G R C K L T D

Cybersecurity · Data Privacy · Data Governance · AI Readiness · AI Governance

ADVISORY GUIDE

NDPA vs GDPR:

Navigating Dual Compliance Requirements

Published by GRCK Ltd · Advisory in Cybersecurity, Data Privacy, Data Governance, AI Readiness & AI Governance

February 2026 | www.grckco.com

EXECUTIVE SUMMARY

For organisations operating across Nigerian and European markets, or processing the personal data of citizens in both jurisdictions, the regulatory landscape has become significantly more complex. Nigeria's data protection framework is now primarily governed by the **Nigeria Data Protection Act (NDPA) of 2023**, which supersedes the earlier Nigeria Data Protection Regulation (NDPR) of 2019. The NDPR was the founding instrument but has been legislatively replaced by the NDPA, which substantially elevated Nigeria's data protection standards and established an independent supervisory authority. Together with the European Union's General Data Protection Regulation (GDPR), which came into force in 2018, these represent two of the most consequential data privacy frameworks in their respective geographies. While they share a philosophical commitment to individual data rights, they differ substantially in scope, enforcement mechanisms, technical requirements, and organisational obligations. This article provides a structured comparison and a practical framework for organisations that must satisfy both regimes simultaneously.

1. The Regulatory Landscape: Origins and Objectives

1.1 The NDPA: Nigeria's Data Protection Framework

Nigeria's data protection framework has evolved rapidly. The Nigeria Data Protection Regulation (NDPR), issued by the National Information Technology Development Agency (NITDA) in January 2019, was a landmark instrument — the first comprehensive data protection regulation for Africa's most populous nation and largest economy. It established core principles of lawful processing, data subject rights, and mandatory breach notification, drawing conceptually from international best practices including the GDPR. However, **the NDPR has since been superseded by the Nigeria Data Protection Act (NDPA) of 2023**, which is now the primary operative law governing data protection in Nigeria.

The Nigeria Data Protection Act of 2023 significantly elevated the framework established by its predecessor, establishing the **Nigeria Data Protection Commission (NDPC)** as an independent supervisory authority, codifying data subject rights with greater specificity, and introducing stronger enforcement powers including the ability to impose administrative fines. The NDPA represents Nigeria's signal to international investors and trading partners that its data governance architecture meets globally recognised standards — a necessary precondition for data transfers with GDPR-regulated entities. Where reference to the NDPR appears in older contracts, policies or literature, organisations should treat the NDPA as the governing instrument.

1.2 The GDPR: Europe's Gold Standard

The GDPR, which replaced the 1995 Data Protection Directive, applies across all 27 EU member states and, critically, extends extraterritorially to any organisation, regardless of where it is established, that processes the personal data of EU data subjects in connection with offering goods or services, or monitoring their behaviour. This extraterritorial reach means that Nigerian businesses with EU customers, European operations, or digital services accessible to EU users are likely subject to GDPR obligations regardless of their headquarters jurisdiction.

Enforced by 27 national supervisory authorities coordinated through the European Data Protection Board (EDPB), the GDPR carries some of the heaviest penalties in global data regulation: fines of up to €20 million or 4% of global annual turnover, whichever is higher. The GDPR has set the global benchmark against which all other data protection frameworks are assessed — including, increasingly, the NDPA.

2. Side-by-Side Comparison: Key Provisions

The table below summarises the principal dimensions across which the two frameworks align, diverge, and interact. Understanding these differences is the first step towards building a coherent dual-compliance programme.

Dimension	NDPA (Nigeria)	GDPR (EU)
Governing Authority	Nigeria Data Protection Commission (NDPC)	National supervisory authorities (27) + European Data Protection Board (EDPB)
Territorial Scope	Applies to processing of personal data of Nigerian residents; extraterritorial reach strengthened under the NDPA	Extraterritorial: any organisation processing EU data subjects' data, regardless of location
Legal Bases for Processing	Consent, contract, legal obligation, legitimate interest, vital interests, public interest	Same six bases; legitimate interest requires a Legitimate Interests Assessment (LIA) with EDPB guidance
Data Subject Rights	Access, rectification, erasure, objection, portability (codified and strengthened under NDPA)	Access, rectification, erasure, restriction, portability, objection, automated decision-making rights
Breach Notification	72 hours to NDPC; notice to data subjects where high risk	72 hours to supervisory authority; without undue delay to data subjects where high risk
Data Protection Officer	Required for certain categories under the NDPA	Mandatory for public bodies, large-scale sensitive processing, systematic monitoring
Cross-Border Transfers	Permitted with adequate safeguards; adequacy decisions possible under NDPA framework	Adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), derogations
DPIAs	Required under NDPA for high-risk processing	Mandatory for high-risk processing; EDPB guidance defines specific trigger scenarios
Penalties	Up to 2% of annual gross revenue (NDPA)	Up to €20m or 4% of global annual turnover for serious infringements

Dimension	NDPA (Nigeria)	GDPR (EU)
Audit / Compliance Filing	Annual data protection audit required; licensed DPCO must be engaged above processing thresholds	No mandatory annual audit; accountability demonstrated through records, DPIAs, and policies on demand

> *"Dual compliance is not about maintaining two separate programmes — it is about designing a unified framework sophisticated enough to satisfy the higher standard in every material dimension."*

3. Where the Frameworks Diverge: High-Stakes Differences

3.1 The Annual Audit Obligation

One of the most significant differences for organisations new to NDPA compliance is the annual audit requirement — a feature carried forward and formalised from the earlier NDPR regime. Organisations that process personal data of more than 1,000 data subjects annually must conduct a Data Protection Audit and file a summary with the NDPC through a licensed Data Protection Compliance Organisation (DPCO). The GDPR imposes no equivalent periodic filing obligation; instead, it requires ongoing accountability through documentation, records of processing activities, and policies that can be produced on demand by a supervisory authority.

For dual-compliance organisations, the NDPA audit cycle creates a structured annual checkpoint that, if well-designed, can also serve as a health-check against GDPR requirements. Leading practice is to align the NDPA audit cycle with an internal GDPR compliance review, treating both as components of a unified annual privacy programme.

3.2 Cross-Border Data Transfers

The treatment of cross-border data transfers is an area of growing complexity for organisations operating between Nigeria and the EU. The GDPR is highly prescriptive: transfers outside the European Economic Area require either an adequacy decision, Standard Contractual Clauses, Binding Corporate Rules, or one of a limited set of derogations. Nigeria has not yet received an EU adequacy decision, meaning transfers of EU personal data to Nigerian entities must be covered by appropriate safeguard mechanisms — most commonly SCCs incorporated into data processing agreements.

From the Nigerian side, the NDPA permits cross-border transfers where the receiving country provides adequate data protection or where appropriate contractual safeguards are in place. Organisations must map their data flows carefully and ensure each transfer is covered by a lawful mechanism under both regimes simultaneously — a task requiring careful legal analysis and ongoing maintenance as data flows evolve.

3.3 Consent Standards

Both frameworks require consent to be freely given, specific, informed, and unambiguous. The GDPR adds a requirement that consent be as easy to withdraw as to give and has generated extensive supervisory authority guidance on valid consent in specific contexts including cookie banners, employment relationships, and children's data. For dual-compliance purposes, applying the higher GDPR consent standard across all processing activities is generally the safest approach, reducing the risk of inadvertent non-compliance and simplifying governance by avoiding jurisdiction-specific consent mechanisms for overlapping data sets.

3.4 Enforcement Posture and Risk Calibration

The GDPR's enforcement record is extensive and well-publicised, with fines totalling several billion euros since 2018. The NDPC is a newer institution with a developing enforcement track record, but early signals suggest an increasingly assertive posture. Organisations should not assume NDPC enforcement risk is materially lower than GDPR risk. The reputational, commercial, and operational costs of a data protection enforcement action, regardless of jurisdiction, are substantial, and the trend across African data protection authorities is towards greater capacity and willingness to act.

4. Building a Dual-Compliance Programme: A Practical Framework

4.1 Step One: Data Mapping and Flow Analysis

No compliance programme can be designed without a clear picture of what personal data the organisation holds, how it was collected, where it is stored, how it is used, who has access, and where it flows — both internally and externally. For dual-compliance purposes, data mapping must explicitly identify the jurisdictional nexus of each data set: is this the data of Nigerian residents, EU data subjects, or both? Does it flow across borders, and if so, under what legal mechanism? The output is a Record of Processing Activities (RoPA) that documents each processing activity with sufficient granularity to demonstrate compliance with both frameworks.

4.2 Step Two: Gap Analysis Against Both Frameworks

A structured gap analysis should assess the organisation's current policies, procedures, technical controls, and governance arrangements against the requirements of both the NDPA and the GDPR. Areas to examine include: lawful basis documentation; data subject rights procedures; breach notification processes; data processing agreements; privacy notices; consent mechanisms; data retention schedules; and cross-border transfer safeguards. Gaps should be prioritised by risk and assigned to remediation workstreams with clear ownership and timelines.

4.3 Step Three: Policy and Governance Alignment

Dual-compliance organisations should operate a single, unified privacy governance framework — not parallel NDPA and GDPR programmes. This means a single Privacy Policy addressing the requirements of both frameworks; unified data subject rights procedures capable of responding within applicable timeframes under either regime; a single Data Protection Officer or equivalent role with cross-framework responsibility; and a unified incident response and breach notification procedure that satisfies the 72-hour reporting requirement of both regimes.

4.4 Step Four: Third-Party and Vendor Management

Under both the NDPA and the GDPR, organisations retain responsibility for the personal data they share with processors and sub-processors. Data Processing Agreements must be in place with all third parties processing personal data on the organisation's behalf, and those agreements must address the requirements of both frameworks — including security obligations, breach notification timelines, sub-processing restrictions, and data transfer mechanisms. For organisations engaged in Nigeria-EU business, vendor contract templates should incorporate GDPR-compliant SCCs for any transfers of EU personal data to Nigerian processors.

4.5 Step Five: Training, Awareness and Culture

Technical and legal compliance without cultural embedding is fragile. Staff at all levels must understand their obligations under both frameworks as practical behavioural expectations, not abstract legal requirements. Annual training is a minimum; organisations with significant data processing operations should invest in role-specific training, privacy champions programmes, and regular communications. This is particularly important where staff operate across Nigerian and European markets and may encounter data subjects and regulatory expectations from both jurisdictions.

> *"The organisations that manage dual compliance most effectively treat it as a business capability — building privacy into their products, processes and culture from the ground up."*

5. Emerging Intersections: AI, Data Governance and the Road Ahead

The intersection of AI adoption with data protection compliance adds a further layer of complexity for organisations navigating both the NDPA and the GDPR. AI systems are data-intensive by nature: they are trained on personal data, they may generate outputs that constitute personal data, and they are increasingly used to make or inform decisions with significant consequences for individuals. Both the NDPA and the GDPR impose obligations applicable to automated processing and profiling, and the EU's AI Act — now entering force — adds a further compliance layer for AI systems used in connection with EU data subjects.

For organisations with AI readiness and AI governance on their agenda, embedding data protection compliance into the AI development and deployment lifecycle is both a legal necessity and a business imperative. Data Protection Impact Assessments are required under both frameworks for high-risk AI processing. AI-specific provisions on transparency, explainability, and the right not to be subject to solely automated decisions create obligations that must be designed into AI systems from the outset — not retrofitted after deployment. Organisations that have invested in robust data governance — clear data ownership, quality standards, retention schedules, access controls, and lineage tracking — are best positioned to demonstrate compliance with both data protection and AI-specific regulatory requirements.

6. Conclusion

The NDPA and GDPR share a common philosophical core — the protection of individuals' rights in relation to their personal data — but they differ in ways that matter for organisations operating across both jurisdictions. The NDPA's enactment in 2023 represented a decisive step forward for Nigerian data protection, superseding the NDPR and establishing a more robust, independently enforced framework. Navigating the differences between the NDPA and GDPR requires more than a compliance checklist; it requires a strategic, integrated approach to privacy governance that treats data protection as a business capability, aligns policy and process across jurisdictions, and embeds compliance into the organisation's culture and technology architecture.

The regulatory landscape will continue to evolve. The NDPC is building enforcement capacity and publishing additional guidance. The GDPR is subject to ongoing interpretation by the EDPB. The EU AI Act is creating new obligations that intersect with data protection requirements. Organisations that build adaptive, well-governed compliance programmes today will be better positioned to absorb these changes without disruption — and to demonstrate to their customers, partners, and regulators that they take the protection of personal data seriously.

Have Questions Navigating NDPA & GDPR?

GRCK Ltd

We are a specialist advisory firm with deep expertise in Cybersecurity · Data Privacy · Data Governance · AI Readiness · AI Governance. Whether you are building a dual-compliance programme from scratch, conducting a gap analysis, preparing for a regulatory audit, or embedding privacy into your AI systems, our team has the knowledge and experience to guide you.

Get in touch: www.grckco.com | info@grckco.com

Your data. Your compliance. Our expertise.