

Data Protection Outlook 2026

Nigeria

A forward-looking assessment of the regulatory, judicial, and legislative landscape shaping Nigeria's digital economy.



Executive Summary

Data protection is no longer a peripheral compliance activity but a core infrastructural component of Nigeria's digital economy. This report provides strategic intelligence for navigating the transition from policy articulation to rigorous enforcement in 2026.

1 The Digital Economy Context

Data protection has become foundational to Nigeria's digital economy. As financial services, telecommunications, e-commerce, digital lending, health technology, and platform-based business models continue to expand, personal data now forms a critical part of the infrastructure.

The integration of data-driven technologies has created a landscape where the lawful processing of personal information is inextricably linked to operational viability and market access.

2 Trust and Accountability

Trust, accountability, and lawful data processing are no longer minor compliance considerations but essential enablers of innovation, investment, and cross-border trade.

Organizations that fail to embed these principles risk not only regulatory sanctions but also reputational damage that can erode consumer confidence and investor trust in an increasingly competitive digital marketplace.

3 Report Scope and Objectives

It is against this backdrop that this KENNA Data Protection Outlook 2026 provides a forward-looking assessment of Nigeria's data protection landscape. We examine regulatory, judicial, legislative, and market developments that will shape compliance and enforcement over the next 12 months.

This report is designed to help you understand emerging risks, opportunities, and strategic imperatives under Nigeria's evolving data governance framework.

Growth Metrics

15%  YoY

Projected expansion of digital economy contribution to GDP in 2026.

Strategic Pillars

- ✓ Regulatory Enforcement
- ✓ Judicial Precedents
- ✓ Market Adaptation
- ✓ Global Integration

“

“Compliance has transitioned from a mere obligation to an immediate and enforceable reality.”

— 2025 Retrospective

Reflections on 2025

Analyzing the transition from policy articulation to sustained regulatory enforcement under the Nigeria Data Protection Commission.



Section Overview

The year 2025 marked an expansion of the Nigeria Data Protection Commission's regulatory foothold. With the release of the General Application and Implementation Directive (GAID) 2025 and increasingly assertive supervisory actions, data protection compliance transitioned from a mere obligation to an immediate and enforceable reality.



Early 2025
Ongoing

2.1 Institutional Enforcement Posture

In 2025, the NDPC enhanced its regulatory authority, advanced its supervisory mandate, and positioned itself as a central actor in Nigeria's digital governance ecosystem. Its actions reflected a regulator confident in its statutory footing.

Execution of sector-wide compliance initiatives.
Deployment of targeted investigations¹ into systemic breaches.
Imposition of material administrative sanctions to deter non-compliance.



March 2025
Published

2.2 GAID Issuance & Implementation

The publication of the General Application and Implementation Directive (GAID) was the year's most significant regulatory milestone. Following extensive consultations, it provided operational clarity on:

Effective Date: September 19, 2025
Key Provisions: Lawful bases for processing, cross-border transfer mechanisms, audit requirements, and institutional accountability frameworks.



Mid 2025
Regulatory Update

2.3 Registration Framework Revision

The NDPC revised the mandatory registration guidance note² following judicial intervention.³ This demonstrated the Commission's responsiveness to legal scrutiny and its willingness to refine regulatory instruments to withstand judicial review, ensuring a robust and legally sound registration process.



August 2025
Enforcement Action

2.4 Investigation List Publication

In a major transparency initiative, the NDPC published a comprehensive list of over 1,300 organisations under investigation. These entities were named for potentially failing to comply with their statutory obligations under the Nigeria Data Protection Act (NDPA) 2023.

This action signaled a shift towards "naming and shaming" as a tool for enforcing accountability.

Key Takeaway for 2025

"The central lesson of 2025 is that accountability is now immediate. Non-compliance carries tangible financial, operational, and reputational consequences, driven by a regulator equipped with a full enforcement toolkit."

Reflections on 2025 (II): Enforcement Analysis & Judicial Trends

03

2.1 Financial Penalties Analysis

Administrative Sanction

₦766.2M

Imposed on a digital satellite TV provider (August 2025)

The imposition of a ₦766.2 million fine marked a watershed moment⁴ in Nigerian data protection enforcement. Unlike previous warnings, this sanction targeted a major player in the telecommunications and media sector, directly addressing privacy breaches and unlawful cross-border data transfers.

Implication:

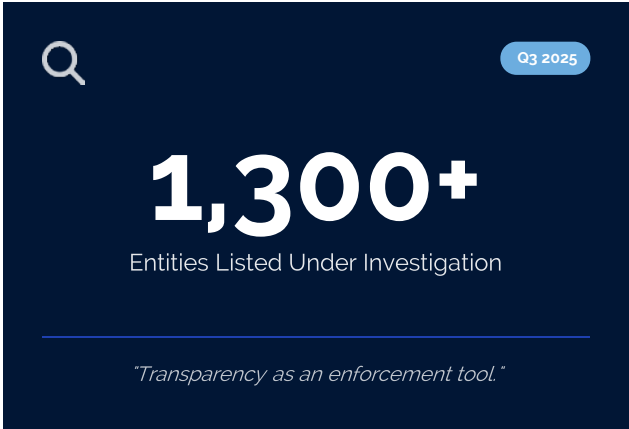
This sends a definitive signal that the NDPC has moved from "correction" to "deterrence," with penalties now scaled to reflect the severity of the breach and the entity's financial standing.

2.2 Investigations Overview

In August 2025, the NDPC published a comprehensive list of organizations under investigation, signaling a new era of transparency and public accountability. This "naming and shaming" approach complements traditional enforcement mechanisms.

Furthermore, the launch of an investigation into the Joint Admissions and Matriculation Board (JAMB)⁶ demonstrates that **public institutions are not insulated** from regulatory oversight.

Additionally, a dispute with a major international social media platform was resolved through an out-of-court settlement in November⁵, illustrating the NDPC's capacity to engage global tech giants while asserting Nigerian data sovereignty.



2.3 Judicial Developments & Precedents

High Court Ruling: Commercial Bank Liability⁷

Case Reference: Data Mismanagement & Economic Loss

Damages Awarded

₦5,000,000

Transaction Failure

₦200,000,000

The court affirmed that economic loss flowing from data misuse is actionable.⁸ A bank's data mismanagement led to a failed property transaction, resulting in liability.

Key Judicial Principles Established in 2025:

➤ **Direct Access to Courts:** Courts clarified that aggrieved data subjects may approach the court directly without first petitioning the NDPC. Regulatory complaints are discretionary, not mandatory.⁹

➤ **Marketing Consent:** In decisions involving intrusive robocalls, courts issued perpetual injunctions and clarified that a data subject's objection to marketing is absolute.¹⁰

"Collectively, these decisions strengthened private enforcement and significantly increased litigation risk for non-compliant organizations."

2.4 Sectoral Regulation Expansion

Sectoral regulators deepened data governance obligations across regulated industries¹⁶ in 2025:

- ✓ NAICOM's Insurtech Guidelines
- ✓ FCCPC's Digital Lending Regulations
- ✓ NCC's draft Internet Code of Practice

2.5 International Alignment

Nigeria reinforced its continental leadership and global integration efforts:

Hosted African DPAs

Global CBPR Forum
Associate Member

Regulatory Pipeline & GAID Enforcement

Strategic Shift: From Interpretation to Implementation

Nigeria enters 2026 with a data protection framework that has moved beyond the formative era into an era of operational maturity. The coming year will be defined less by new statutory architecture and more by how aggressively, consistently, and strategically existing powers are exercised.

The NDPC's regulatory posture in 2026 will be anchored on deepening implementation rather than expanding statutory scope. The focus will be on refining compliance mechanics, closing enforcement gaps, and increasing regulatory predictability.

— 3.1 Full Enforcement of the GAID

The General Application and Implementation Directive (GAID) will continue to function as the NDPC's principal compliance instrument. In 2026, the emphasis will shift from reliance on interpretation to strict operational enforcement. Organisations should expect the following developments:

Standard Contractual Clauses (SCCs)

Transfer-safeguard templates will be formally issued, eliminating uncertainty around lawful cross-border transfers. This will provide a definitive mechanism for multinational entities to regularize international data flows.

Sector-Specific Codes of Conduct

Introduction of tailored compliance benchmarks, particularly for **fintech, telecommunications, digital lending, and platform-based businesses**. These codes will introduce granular obligations that go beyond generic NDPA requirements.

Compliance Audit Return (CAR) Guidance

Expect detailed guidance including standardised reporting templates and significantly increased scrutiny of submissions. The era of "tick-box" compliance audits is effectively over; audits must now demonstrate substantive governance controls.

Professionalisation of Compliance

Formalisation of Data Protection Officers (DPO) Annual Credential Assessments (ACA) and a clearer licensing and supervision framework for Data Protection Compliance Organisations (DPCOs), effectively professionalising the compliance market.

Expected Developments

- ✓ Formal issuance of transfer-safeguard templates.
- ✓ Tailored benchmarks for fintech & digital lending.
- ✓ Standardised reporting templates for CAR.
- ✓ Licensing framework for DPCOs.

Compliance Implications

Non-compliance with GAID-driven obligations is likely to attract **expedited enforcement**.

Critical Risk: Breaches that expose systemic governance failures will face the harshest penalties, moving beyond simple fines to operational restrictions.

Maturity Curve



Regulatory Harmonisation & Open Banking Governance

— 3.2 NDPC and Sectoral Regulatory Harmonisation

Regulatory fragmentation has historically increased compliance friction for Nigerian businesses operating across multiple jurisdictions. In 2026, regulatory harmonisation will transition from a policy aspiration to an operational necessity. The NDPC is expected to conclude formal Memoranda of Understanding (MOUs) and joint supervisory frameworks with key sector regulators to eliminate overlaps and enforcement conflicts.

This strategic alignment will focus on synchronising breach-reporting timelines, unifying consumer consent standards, and harmonising data processing obligations. Joint guidance notes and coordinated inspections are likely to reduce regulatory arbitrariness while simultaneously increasing the effective reach of enforcement actions.



— 3.3 Open Banking Implementation and Data Governance

With Open Banking transitioning from framework to live operation, 2026 will be a stress test for consent architecture, data minimisation, and third-party accountability. Key developments include enhanced participant accreditation requirements that tie Open Banking eligibility directly to demonstrable NDPA compliance.

Regulators will apply greater scrutiny to Application Programming Interfaces (APIs) and data-sharing protocols. There will also be a clearer legal allocation of liability between data controllers (banks) and processors (fintechs). Expect potential joint enforcement actions by the NDPC and CBN against aggregators that fail to maintain robust controls.

Key Implementation Milestones

- **Q1 2026**
Finalisation of joint supervisory frameworks with CBN and NCC.
- **Q2 2026**
Publication of unified consumer consent standards for telecom and fintech.
- **Q3 2026**
Launch of coordinated audit inspections for high-risk data processors.

Strategic Insight

"Organisations can no longer treat sectoral compliance and data protection as separate silos. The convergence of regulatory mandates requires a unified governance framework."

Business Impact Summary

- ✓ Reduced regulatory arbitrage opportunities.
- ✓ Streamlined reporting for multi-sector entities.
- ▲ Increased risk of cascading enforcement actions across regulators.

Open Banking Governance Flow



Legislative Outlook 2026

Navigating a landscape of active, uneven, and potentially overlapping statutory reforms.

Legislative activity in 2026 will remain heightened as the National Assembly targets the digital economy. While new bills aim to strengthen digital sovereignty and governance, the primary challenge for businesses will shift from a lack of regulation to navigating overlapping regulatory requirements across multiple frameworks.

4.1 NDPA Amendment Proposals

Primary Focus:

Regulation of foreign platforms and application developers.¹¹

Two proposed amendment bills are likely to advance, targeting foreign entities operating within Nigeria's digital space. Key provisions include:

Mandatory Registration

Enforced registration with the NDPC for all foreign platforms.

Standardised Consent Interfaces

Strict requirements for how consent is sought and obtained from Nigerian users.

Annual Impact Assessments

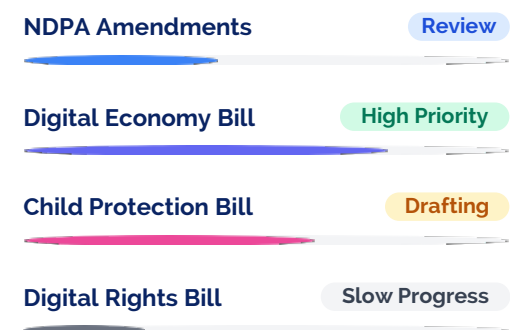
Compulsory submission of assessments detailing data processing risks.

App Removal Powers

Empowers the NDPC to recommend the removal of non-compliant applications from app stores.

Analysis: While ambitious, these obligations largely mirror existing requirements under the NDPA and GAID, raising valid concerns about legislative redundancy¹² and administrative inefficiency.

Legislative Roadmap



4.2 National Digital Economy & E-Governance Bill

This bill is expected to gain significant traction, effectively positioning the **National Information Technology Development Agency (NITDA)** as a digital-economy super-regulator.

AI Oversight

Explicit powers to govern Artificial Intelligence standards and deployment.

Bill Consolidation

Standalone AI bills may be consolidated under this framework or rendered redundant.

4.3 Cybersecurity & Digital Rights

Progress is anticipated on cybersecurity-specific legislation to bolster national resilience. Simultaneously, the **Digital Rights and Freedom Bill** will likely see renewed attention, focusing on civil liberties in the digital age.

4.4 Child Online Protection

Child safety will become a legislative priority. The **Child Online Access Protection Bill** is likely to be enacted, imposing strict age verification and duty-of-care obligations on platforms accessible to minors.

⚠ Strategic Risk Assessment

Overlapping Regulatory Requirements

For businesses, the primary risk in 2026 will not be the *absence* of regulation, but rather the friction caused by concurrent and potentially duplicative obligations across these emerging frameworks.

Recommendation

Adopt an integrated compliance strategy that maps data flows against multiple statutory regimes simultaneously.

Enforcement & Supervisory Trends

Enforcement in 2026 will be **risk-based, sector-targeted, and reputationally consequential**. The NDPC is shifting from broad awareness campaigns to precise regulatory interventions targeting high-impact data processors. The focus will be on tangible accountability, where non-compliance carries not just financial penalties but operational and reputational costs.

— 5.1 Priority Sectors

The Commission will prioritize enforcement actions based on the volume of data processed and the sensitivity of personal information. Key sectors under intensified scrutiny include:

Fintech & Digital Lending

Focus on aggressive data collection and unauthorized sharing for recovery.

Telecommunications

Scrutiny of subscriber data management and value-added service consent.

Adtech & Platforms

Investigation of profiling algorithms and real-time bidding compliance.

Large Data Processors

Organizations processing data of major importance (ODPMI) will face regular audits.

— 5.2 Enforcement Mechanisms

The NDPC will deploy a diversified toolkit to ensure compliance, moving beyond simple administrative fines:

📌 Public Accountability ("Naming and Shaming")

Continued use of public listings of non-compliant organizations to leverage reputational risk as a compliance driver.

🔍 Enhanced Investigatory Powers

Greater reliance on compulsory information requests and unannounced on-site inspections to verify compliance claims.

— 5.3 Sanctions Framework

The sanctions regime will expand beyond financial penalties to include **corrective orders** (mandating specific governance changes), **compliance undertakings** (legally binding agreements to remediate), and **operational restrictions** (limitations on data processing activities until compliance is achieved).

Operational
Restrictions

Corrective
Orders

Fines

📌 Expected Enforcement Policy Framework

The NDPC is expected to publish a formal enforcement policy in 2026 to clarify penalty assessments.

| Aggravating Factors

- ✗ Systemic governance failure
- ✗ Repeat offenses
- ✗ Financial gain from breach

| Mitigating Factors

- ✓ Self-reporting of breach
- ✓ Cooperation with investigation
- ✓ Remedial actions taken

| Strategic Goal

To introduce **proportionality** and **predictability** for regulated entities while preserving deterrence against willful non-compliance.

Market & Industry Impact

Convergence of data sovereignty, ESG imperatives, and AI governance reshaping the business landscape.

6.1 Data Sovereignty & Local Hosting

There is likely to be increased pressure on organisations to store and process certain categories of data within Nigeria only.¹³ This trend will be especially pronounced for sensitive data in sectors such as **finance, healthcare, and critical infrastructure**.¹⁴

Factors such as government procurement requirements, the use of tax incentives to encourage local investment, and broader national security considerations are expected to drive greater adoption of Nigerian-based data hosting and storage solutions. Multinational entities must re-evaluate their cloud architecture to ensure primary copies of critical national data reside within Nigerian borders.

2 Strategic Implications

Local Infrastructure Budget for local data center migration for critical workloads.

Investor Readiness Conduct pre-audit privacy gap analyses before funding rounds.

AI Documentation Maintain explainability logs for all automated decision systems.

6.2 ESG & Corporate Governance Convergence

Data protection is increasingly being viewed not just as a legal compliance matter, but as a core **Environmental, Social, and Governance (ESG)** and enterprise-risk issue. It is projected that investors, lenders, and auditors will now expect organisations to show clear and effective privacy governance.

Consequently, data protection metrics will become an important consideration in capital-raising activities, audits, and due-diligence processes. Companies with poor data hygiene will face higher costs of capital and exclusion from premium investment tiers.

Market & Industry Impact

Fig 6.1: Sovereignty Drivers



Fig 6.2: The ESG Nexus

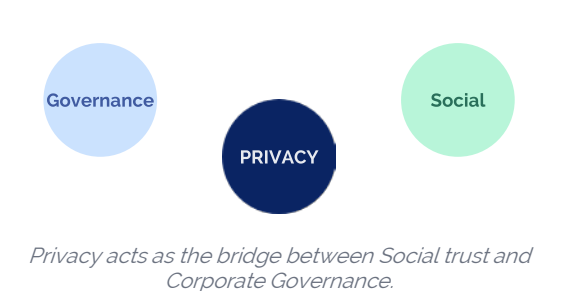


Fig 6.4: AI Oversight

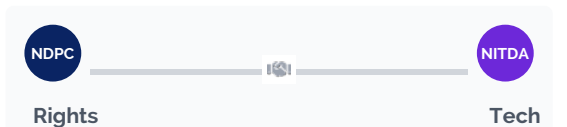


Fig 6.5: Sector Impact Intensity



6.3 Platform Economies & Consent Models

Stricter consent rules are continuing to change how digital advertising works.¹⁵ Businesses that rely on unclear or implied consent, especially for user profiling and targeted advertising, will need to rethink how they collect data, design user journeys, and generate revenue.

Operational Shift: Without explicit opt-in mechanisms, businesses face ongoing regulatory scrutiny and enforcement risk. The "pay-or-consent" models seen in other jurisdictions may begin to emerge in the Nigerian market.

6.4 AI & Emerging Technologies

Data protection will become a central pillar of AI governance in 2026. A key development will be the operationalisation of a **dual-regulatory environment**:

- ✓ **NDPC:** Oversees lawful processing of personal data in AI systems.
- ✓ **NITDA:** Shapes broader AI governance, standards, and innovation frameworks.

We anticipate AI risk-classification frameworks where higher-risk applications (finance, healthcare) attract stricter transparency and human oversight obligations.

Litigation & Dispute Trends

In 2026, data protection is likely to become a more active and contested area of litigation. Following a year where the Court delivered more than **5 significant judgments** on data protection—with several cases still pending determination—Courts will increasingly be called upon to interpret obligations, assess compliance failures, and determine substantive issues such as lawful processing, consent, proportionality, and accountability.

7.1 Emerging Judicial Precedents

A key driver of the litigation trend will be the emergence of successful judicial precedents. Once courts begin awarding damages or granting relief in data protection cases—as seen in the 2025 judgments awarding millions in damages for data mismanagement—similar claims are likely to follow.

"The affirmation that economic loss flowing from data misuse is actionable creates a tangible financial risk for controllers."

7.2 Litigation Drivers

Individuals and advocacy groups will be encouraged by early successes, leading to **copycat litigation** against both public institutions and private companies that process personal data at scale. The clarification that aggrieved data subjects may approach the courts directly, without first petitioning the NDPC, removes procedural bottlenecks and accelerates the pace of filings.

7.3 Exposure Areas

Organizations should expect higher exposure to damages and more frequent disputes. Data protection is becoming a routine feature across various legal domains:

Commercial Litigation

Breach of contract involving data clauses.

Employment Disputes

Employee surveillance and data rights.

Consumer Protection

Unsolicited marketing and profiling.

Public Law

Challenges to state data collection.

Litigation Volume Projection

Based on 2024-2025 filing trends

Litigation Risk Mitigation

Those that invest early in defensible compliance practices will be better positioned to manage this evolving landscape.

Immediate Action

Audit all consent collection mechanisms.

Documentation

Ensure ROPAs are litigation-ready.

Training

Train staff on data subject rights handling.

7.4 Organizational Readiness Framework

To reduce the risk of adverse judicial outcomes, organizations must evidence the following controls:

Robust data governance framework

Defensible compliance practices

Data Protection Impact Assessments (DPIA)

Executed Processor Contracts

Clear & accessible documentation

Records of Processing Activities (ROPA)

Verifiable Consent Records

Tested Incident Response Plans

Litigation Risk Exposure

HIGH EXPOSURE

International Data Transfers & Global Integration

2026 is poised to be the year Nigeria fully operationalises international transfer mechanisms. Moving beyond theoretical frameworks, the NDPC will introduce definitive tools that provide legal certainty for cross-border data flows, integrating Nigerian businesses more deeply into the global digital economy.

— 8.1 Transfer Tools Under the NDPA

The uncertainty surrounding lawful cross-border transfers will be addressed through the issuance of definitive guidance and standardised instruments.

Standard Contractual Clauses (SCCs)

Formal issuance of NDPC-approved SCC templates, eliminating the need for ad-hoc contract drafting for international transfers.

Adequacy Framework

Establishment of a clear whitelist of jurisdictions with adequate data protection laws, streamlining transfers to key trading partners.

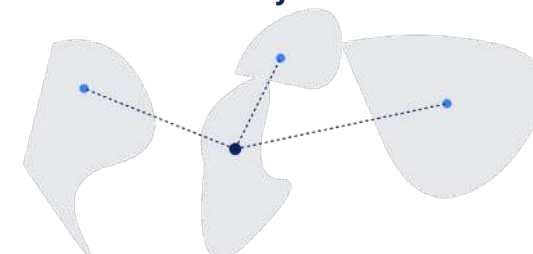
Binding Corporate Rules (BCRs)

Framework for multinational groups to approve intra-group transfers through a single regulatory approval process.

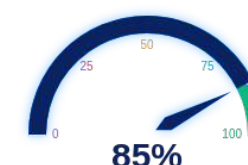
Transfer Mechanism Hierarchy



Global Connectivity



Legal Certainty Index



Implementation Guidance

Audit Data Flows

Map all cross-border transfers and identify the legal basis currently used.

Update Contracts

Prepare to migrate existing agreements to the new NDPC Standard Contractual Clauses.

Assess Certification

Evaluate if CBPR certification offers a competitive advantage for your export markets.

— 8.2 Global CBPR Forum Integration

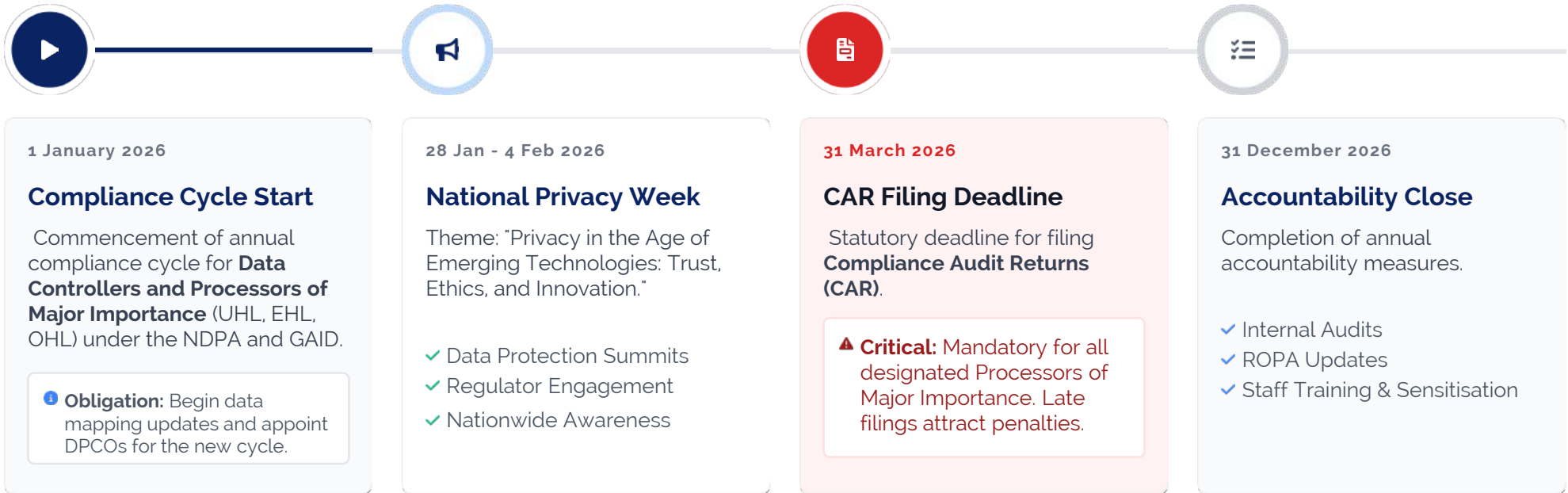


Nigeria's associate membership in the **Global Cross-Border Privacy Rules (CBPR) Forum** signals a strategic pivot beyond GDPR-centric models. In 2026, we expect the licensing of local certification bodies, creating a pathway for Nigerian companies to obtain CBPR certification. This will facilitate seamless data flows with Asia-Pacific and American markets, enhancing interoperability.

— 8.3 Business Impact & Certainty

The operationalisation of these tools will significantly reduce legal friction for cross-border trade. For data controllers and processors, this means clearer compliance playbooks and reduced liability risks when engaging international partners.

Nigeria Data Protection Calendar 2026



Section 10 Final Assessment

Conclusion

After years of regulatory milestones, Nigeria's data protection system is largely ripe for implementation and enforcement. Without a doubt, businesses operating in Nigeria have no excuse for not being fully compliant with data protection laws and best practices. From both a judicial and regulatory perspective, it is no longer tenable for businesses to be more reactive than proactive in their data protection compliance.

It is now essential that data protection be embedded efficiently and effectively across governance structures, product design, procurement, cross-border operations, and risk management processes.¹⁷ In particular, as the digital economy continues to grow as it has for the last decade, the trust value of effective data protection compliance cannot be overstated.

"For regulators, 2026 will mark the continued implementation of regulations that have been developing since 2019. For businesses, it will be essential to define their data protection compliance strategies based on their size and business operations."

Strategic Imperatives for 2026

- Embed Compliance Early**
 Integrate privacy-by-design into all product development cycles and procurement processes.
- Conduct Gap Assessments**
 Review current practices against GAID requirements and sector-specific codes immediately.
- Invest in Documentation**
 Ensure ROPAs, DPIAs, and transfer impact assessments are audit-ready at all times.
- Prepare for Coordination**
 Anticipate joint enforcement actions from NDPC and sectoral regulators like CBN/NCC.

Action Required

Endnote

1. Nigeria Data Protection Commission (NDPC), List of Defaulters under the Nigeria Data Protection Act 2023. Published in BusinessDay Newspaper, 25 August 2025, Lagos
2. Nigeria Data Protection Commission, National Digital Economy Policy and Strategy https://ndpc.gov.ng/resources/#flipbook-df_2446/1/ accessed January 3, 2026
3. Judgment on Registration as a Data Controller (Scribd, Federal High Court of Nigeria, Kaduna Judicial Division, Suit No. FHCKD/CS/34/2024,(Unreported) 22 Nov. 2024) <https://www.scribd.com/document/802356606/Judgment-on-Registration-as-a-Data-Controller> accessed January 3, 2026
4. Businessday, 'NDPC fines MultiChoice N766m for privacy violation' <https://businessday.ng/technology/article/ndpc-fines-multichoice-n766m-for-privacy-violation/> accessed January 3, 2026
5. Businessday 'Meta, NDPC resolve \$32.8m privacy dispute out of court' <https://businessday.ng/news/article/meta-ndpc-resolve-32-8m-privacy-dispute-out-of-court/> accessed January 3, 2026
6. The Nation "NDPC investigates data breach in JAMB" <https://thenationonline.ng.net/ndpc-investigates-data-breach-in-jamb/> accessed January 3, 2026
7. Rebecca Bonje v. GTBank (Unreported) Suit No. LD/18590MFHR/2024
8. Businessday "Inaccurate or misleading financial records by banks constitute a breach of customers' data privacy rights" <https://businessday.ng/news/legal-business/article/inaccurate-or-misleading-financial-records-by-banks-constitute-a-breach-of-customers-data-privacy-rights/> accessed January 3, 2026
9. Chukwunweike Araka Akosa v. ECART Internet Serviced Nigeria Limited and Anor. (Unreported) FHC/ABJ/CS/79/2024
10. Iyanuoluwa Afolabi v United Bank for Africa .(Unreported) Suit No: FHC/L/CS/2624/23
11. News Agency of Nigeria, Data Protection Amendment Bill Meant To Protect Nigerians (online), 21 March 2025 <https://nannews.ng/2025/03/21/data-protection-amendment-bill-meant-to-protect-nigerians-nwoko/> accessed January 3, 2026
12. Ibid
13. CYFIRMA, Cyber Threat Assessment on Nigeria (online, published 30 September 2025) <https://www.cyfirma.com/research/cyber-threat-assessment-on-nigeria/> accessed January 3, 2025.
14. Ibid
15. Katrina Toyer, Privacy Concerns in Digital Advertising: Navigating Challenges in 2025 (Postmedia Solutions, 19 February 2025) <https://www.postmediasolutions.com/en-ca/blog/privacy-concerns-in-digital-advertising-navigating-challenges-in-2025> accessed on January 4, 2026
16. CYFIRMA Digital / Nemko Digital, AI Regulation in Nigeria: The Evolving Legal Landscape (online) <https://digital.nemko.com/regulations/ai-regulation-in-nigeria> accessed January 3, 2026.
17. The Year of the Teeth: Data Protection in Africa Roundup, 2025, Projections for 2026 (Digital Policy Alert, 11 January 2026) <https://digitalpolicyalert.org/blog/data-protection-in-africa-roundup> accessed 13 January 2026



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

