tnp.com.ng

The New Practice (TNP)
- An Andersen Collaborating Firm

Understanding the Compliance Obligations of Data Controllers and Processors under the Nigeria Data Protection Act

Olawale Atanda
Senior Associate
E: olawale@tnp.com.ng

Oluwatomini Ibitoye
Associate
E: tomini@tnp.com.ng

The recently concluded 2026 National Privacy Week, themed "Privacy in the Age of Emerging Technologies: Trust, Ethics, and Innovation," highlighted the increasing regulatory emphasis on accountability in data processing. As organisations deploy more sophisticated technologies and data-driven systems, regulators have shifted their focus to ensuring personal data is processed lawfully in an environment that is well-governed.

In Nigeria, this accountability framework is established under the Nigeria Data Protection Act, 2023 ("NDPA") and operationalised through the General Application and Implementation Directive 2025 ("GAID"). Together, they impose specific compliance obligations on data controllers and data processors, including registration requirements and data governance measures.

In this article, we will outline the key regulatory obligations of data controllers and data processors under the NDPA.

What is Personal Data?

The NDPA[1] defines personal data as any information relating to an individual, who can be identifiable or is identifiable, whether directly or indirectly. Identification may occur through a direct identifier, such as a name, or through an indirect identifier, such as an IP address or other online identifier. It may also arise from information relating to a person's physical, genetic, psychological, cultural, social, or economic identity.

In practical terms, if information can be used, whether on its own or in combination with other data, to identify a person, it qualifies as personal data under the NDPA.

Who is a Data Controller?

A data controller is defined in the NDPA[2] as an individual, private entity, public commission, agency or other body who, alone or jointly with others, determines the purpose and means of processing personal data. Put simply, the data controller decides why personal data is collected and how it is processed.

In practice, data controllers are typically the entities that have a direct relationship with individuals whose data are collected and processed. For example, an employer that collects employee records, a fintech company that collects customer information, or a retail business that gathers customer details for onboarding or marketing purposes will be considered data controllers.

Who is a Data Processor?

The NDPA describes a data processor as an individual, private entity, or any other body who processes personal data on behalf of or at the direction of a data controller or another data processor.[3] Unlike a data controller, a data processor does not determine the purpose of processing. Instead, it processes personal data strictly in line with the instructions of the data controller.

In practice, data processors are typically third-party service providers engaged to carry out specific data processing activities. These include cloud service providers, payment processors, payroll administrators, customer support vendors, and IT service providers that handle personal data for and on behalf of data controllers.

Key Regulatory Compliance Obligations for Data Controllers and Processors

1. **Registration as a Data Controller or Data Processor of Major Importance (DCPMI)**

   Under the NDPA and the GAID, an organisation qualifies as a "Data Controller or Data Processor of Major Importance" ("DCPMI") and is required to register with the Nigeria Data Protection Commission ("NDPC") within six (6) months if it meets any of the following criteria:

   a. it processes personal data of more than two hundred (200) data subjects within a six-month period;

   b. it provides commercial Information and Communication Technology (ICT) services on digital devices storing personal data belonging to another individual; or

   c. it processes personal data in any of the following sectors: aviation, communication, education, electric power, export and import, financial services, health, hospitality, insurance, oil and gas, tourism, e-commerce, or public service.

   DCPMIs are classified into three levels based on the scale and volume of data processed: Major Data Processing Ultra High Level, Major Data Processing Extra High Level, and Major Data Processing Ordinary High Level. Each category is subject to strict data protection and compliance standards.

2. **Carrying out of Annual Data Protection Compliance Audits**

   The GAID[4] requires DCPMIs to conduct periodic compliance audits of their data processing activities to mitigate data protection risks.

   Furthermore, DCPMIs are required to file Compliance Audit Returns (CAR) with the NDPC not later than 31st of March every year. These audits must be conducted by a Data Protection Compliance Organisation (DCPO) licensed by the NDPC. Upon successful filing of the CAR, the NDPC issues a Compliance Audit Returns Certificate which serves as evidence of filing the CAR for the audited year.

3. **Appointment of a Data Protection Officer**

   A DCPMI is required to appoint a Data Protection Officer ("DPO") with adequate knowledge of data protection law and practice.[5] The DPO may be a member of the staff of the organisation or be engaged under a service contract.

   The DPO is responsible for overseeing compliance with data protection obligations, advising on data protection risks, and acting as a point of contact with the NDPC and data subjects. The contact details of the DPO must be made publicly available and communicated to the NDPC in accordance with regulatory requirements.

4. **Conducting a Data Protection Impact Assessment**

   Where a proposed data processing activity is likely to result in high risk to the rights and freedoms of data subjects, a data controller is required, prior to commencing the processing, to carry out a Data Protection Impact Assessment ("DPIA")[6]. A DPIA is particularly required where processing involves automated decision-making with legal or similarly significant effects, profiling or large-scale evaluation of individuals, processing of sensitive personal data, systematic monitoring of data subjects, deployment of new or emerging technologies, or processing relating to vulnerable persons. The DPIA is intended to identify data protection risks and document measures adopted to mitigate those risks.

5. **Notification of Personal Data Breaches**

   Data controllers are required to notify the NDPC within seventy-two (72) hours of becoming aware of a personal data breach that is likely to pose a risk to the rights and freedom of data subjects[7]. Where the breach is likely to result in a high risk to affected data subjects, the data controller is also required to notify the affected data subjects without undue delay. Data processors, on the other hand, are required to promptly notify the relevant data controller upon becoming aware of a personal data breach.

6. **Management of Data Subject Rights**

   Data controllers and processors must implement effective systems to receive and respond to data subject requests. The NDPA recognises specific rights, including the right of access, rectification, erasure, and data portability.[8]

   Organisations are expected to respond to data subject requests in a timely manner and ensure that such requests are handled in a lawful, transparent, and consistent manner.

7. **Semi-Annual Data Protection Reports**

   As part of ongoing governance obligations, DCPMIs are required to maintain Records of Processing Activities ("ROPA") and ensure continuous internal oversight of data protection compliance.[9]

   In this regard, DCPMIs are to ensure their DPOs compile and submit a semi-annual data protection report to management. This report should outline the organisation's purposes for processing, categories of personal data involved, and any third parties with whom personal data is shared. These records must be made available to the NDPC upon request.

> **"With the annual audit cycle now underway, organisations should actively review their compliance framework, confirm whether applicable registration and audit obligations apply to them, and assess the adequacy of existing governance measures. Early attention to these requirements can help avoid gaps, delays, and regulatory exposure."**

Other Ongoing Compliance Obligations for Data Controllers and Processors

8. **Ensuring Regular Staff Training and Awareness**

   DCPMIs are expected to conduct regular data protection training and awareness programmes for their employees, particularly staff directly involved in data processing activities[10]. This helps ensure that data protection obligations are understood and applied in day-to-day operations.

9. **Implementation of Data Security Measures**

   DCPMIs must implement appropriate technical and organisational security measures to protect personal data from unauthorised access, loss, misuse, or alteration. These measures may include access controls, encryption, routine security assessments, incident response procedures, and staff training aimed at reducing data breach risks[11].

10. **Compliance with Data Protection Principles**

    Personal data must be processed in line with the data protection principles under the NDPA[12]. This includes ensuring that processing is lawful, fair, and transparent; limited to specified and legitimate purposes; adequate and not excessive; accurate and kept up to date; retained only for as long as necessary; and protected through appropriate technical and organisational measures to ensure its confidentiality, integrity, and availability.

11. **Lawful Basis for Data Processing Activities**

    DCPMIs must ensure personal data are processed only where a lawful basis exists under the NDPA. Data processing shall be lawful where the consent of the data subject has been obtained or it is necessary for the performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest or under official authority, or for the purposes of the legitimate interests of the controller or a third party[13].

    Where reliance is placed on a lawful basis, it must be appropriate to the processing activity and properly documented, particularly for audit and regulatory review purposes.

Conclusion

The NDPA and GAID set out the regulatory requirements for data protection and accountability and establish clear obligations for both data controllers and processors. Organisations that implement these requirements effectively will ensure the protection of data subjects' rights, mitigate regulatory and operational risks, and maintain demonstrable compliance with Nigerian data protection laws.

With the annual audit cycle now underway, organisations should actively review their compliance framework, confirm whether applicable registration and audit obligations apply to them, and assess the adequacy of existing governance measures. Early attention to these requirements can help avoid gaps, delays, and regulatory exposure.

TNP is licensed by the NDPC as a DPCO.

[1] Section 65 of the NDPA
[2] Section 65 of the NDPA
[3] Section 65 of the NDPA
[4] Article 10 of the GAID
[5] Section 32 of the NDPA
[6] Section 28 of the NDPA
[7] Section 40 of the NDPA
[8] Section 34 of the NDPA
[9] Article 13 of the GAID
[10] Article 7(g) of the GAID
[11] Section 39 of the NDPA
[12] Section 24 of the NDPA
[13] Section 25 of the NDPA