The NDPC's New Circular on Data Protection and Responsible Data Governance: Key Considerations for Ministries, Departments, Agencies "MDAs"

Regulatory Update

Introduction

On August 4, 2026, the Nigeria Data Protection Commission ("NDPC") published a press release announcing the Federal Government's commitment to mandating data compliance across public institutions. The Press release highlighted the issuance of a compliance circular ("Circular No. 59805/S.I/7) directed to Ministries, Departments, and Agencies ("MDAs") by the Federal Government to promote public trust and strengthen data governance across public institutions.[1] The underlying Circular invokes the Federal Government's directive that all MDAs should "capture information rigorously and safeguard it under the Nigeria Data Protection Act 2023" ("NDP Act").[2]

Significance of the Circular

Elevated to the highest levels of government

It elevates data protection from a simple compliance issue to a priority at the highest levels of government.

Personal accountability of leadership

It mandates that Permanent Secretaries, Accounting Officers, and Chief Executive Officers are personally responsible for institutional compliance.

Commercial Reach beyond government

There are commercial implications not just for the MDAs of government but also for private entities, such as data processors, that process personal data on behalf of government institutions.

In light of the above, this insight sets out the Circular's principal requirements, examines the implications for MDAs, and identifies practical challenges that may arise from the FG's renewed focus on data protection.

What MDAs are Required to Do

The Circular directs MDAs to ensure "full compliance with the NDP Act, Regulations, Guidelines and Directives issued by the NDPC in relation to the processing of personal data." To this end, the Circular imposes the following obligations:

01 · Appoint

Appointment of Data Protection Officers:

MDAs must designate qualified officers as Data Protection Officers (DPOs) to oversee data protection compliance and advise management on all matters relating to the lawful processing of personal data.

02 · Register

Registration of DPOs with NDPC:

MDAs are required to communicate the names and contact details of their designated DPOs to the NDPC for registration and official records. This creates an accountability link between each institution and the regulator.

03 · Engage

Engagement of licensed Data Protection Compliance Organisations:

MDAs may also engage the services of licensed Data Protection Compliance Organisations ("DPCOs") to facilitate compliance with the NDP Act and to support statutory compliance audits.

04 · Budget

Budgetary Allocation for Data Protection:

MDAs are required to allocate adequate budget for data protection compliance activities, including capacity building, awareness programmes, deployment of appropriate technical safeguards, and compliance audits.

05 · Submit

Submission of mandatory audit returns:

MDAs must submit all mandatory Data Protection Compliance Audit Returns (CAR) not later than March 31st of each year.[3] and other Statutory returns to the NDPC within timelines prescribed by law.

06 · Personalise

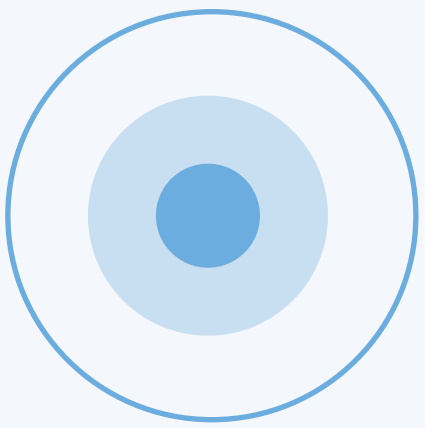
Personal accountability of leadership:

The Circular states that Permanent Secretaries, Accounting Officers, and Chief Executive Officers of all MDAs "shall be personally responsible for ensuring institutional compliance with the Circular and the provisions of the NDP Act.

NDPC support

A regulatory clinic for MDAs

Additionally, the NDPC confirmed that the Commission has established a regulatory clinic to provide technical support to MDAs to achieve compliance.



Implications for MDAs and the Private Sector Entities Contracting with MDAs

MDAs will need to undertake a range of activities to ensure compliance with the circular. These include identifying data-processing activities across departments and appointing qualified, experienced DPOs. MDAs will also be required to establish internal data-protection policies and operational procedures, and budget for staff training and awareness programmes. Where internal capacity is limited, MDAs will need to engage licensed DPCOs, prepare and submit data-compliance audit returns, and strengthen internal frameworks to address data-protection risks in third-party arrangements. Overall, for MDAs, this means stronger internal accountability, documentation, oversight and budgeting.

The implications of the Circular may extend well beyond the public sector. This means MDAs must require private contractors, technology vendors, cloud service providers engaged by them, and other private entities that may process data on their behalf to comply with data protection obligations under the NDP Act.

To address these risks, MDAs should incorporate appropriate data protection safeguards into their engagements with such third parties, including entering into data processing agreements, clearly defining the parties' respective data protection responsibilities, conducting Data Protection Impact Assessments (DPIAs) where required, and implementing appropriate technical and organisational measures to protect personal data. MDAs should also establish mechanisms to monitor third-party compliance and manage data breaches and other data protection incidents throughout the engagement.

These entities should anticipate heightened due diligence requirements in their procurement processes.[4] Data processing agreements would need to reflect the requirements of the NDP Act; there would also be audit requirements and rights of inspection by MDAs or their licensed DPCOs; and higher standards for documentation and record-keeping.

For vendors and service providers already engaged with MDAs, there may be a need to revise or supplement [RPC3.1]existing data processing agreements to incorporate additional data protection obligations. In particular, where these engagements involve the processing of personal data on behalf of MDAs, the parties may need to update their agreements to clearly set out their respective obligations under the NDP Act. This may include provisions on data security, audit and inspection rights, record-keeping, and the handling of data breaches and other data protection incidents.

Overall, for private-sector entities dealing with MDAs, it means greater scrutiny of their data-protection practices, contractual obligations and ability to safeguard government-held personal data. Businesses with demonstrable data-protection compliance may be better positioned to participate in government procurement processes and secure contracts involving the processing of personal data.

Reach of change

The implications extend well beyond the public sector.

Practical Challenges for MDAs

The Circular requires MDAs to make "adequate budgetary provision" for data protection. For example, recruiting qualified DPOs, ensuring technical safeguards, and engaging licensed DPCOs would require funding that may not have been anticipated in current budgetary cycles.

Second, many MDAs process personal data on systems not designed with data protection principles in mind and may lack support for modern access controls, encryption, or audit trails.

In addition, the Government procurement processes are often lengthy and procedurally rigid. Integrating data protection due diligence into procurement, renegotiating existing contracts, and ensuring vendor compliance may strain already slow processes.

Conclusion

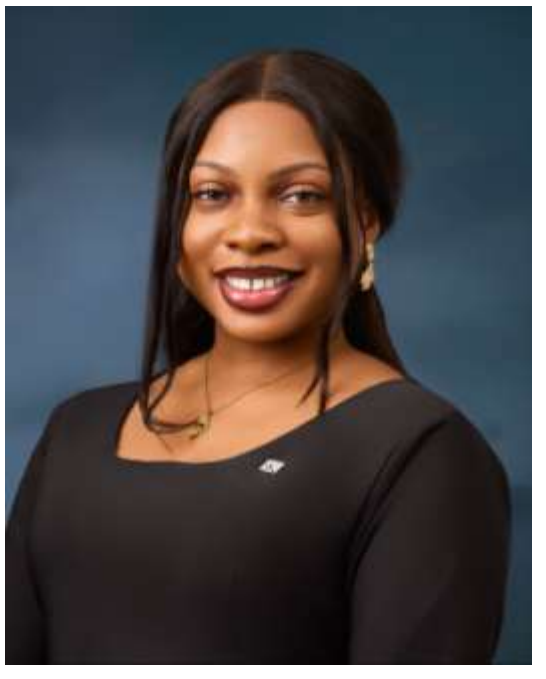
The Circular reflects the Federal Government's renewed focus on data protection compliance and mandates MDAs to understand and implement its requirements. This will require MDAs to review their existing internal data protection frameworks to identify gaps and ensure the integration of data protection practices into their day-to-day operations to ensure compliance with the NDP Act. For private entities dealing with MDAs, the Circular also signals the need for data protection compliance; therefore, they should ensure that their data protection agreements are sufficiently robust to meet the expectations of MDAs and the requirements of the NDP Act.

Kenna is licensed by the NDPC as a Data Protection Compliance Organisation (DPCO) to, among other things, provide audit services for the purpose of compliance with the NDP Act. Consequently, we are available to advise the MDAs on their obligations under the NDP Act and other applicable data protection regulations.

Practical Challenges for MDAs

Nimma Jo-Madugu
Partner, Data Protection

Amanda Abor
Associate, Data Protection



Vivienne Orji
Associate, Data Protection

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

Endnotes

1. Nigeria Data Protection Commission, Press Release: 'FG Issues Compliance Circular to MDAs on Data Protection and Responsible Data Governance' (4 August 2026).
2. Federal Government Circular No. 59805/S.I/74 dated 27 July 2026.
3. Article 10 (7) and (8) of the General Application and Implementation Directive (GAID) 2025. NDPC/NDP Act-GAID/01/2025.
4. Section 24 (Principles of personal data processing), Section 29 (Obligations of the data controller and data processor) and Section 39 (Security, integrity and confidentiality) of the Nigeria Data Protection Act, 2023.

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