The NDPC's 21-Day Compliance Ultimatum: *A Practical Roadmap for Organizations*

abcs Alert

Volume 1 October 2025

On Monday, the 25th of August 2025, the Nigerian Data Protection Commission (NDPC) ushered in a new era of enforcement action by issuing a compliance notice targeted at organizations suspected of non-compliance with the Nigeria Data Protection Act (NDPA) as part of the NDPC's aggressive crackdown on data controllers and processors in critical sectors of the Nigerian economy.

From the compliance notice in question, the NDPC announced that it is embarking on a sector-by-sector investigation of organizations in non-compliance with NDPA. It has therefore directed target organizations in the pension, gaming, insurance and financial sectors to show evidence of compliance with the NDPA in a bid to safeguard the fundamental rights and freedoms of Nigerians, including the right to privacy as enshrined in the constitution to foster ethical and responsible data practices.

With a 21-day deadline issued, the defaulting controllers are expected to provide as proof of compliance to the Commission:

- Evidence of filing NDPA Compliance Audit Returns (CAR) for 2024.
- Evidence of designation or appointment of a Data Protection Officer, including the name and contact details of such officer.
- Summary of technical and organizational measures for data protection within the organization.
- Evidence of registration as a Data Controller or Processor of Major Importance.

This move demonstrates the NDPC's seriousness in enforcing the NDPA's provisions against possible defaulters, as penalties or criminal prosecution may be initiated against those found wanting. This article seeks to delineate the requirements of the NDPA and provide a practical guide for compliance for organizations.

DECONSTRUCTING THE REQUIREMENTS

1. Compliance Audit Returns (CAR)

A data controller or processor generally has obligations to comply with the relevant provisions of the NDPA. One of the ways to demonstrate that is through the filing of compliance audit returns. This is a mandatory annual report that assesses a controller or processor's data processing activities and practices to determine its compliance with obligations under the NDPA. A data controller or processor is mandated to carry out a periodic audit of its processing activities with a view to mitigating data protection breaches through technical and organizational measures.

The compliance obligations stipulated by the Commission are as follows:

- A controller is expected to file the returns annually. In the case of a controller established before the enactment of the Act, it must be filed not later than 31st of March each year. But in the case of a controller established after the Act, its audit returns must be filed within 15 months of its establishment and afterwards, not later than the 31st of March each year.
- A controller is expected to file the returns per the template provided in Schedule 2 to the General Application and Implementation Directive (GAID).
- A data controller or processor is also expected to pay filing fees for the audit returns where it falls in the category of Extra High-Level or Ultra High-Level processing.
- Controllers or processors that fall in the category of Ultra High-Level and Extra High-Level processing are required to file their compliance audit returns through a certified Data Protection Compliance Organization.

After the filing of CAR, the Commission will issue a Compliance Audit Returns Certificate as proof of compliance. It should be noted that failure to file these returns on time attracts an administrative penalty of an additional fifty percent of the filing fees.

2. Designation of a Data Protection Officer (DPO)

The role of a Data Protection Officer (DPO) is indispensable to data protection compliance. The office exists to ensure an organization meets its responsibilities and obligations under the NDPA and the GAID. The role of DPO is one of enormous dimension within any organization as they bear responsibility for overseeing all data processing activities in which an organization is engaged, ensuring they are fully compliant with the law while also acting as the organization's point of contact for data subjects, relevant stakeholders and the NDPC.

- What does a DPO do?

DPOs have a range of responsibilities including advising on compliance with data protection regulations, coordinating data breach responses and acting as a liaison between the key stakeholders such as management, data subjects and NDPC, amongst other responsibilities.

- When is a DPO needed?

Section 32 of the NDPA provides for the appointment of a Data Protection Officer and mandates data controllers or processors of major importance to have a DPO in its employ. This class of controllers and processors are those that undertake processing which are of significant value to the economy and security of the country. Hence for non-DCPMIs, the appointment of a DPO is optional.

This officer could be an existing member of staff of the controller or processor or could be outsourced on a service contract. On appointment, their details must also be published and communicated to the Commission. This is to ensure accessibility.

- What does a DPO need?

The General Application and Implementation Directive 2025 provides for what the DPO should be provided with upon appointment.

- Adequate resources: The organization should avail the DPO of sufficient resources to fulfill their duties and responsibilities ranging from a robust financial budget to implement a comprehensive privacy program to technical infrastructure to automate and ease compliance administration.

- Access to data processing activities: The DPO should be engaged on all issues relating to processing of personal data in the organization for visibility and evaluation.

- Continuous training: Likewise, a DPO is an investment in that the organization is expected to undertake continuous training of the DPO to enable them shore up and broaden their expertise and skills to effectively discharge their duties within the organization.

- Independence: The DPO should be allowed to perform their functions independently and hence provided a neutral work environment in which to make decisions. One way of doing this is by ensuring the

DPO has no other duties that undermine their primary responsibility of overseeing compliance such as being involved in any form of data processing activity.

- Confidentiality: The officer should be bound by secrecy and confidentiality. This includes ensuring they report only to the highest management of the data controller or processor.

- Protection from retaliation: The officer must be protected from retaliation in the course of performing their duty. For example, the DPO advises against any proposed data processing project or activity by management, they should be able to do this without fear of reprimand or penalty from management.

- No conflict of interest: Regardless of their mode of appointment, the organization should ensure that there is no conflict of interest. Where the officer has to juggle competing responsibilities, one to data protection and the other to the business goals, it may hinder their objectivity.

The Commission operates a database of certified DPOs and carries out an annual credential assessment of the DPOs to ensure they maintain a level of professionalism needed to discharge their duties and responsibilities.

3. Implementing Technical and Organizational Measures

As part of the measures to protect the confidentiality, availability and security of data, under Section 39, the data controller or processor is obliged to employ technical and organizational measures to protect personal data in their care. These measures were enunciated in the Act; they include but are not limited to:

- Pseudonymization or other methods of de-identification of personal data.
- Encryption of personal data.
- Processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services.
- Processes to restore availability of and access to personal data in a timely manner, in the event of a physical or technical incident.
- Periodic assessments of risks to processing systems and services, including where the processing involves the transmission of data over an electronic communications network.
- Regular testing, assessing, and evaluation of the effectiveness of the measures implemented against current and evolving risks identified.
- Regular updating of the measures and introduction of new measures to address shortcomings in effectiveness, and accommodate evolving risks.

4. Evidence of Registration as a Data Controller or Processor of Major Importance (DCPMIs)

A data controller or processor is considered to be of major importance if it has particular value or significance to the economy, society or security of Nigeria. What qualifies the controller as having particular value or significance to the economy includes:

- Where it processes the personal data of more than two-hundred (200) data subjects in six (6) months.
- Where it carries out commercial Information Communication Technology (ICT) services on any digital device which has storage capacity for personal data and belongs to another individual.
- Where it processes personal data as an organization or a service provider in anyone of the following sectors:
  - Aviation
  - Communication
  - Education
  - Electric power
  - Export and import
  - Financial
  - Health
  - Hospitality
  - Insurance
  - Oil and gas
  - Tourism
  - E-commerce
  - Public service

Based on this, a data controller is required to register with the NDPC as a DCPMI if they fall into this category and to pay the required registration fees.

The registration fee varies depending on the class of DCPMI it falls into. Ultra-High Level Controllers are required to pay a fee of N250,000, Extra-High Level Controllers are required to pay a fee of N100,000 while Ordinary-High Level Controllers are required to pay a fee of N10,000.

Wrapping Up

These extensive compliance obligations may seem daunting or even a setback for the affected organizations but in the long run, they should be viewed as laying the essential foundation for a stronger digital economy built on respect for fundamental rights and freedoms of the public. The NDPC is setting a higher standard for data governance and reinforcing that data protection and privacy should now be an indispensable aspect of business. These moves from the Commission will shape consumer confidence and also create a more secure online environment. The future of businesses will soon depend on how they can prove they are responsible enough to be trusted with customers' sensitive information. A strong commitment to data protection is the most valuable investment an organization can make.

5 /7 Ademola Street,
off Awolowo Road
South West Ikoyi, Lagos, Nigeria

19 Kolda Street,
Off Adetokunbo Ademola Crescent
Wuse II, Abuja, Nigeria

(+234) 906 902 2222
(+234) 906 903 3333
(+1) 917 809 4981
(+44) 203 807 9070

abcs-global.com
solutions@abcs-global.com