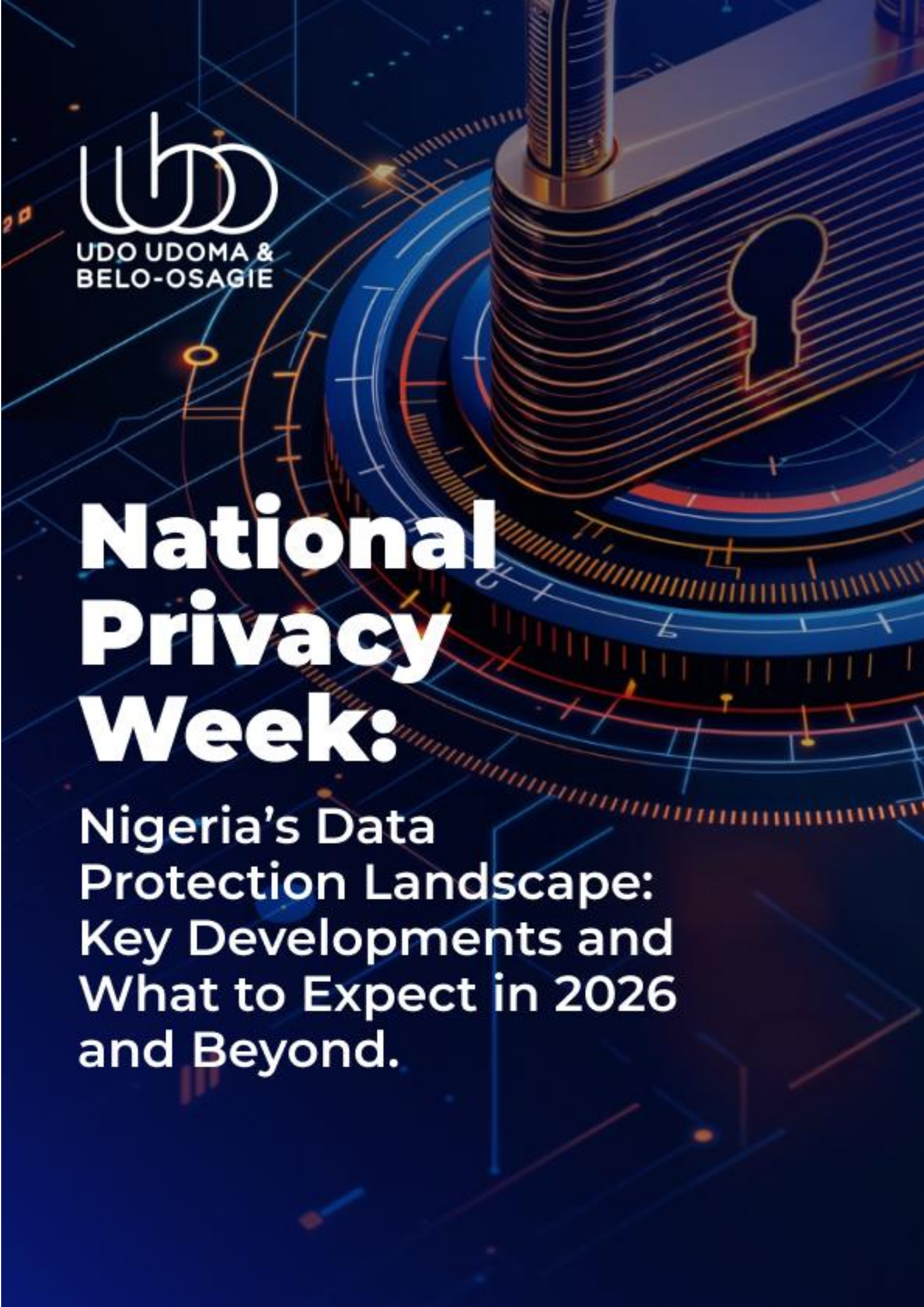

UDO UDOMA & BELO-OSAGIE

National Privacy Week:

Nigeria's Data Protection Landscape: Key Developments and What to Expect in 2026 and Beyond.

Introduction

Since the inception of the Nigeria Data Protection Regulation in 2019 (“the NDPR”), the first principal regulation on data protection in Nigeria, by the National Information Technology Development Agency (“NITDA”), the data protection landscape has been significantly transformed. Data protection has evolved from an issue that received limited attention into one of growing importance for regulators, data subjects, processors, and organisations.

As businesses scale through the application of technological advancements, which places an increasing reliance on data-driven business decisions, the processing of personal data has become an important consideration for stakeholders such as regulators, businesses (data controllers and processors), and data subjects. What began as a framework-building phase, in which organisations were largely encouraged to adopt basic data protection practices, is now firmly embedded in Nigeria’s legal and regulatory landscape.

Regulatory expectations are clearer, compliance obligations are more defined, and organisations are increasingly being assessed on how their data protection systems and processes are being implemented in practice and not relying solely on documentation. This article reviews the evolution of the data protection landscape in Nigeria from 2019 to date and considers what organisations should expect in 2026 and beyond as the sector continues to mature.

Evolution of Data Protection Regulation in Nigeria

Nigeria’s data protection regime started with the introduction of the NDPR, which defined what data protection meant in the Nigerian context and established baseline compliance obligations. The NITDA drove awareness across organisations. Compliance during this period was largely procedural, with an emphasis on policy adoption and regulatory familiarisation, as the NITDA prioritised awareness and voluntary compliance over enforcement.

The NDPR Implementation Framework was issued by the NITDA in 2020 to support the effective implementation of the NDPR. While the NDPR established high-level data protection principles and obligations, it left several areas open to interpretation. The Implementation Framework was, therefore, seen as a necessary tool to provide practical guidance to organisations and clarify how they were expected to comply with the NDPR. The Framework was widely relied upon by regulators, organisations,

and other stakeholders prior to the enactment of a substantive data protection legislation.

Recognising the need for a stronger legal framework that aligned with global standards such as the GDPR, the Nigeria Data Protection Act ("NDPA") was enacted on 12 June 2023 to give statutory force to data protection regulation in Nigeria. The enactment of the NDPA marked a clear regulatory shift, providing a statutory basis for data protection and establishing the Nigeria Data Protection Commission ("NDPC") as the data protection regulatory authority in Nigeria.

The NDPA sets clear rules on how personal information should be handled and makes data controllers and processors responsible for compliance. Key pillars of the NDPA include transparency, data security, and the enforcement of data subjects' rights. Furthermore, the NDPA introduces robust cross-border transfer mechanisms and significant administrative sanctions to ensure compliance and accountability.

The NDPA has clearly strengthened regulatory oversight, moving Nigeria toward a culture of enforceable obligations. The NDPC's track record of investigating and imposing sanctions on non-compliant organisations since its inception, is a clear demonstration of the importance of data protection and privacy compliance to Nigeria and the NDPC will take every action to ensure the safety of the personal data of data subjects who are within the ambit of the NDPA's protection.

A major development in Nigeria's data protection regime in 2025 was the issuance of the General Application and Implementation Directive (GAID) by the Nigeria Data Protection Commission (NDPC) on 20 March 2025. The GAID came into effect on 19 September 2025, and it serves as the principal instrument for the implementation of the NDPA. Compliance under the NDPA will now be assessed in accordance with both the Act and the GAID.

The GAID replaces the NDPR and NDPR Implementation Framework, and compliance is no longer evaluated against the broad principles set out in those regulations and guidance rules but against the specific, mandatory obligations defined in the GAID. The GAID sets out detailed requirements on data governance, including the identification and mapping of processing activities, lawful bases for processing, content of privacy and cookie notices, and the standards applied by the NDPC during audits and investigations.

Operationally, the GAID reinforces structured compliance mechanisms, including mandatory Compliance Audit Returns (CARs) for Data Controllers and Data Processors of Major Importance (DCPMIs), 72-hour data breach notification,

compulsory Data Protection Impact Assessments (DPIAs) for high-risk processing activities, and prescribes minimum requirements for data processing agreements. It also formalises internal governance measures, including the appointment of qualified Data Protection Officers (DPOs), semi-annual internal data protection reports, organisation-wide training schedules, and ongoing monitoring and maintenance of data security systems.

An important feature of the GAID is its emphasis on verifiable continuous compliance. The requirement for semi-annual DP reports and verifiable documentation is designed to ensure ongoing risk assessment and management rather than reactive compliance triggered by regulatory scrutiny.

While the NDPC is still keen on increasing data protection awareness, it has started to take the enforcement of data breaches very seriously. In 2025, the NDPC launched sector-wide enforcement actions across multiple industries, and imposed administrative penalties, sometimes quite significant fines, on organisations that were found to be non-compliant. These actions signal a decisive shift from encouraging compliance to active enforcement.

The NDPA and the GAID require organisations to reassess their roles as data controllers, processors, or both, with direct consequences for registration, audit, and reporting obligations. Greater accountability now applies to the engagement and oversight of third-party processors, and responsibility for data protection compliance now sits squarely with senior management and the board. With enforcement now firmly established, non-compliance carries not just material financial penalties, but operational and reputational risks.

What to Expect in 2026 and Beyond: Enforcement Outlook

Looking ahead to 2026 and beyond, regulatory attention is expected to focus on the continuation and intensification of the NDPC's investigations initiated in 2025. Organisations previously scrutinised or investigated during the 2025 enforcement cycle are likely to be required to demonstrate ongoing compliance through verifiable documentation and processes. The NDPC is expected to place particular emphasis on practical compliance with the GAID, including governance, audit, registration and reporting obligations. Increased scrutiny is also anticipated regarding semi-annual data protection reports, cross-border data transfer arrangements, and the qualifications and certifications of appointed DPOs. The GAID's requirements signal a clear expectation that DPOs possess demonstrable data protection expertise, marking a departure from the appointment of any officer in the organisation to a

specific person who has received training from recognised bodies on data protection. High-risk processing activities and large-scale data operations are also likely to remain under close regulatory scrutiny, particularly for organisations that process significant volumes of personal data.

Strategic Considerations

As organisations plan for 2026, data protection compliance matters must move beyond baseline requirements to focus on effective implementation. This requires a thorough review of the GAID, consideration of enforcement trends from 2025, and the strengthening of internal controls, reporting structures, and accountability mechanisms. Key focus areas include audit readiness, cross-border data transfer arrangements, DPO capacity building and certification, and the depth of internal monitoring and documentation. A proactive compliance strategy supported by early engagement with experienced Data Protection Compliance Organisations (DPCOs) is critical. Beyond the risk of administrative penalties of up to 2% of annual gross revenue for DCPMIs, enforcement actions carry significant reputational risks. In many cases, the resulting loss of trust, heightened regulatory scrutiny, and public exposure may be more damaging than the financial penalties.

Conclusion

As Nigeria marks the 2026 Privacy Week, the evolution of the data protection landscape underscores a clear regulatory message: privacy compliance is no longer aspirational or reactive, but a core governance obligation. The NDPA and the GAID have firmly shifted the regime towards structured, verifiable accountability, supported by active enforcement and heightened regulatory scrutiny.

For organisations, the challenge and opportunity lie in embedding data protection into everyday operations, decision-making, and risk management frameworks. Those that invest early in robust governance structures, qualified data protection leadership, and continuous compliance monitoring will be better positioned to navigate regulatory expectations, maintain stakeholder trust, and mitigate both legal and reputational risk.

Privacy Week, therefore, serves not only as a moment of reflection but as a call to action: to move beyond formal compliance and to treat the protection of personal data as a fundamental element of responsible, sustainable business in Nigeria’s digital economy.

Udo Udoma & Belo-Osagie is a licensed Data Protection Compliance Organisation (DPCO) with extensive experience advising organisations across sectors on their compliance obligations under the NDPA and the GAID. We conduct annual audits, assist with regulatory investigations, and the design of practical data protection governance frameworks. If you have any questions regarding your compliance status under the NDPA or the GAID, or require support with data protection compliance, please contact us at **dpteam@uubo.org**.
