HERMON
LEGAL PRACTITIONERS

FROM REGISTRATION TO AUDIT RETURNS: NDPC COMPLIANCE OBLIGATIONS IN NIGERIA

www.hermonlaw.com

Introduction

Data protection has become a central compliance obligation for organizations operating within Nigeria's increasing digital economy. As businesses heavily rely on personal data for operations, service delivery, and growth, regulatory oversight has shifted decisively from voluntary compliance to enforceable governance standards.

The enactment of the Nigeria Data Protection Act 2023 (NDPA or "The Act") and the establishment of the Nigeria Data Protection Commission (NDPC) marked a significant milestone in Nigeria's data governance framework. These obligations are further operationalized by the General Application and Implementation Directive (GAID) issued by the NDPC, which prescribes the practical mechanisms for registration, audit, reporting, and enforcement.

One of the core obligations under this framework is mandatory registration and continuous compliance for organizations classified as Data Controllers and Data Processors of Major Importance, including the filing of Annual Compliance Audit Returns (CAR). This publication explains who must register, how registration works, the structure of ongoing compliance, applicable audit obligations, timelines, fees, and the consequences of non-compliance.

Why Data Protection Registration Matters

Data protection registration and compliance are no longer box-ticking exercises. They are fundamentally about accountability, trust, and operational legitimacy. Organizations in Nigeria routinely process sensitive personal data, including financial records, health information, biometric identifiers, and digital transaction data

It is required that such data be processed lawfully, securely, and transparently. Failure to comply exposes organizations not only to financial penalties of up to ₦10 million or 2% of annual gross revenue, whichever is higher, but also to reputational damage, regulatory scrutiny, and reduced commercial confidence, particularly in transactions involving international partners.

Who Is Required to Register with the NDPC?

Registration is mandatory for entities designated as Data Controllers and Data Processors of Major Importance (DCPMIs) pursuant to sections 5(d), 44, 45, and 65 of the NDPA, as further clarified by the NDPC Guidance Notice.

Meaning of Data Controllers and Processors of Major Importance

The Act defines a data controller and processor of major importance as an entity which is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate.

Under the Guidance Notice, an organization is deemed to be of major importance where it keeps or has access to a filing system (whether analogue or digital) for the processing of personal data and, among others, where it:

- Processes the personal data of more than 200 data subjects within six months;
- Provides commercial ICT or digital services involving access to personal data; or
- Operates within designated high-impact sectors such as finance, health, education, communications, oil and gas, tourism, e-commerce, hospitality, aviation, public service, insurance, electric power, and export and import.

The NDPC adopts a risk based regulatory approach. The greater the scale, sensitivity, or societal impact of data processing, the higher the compliance obligations imposed.

Classification of Major Data Controllers and Processors

For regulatory clarity, eligible organizations are classified into three tiers:

1. Ultra-High Level (UHL)

This category includes commercial banks, telecommunication companies, fintechs, multinational corporations, oil and gas companies, public social media and email application developers, payment gateway service providers, and organizations processing the personal data of over 5,000 data subjects within six months. These entities are expected to comply with international and highest attainable data protection standards.

The Registration Fee for this category is ₦250,000.

2. Extra-High Level (EHL)

This category covers government Ministries, Departments and Agencies (MDAs), tertiary institutions, hospitals providing secondary or tertiary care, microfinance banks, mortgage banks, and organizations processing between 1,000 and 4,999 data subjects.

The Registration Fee for this category is ₦100,000.

3. Ordinary-High Level (OHL)

This includes primary and secondary schools, corporate training service providers, primary health centers, independent medical laboratories, hotels and guest houses with fewer than fifty (50) suites, and organizations processing over 200 data subjects within six months but below EHL thresholds.

The Registration Fee for this category is ₦10,000.

Entities Not Classified as Data Controllers or Processors of Major Importance

Certain entities fall outside the classification of DCPMIs, including traders or artisans who do not transmit personal data as a core business activity, traders with less than fifteen employees or artisans that do not maintain structured filing systems, and informal social or professional groups operating on digital platforms. While such entities may not be subject to mandatory registration, they remain bound by the general data protection principles under the NDPA.

Exemption of Establishmentor Organizations that are Data Controllers and Data Processors of Major Importance

Pursuant to section 44(6) of the NDP Act and the GAID, the following categories of entities are exempt from registration:

- Community-based associations
- Faith-based organizations
- Foreign embassies and high commissions
- Judicial establishments or bodies performing adjudicatory functions
- multi-governmental organizations

Importantly, exemption from registration does not amount to exemption from data protection obligations. All entities must continue to process personal data lawfully, fairly, and transparently in accordance with the NDPA.

Registration with the NDPC

Registration is conducted through the NDPC Information Management Portal (NIMP), which also hosts:

- The public register of compliant entities
- The list of licensed Data Protection Compliance Organizations (DPCOs)
- Annual audit filing and renewal services

NDPC Registration Process: Key Steps

Registration with the NDPC is a structured compliance process combining internal preparation, third-party audit (where applicable) and formal filing:

1. Determine registration status based on processing volume, data sensitivity, and sector.
2. Appoint a Data Protection Officer (DPO) to oversee compliance and act as the regulatory contact.
3. Conduct a data protection audit (for DCPMIs) through a licensed DPCO, for a Data Protection Audit Report (DPAR).
4. Prepare required documentation, including organizational details, DPO information, processing descriptions, and internal policies.
5. Register via the NDPC portal and pay prescribed fees, subject to NDPC review and confirmation. Registration marks the commencement and not the completion of data protection obligations.

The Role of the Data Protection Officer (DPO)

Data Controller or Processor of Major Importance must have a DPO. DPOs plays a central governance and accountability role, including

- Monitoring compliance with the NDPA and related policies
- Advising on lawful bases for processing
- Preparing semi-annual data protection reports
- Supporting audits and regulatory engagements
- Acting as the primary contact point for data subjects and the NDPC

Compliance Audit Returns (CAR) under the GAID

Nature of the CAR

Registration alone is insufficient. Eligible organizations must file Annual Compliance Audit Returns (CAR) in accordance with the NDPA and Schedule 2 of the GAID. The CAR is a structured, evidence-based audit rather than a narrative declaration.

Filing Timeline

Data Controllers and Data Processors are required to conduct a compliance audit within 15 months of commencing business and annually thereafter.

For Ultra-High Level and Extra-High Level entities, CAR must be filed with the NDPC no later than 31 March of each year, through a licensed DPCO.

Scope of the GAID Schedule 2 Audit

The audit assesses compliance across governance, data security, accountability & Risk Evaluation, cross-border transfers, and third-party processing, including DPO certification, staff training, DPIAs, security controls, and processor due diligence etc.

Compliance Audit Filing Fees under the GAID

Under the GAID, compliance audit filing fees are as follows:

For Ultra-High Level (UHL) DCPMIs, the applicable fees are ₦1,000,000 where personal data of 50,000 data subjects and above is processed, ₦750,000 for 25,000–49,999 data subjects, and ₦500,000 for below 25,000 data subjects.

For Extra-High Level (EHL) DCPMIs, filing fees are ₦250,000 where 10,000 data subjects and above are processed, ₦200,000 for 5,000– 2,500 data subjects, and ₦100,000 for below 2,500 data subjects.

Ultra-High Level and Extra-High Level entities register once but must submit CAR annually. Ordinary-High Level entities renew registration annually but are exempt from filing CAR.

Consequences of Non-Compliance

The NDPC is vested with extensive enforcement powers. Non-compliance may result in:

- Late filing penalties equivalent to 50% of applicable CAR fees
- Financial penalties of up to ₦10 million or 2% of annual gross revenue, whichever is higher, for DCPMIs
- Financial penalties of up to ₦2 million or 2% of annual gross revenue, whichever is higher, for other entities
- Administrative sanctions and enforcement order

Beyond financial exposure, non-compliance carries significant reputational and operational risk and may expose organizations to regulatory action or private claims by affected data subjects.

Conclusion

For organizations processing personal data of economic or societal significance, NDPC registration and GAID-driven audit compliance are not optional. A clear understanding of registration thresholds, audit requirements, and filing timelines is essential for lawful operations and effective risk management. Proactive compliance remains significantly less costly than regulatory enforcement.

HERMON®
LEGAL PRACTITIONERS

For further inquiries, send an email to Hermon@hermonlaw.com