria's digital transformation, combined with regulatory reforms, positioned this dialogue as both urgent and necessary for stakeholders navigating the compliance landscape.

Stakeholder Representation

 Regulators NDPC, FCCPC	 C-Suite CEOs & Board Members
 Legal Practitioners & Advisors	 Academia Scholars & Researchers
 Key Sectors Finance, Telecom, Healthcare, Technology	

Publication Unveiled

The dialogue featured the official presentation of "**Legal and Regulatory Aspects of Data Protection in Nigeria**", a comprehensive intellectual resource filling a critical gap in Nigerian legal literature.

The Digital Transformation Imperative

Data as the New Currency

Professor Ajogwu emphasized that data is the new currency of the digital economy , influencing strategic decision-making, customer engagement, financial growth, and competitiveness.

While data provides immense opportunities, it also exposes organizations to grave risks: data breaches, privacy violations, erosion of stakeholder trust, regulatory sanctions, and damage to corporate reputation.

Watershed Regulatory Moment

NDPA 2023 + GAID 2025

Professor Ajogwu stated that these instruments represent a **watershed moment in Nigeria's regulatory framework**, modeled after international standards like the EU GDPR 2018.

They provide a strong legal backbone for data protection in Nigeria's digital economy
The Challenge How to transition from policy to practice within organizations..



Financial Technology

Widespread cloud adoption creating new data storage and processing challenges.



Artificial Intelligence

AI-driven platforms requiring vast datasets for machine learning algorithms.



Cloud Computing

Rapid fintech innovation resulting in unprecedented personal data collection.



E-Governance

Digital government services collecting sensitive citizen information at scale.

The Dual Reality

↑ OPPORTUNITIES

Strategic insights, customer engagement, financial growth, competitive advantage

↓ RISKS

Data breaches, privacy violations, regulatory sanctions, reputational damage

Critical Reality: This digital transformation has introduced heightened risks of cyber-attacks, misuse of personal data, and systemic vulnerabilities that threaten organizational stability and stakeholder trust.

Board Fiduciary Responsibilities in Data Protection

Core Principle: Data protection is no longer a mere compliance function delegated to IT departments but a governance issue requiring board-level oversight.



01

Duty of Care

Ensuring informed and diligent decisions about data governance frameworks, cybersecurity budgets, and risk management policies.

Boards must exercise reasonable care in overseeing data protection strategies, ensuring adequate resources are allocated and risks are properly assessed and mitigated.

- ✓ Review and approve cybersecurity budgets
- ✓ Oversee data governance frameworks
- ✓ Monitor risk management policies



02

Duty of Loyalty

Avoiding conflicts of interest in data use and prioritizing the protection of stakeholders' privacy rights above commercial interests.

Boards must ensure that data processing activities serve the best interests of data subjects and do not create undisclosed conflicts or prioritize profit over privacy.

- ✓ Disclose data use conflicts
- ✓ Prioritize stakeholder privacy
- ✓ Avoid undisclosed commercialization



03

Duty of Good Faith

Embedding ethical standards and transparency in how data is collected, processed, and shared with all stakeholders.

Boards must champion a culture of honesty and integrity, ensuring transparent communication about data practices and honoring the reasonable expectations of data subjects.

- ✓ Champion transparency culture
- ✓ Honor data subject expectations
- ✓ Ensure clear communication

Strategic Implementation Framework

Strategic Imperative: Boards must treat data protection as a strategic pillar of governance, on par with financial performance and operational growth .



01

Budgetary Allocation

Deliberate investment in cybersecurity infrastructure, staff training, compliance audits, and appointment of Data Protection Officers (DPOs) or accredited Data Protection Compliance Organisations (DPCOs).

Cybersecurity Infrastructure

Advanced security tools, firewalls, intrusion detection systems, and encryption technologies.



Staff Training & Awareness

Continuous education programs to embed data protection culture across all organizational levels.



Compliance Audits

Regular assessments using NDPC-licensed DPCOs to ensure ongoing regulatory adherence.



02

Committee Oversight

Integration of data protection into board committees such as the Audit & Risk Committee or creation of a dedicated Technology/Data Committee.

Audit & Risk Committee Integration

Embed data protection oversight into existing committee structures for comprehensive risk management.

✓ Regular compliance reporting

Dedicated Technology Committee

Establish specialized committee focused on technology governance, cybersecurity, and data protection.

✓ Specialized expertise focus



03

Board Expertise

Inclusion of directors with technological literacy and cybersecurity expertise to guide strategic decision-making.

Technological Literacy

Directors who understand technology trends, digital transformation, and data-driven business models.

✓ Cloud computing understanding



Cybersecurity Expertise

Board members with knowledge of cybersecurity frameworks, threat landscapes, and protection strategies.

✓ Incident response planning

Privacy by Design & Case Study



Privacy by Design Principles

Professor Ajogwu stressed the importance of embedding "privacy by design" into organizational culture and processes , rather than treating it as an afterthought.



DPIAs

Identify and mitigate risks in high-risk projects before launch.



Data Minimisation

Collect only what is strictly necessary for defined purposes.



Encryption

Protect data at rest and in transit with strong encryption.



Anonymisation

Remove identifying information to protect individual privacy.



Pseudonymisation

Replace identifiers with pseudonyms to reduce risk.



RBACs

Restrict access based on roles and responsibilities.

Practical Nigerian Examples



Law Firms

Multi-factor authentication



Banks

SIM-NIN linkages



Telecoms

Cloud-based access controls



Case Study

\$220M

Meta/WhatsApp Fine (Nigeria)

Context: FCCPC and NDPC imposed a **\$220 million fine** on Meta/WhatsApp for discriminatory and exploitative data practices.

This case underscores the gravity of board-level responsibility in data governance.

Lesson 1

Compliance frameworks must be constantly updated.

Lesson 2

Transparency is non-negotiable; silence undermines trust.

Lesson 3

Cross-border data transfers require heightened oversight.



Incident Preparedness

Security breaches are inevitable. The true measure of governance lies in preparedness and response.

- 1 Ensure incident response plans are in place and regularly tested.
- 2 Mandate regular reporting on compliance audits, breaches, and remediation.
- 3 Integrate data protection KPIs into corporate performance metrics.

NDPC: Building Trust as a Business Imperative

Core Principle: The NDPA's backbone is to build an "economy of trust" where business sustainability depends on customer trust in data handling.

The Trust Imperative

Ms. Owa emphasized that **businesses must recognize sustainability depends on whether customers trust them** to use personal data responsibly.

48%

Consumer Impact

of consumers stopped using services after discovering data misuse, per a U.S. survey.

Uniquely Nigerian Innovation

Duty of Care Principle

The NDPA introduces a uniquely Nigerian innovation: the **principle of duty of care**. This complements existing principles by establishing that data controllers have a legal duty to prevent harm from their handling of personal data.

Practical Compliance Measures

Boards and CEOs were reminded that **compliance cannot be delegated away** — it must be driven from the top.



Registration with NDPC

Register as a data controller or processor of major importance.



Annual Data Protection Audits

Conduct audits using NDPC-licensed DPCOs, in collaboration with an internal DPO.



Data Privacy Impact Assessments

Carry out DPIAs before high-risk processing (e.g., AI tools, cross-border transfers).



Vendor & Third-Party Compliance

Ensure service providers are contractually and practically compliant.

Compliance Measures & Enforcement Transition

Enforcement Transition

The NDPC has transitioned fully into enforcement mode . Over **1,000 companies** across sectors have been flagged for investigation.

Targeted Sectors

 Finance

 Insurance

 Healthcare

 Gaming

Consequences of Non-Compliance

Boards were urged to take compliance seriously to avoid severe consequences.



Hefty Fines

Significant financial penalties



Expensive Litigation

Legal costs and damages



Reputational Damage



Operational Disruptions

Service shutdowns

Extraterritorial Application

Section 22 of the NDPA

Provides for **extraterritorial application** to cross-border transactions. Companies targeting Nigerian data must comply, regardless of physical presence. NDPC has already taken enforcement against international entities.

Panel Dialogue: From Policy to Practice

The 40-minute panel balanced regulatory, legal, corporate, and academic views. The moderator asked: "Policy rich? Practice efficient? or somewhere in between?"



In-House Counsel

Ms. Ifeoma Utah

General Manager, MTN Nigeria



Advisory Practice

Ms. Nimma Jo-Madugu

Partner, KENNA



Academic Perspective

Dr. Peter Bamkole

Deputy Vice Chancellor, Pan-Atlantic University

Embedding Data Protection in Contracts

Ms. Utah outlined how data protection is embedded in contracts:

- ✓ Begin major transactions with a DPIA.
- ✓ Tailor contracts; data-heavy agreements need elaborate clauses.
- ✓ MTN negotiated a single data protection annexure for **nine months**.

Top Pain Points in Compliance

Ms. Jo-Madugu explained the challenges in interpreting the NDPA and GAID:

- ⚠ Convincing clients to comply is like early corporate governance struggles.
- ⚠ Many boards dismiss compliance as unnecessary until enforcement hits.
- ⚠ Shift from soft law (NDPR 2019) to hard law (NDPA 2023) eliminates excuses.

Preparing Next Generation

Dr. Bamkole highlighted educational and enterprise implications:

- 🛡 Cybersecurity risks are the #1 priority on risk registers.
- 🎓 Universities must educate students early about privacy and digital risk.
- 💻 Data is not just currency but **"trust currency"**.

Interactive Q&A: Critical Legal Clarifications

Q1 Jurisdictional Overlaps

Is there exclusive jurisdiction or can parties engage in forum shopping with NDPC, CBN, FCCPC, and courts active?

NDPC Response:

NDPC is the **primary regulator** for processing personal data. Inter-agency MOUs prevent conflict while NDPC retains enforcement powers.

Q3 Regulator Accountability

How is NDPC addressing public agencies' mishandling of sensitive data?

NDPC Response:

Duty of care applies equally to public regulators.
NDPC is embedding safeguards and will hold regulators accountable for mishandling sensitive data.

Q2 Legislative Timing

Nigeria's NDPA (2023) came six years after GDPR (2018). Is it already outdated?

NDPC Response:

Being "late" was an advantage. NDPA is among the most comprehensive globally, with innovations like the duty of care principle.

Q4 Cross-Border Application

How does the NDPA apply to international companies without a Nigerian office?

NDPC Response:

Section 22 provides for extraterritorial application. Companies targeting Nigerian data must comply, regardless of physical presence.

STRATEGIC IMPERATIVES

Forward Commitments



Business Imperative

Data protection is no longer theoretical but a business imperative requiring board-level leadership.



Globally Relevant

The NDPA is a globally relevant, locally adapted framework suited for Nigeria's digital evolution.



Trust & Competitiveness

Compliance is about building trust, competitiveness, and sustainability .



Ecosystem Strengthening

A commitment to strengthening Nigeria's data protection ecosystem .

“

The question for boards is not whether they can afford to prioritise data protection, but whether they can afford not to.”

— Professor Fabian Ajogwu, OFR, SAN —



CONTACT US

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,
Old Emene Road, by AC Drug,
Thinkers Corner, Enugu.

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

