COMPLIANCE AUDIT REPORT FILING REGIME UNDER THE GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVES: *ASSESSING REGULATORY GAP*

INTRODUCTION

In an era where technological advancement fuels innovation and drives competition, regulatory clarity has become critical to regulate exchange and protection of personal data, and ultimately human privacy and dignity. Recognizing this reality, the Nigeria Data Protection Commission (the **"Commission"**), on March 20, 2025, issued the ***General Application and Implementation Directive*** (the **"GAID"** or **"Directive"**) pursuant to its powers under the Nigeria Data Protection Act 2023 (the **"Act"**).

The issuance of the GAID represents the Commission's commitment to further solidify data protection framework in Nigeria whilst ensuring that every individual and organization subject to the Act understands and implement the provisions of the Act accordingly, thereby upholding the foundational right to privacy as enshrined in section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) (the **"Constitution"**).

The GAID, with a view to ensuring clarity and effectiveness in data protection legal framework, re-emphasizes the clear priority of the Act over conflicting laws as provided in section 63 of the Act[1]. It further directs that where its provisions conflict with the provisions of the Act, the Act takes precedence.[2]

Pertinent to highlight is the fact that the GAID repealed the Nigeria Data Protection Regulation 2019 (the **"NDPR"**)[3] by providing in Article 3 (3) that "Upon the issuance of the GAID, the Commission shall cease to apply the Nigeria Data Protection Regulation (NDPR) 2019 as a legal instrument for regulating data privacy and protection. In line with Section 64 of the NDP Act relating to transitional 11 provisions, this measure shall not affect anything done under the NDPR prior to the issuance of this GAID". However, any actions taken under the NDPR prior to the issuance of GAID will remain valid and enforceable.

The GAID, amongst other innovations, provides for the filing of Compliance Audit Report (**"CAR"**) by Ultra High Level (**"UHL"**) and Extra High Level (**"EHL"**) Data Controllers (***as hereinafter defined***) and Data Processors (***as hereinafter defined***), being of major importance, with the Commission not later than March 31 every year.

However, there seems to be an unclear ground as to obligations of data controller or a data processor (not being of major importance) in relation to filing CAR, specifically, Article 10 (1) of the GAID suggests a periodic compliance audit obligation for all data controllers and processors, irrespective of classification.

This article seeks to highlight the regulatory lacuna in relation to the CAR filing regime under the GAID vis a vis the NDPR, the implication of same and a call for the Commission to provide further clarity.

Before diving into the CAR filing obligation, it is essential to establish the distinction between data controllers, data processors, and data controllers and processors of major importance.

According to section 65 of the Act, a data controller ("Data Controller") means:

> *"An individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data"*

Also, a data processor ("**Data Processor**") means:

> *"An individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor"*

A data controller or data processor of major importance ("**DC/PMI**") means:

> *"a data controller or data processor that 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.*

1. Section 63 of the Act states "Where the provisions of any other law or enactment, in so far as they provide or relate directly or indirectly to the processing of personal data, are inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail"

2. Article 3 (1) & (2) of the GAID

3. And consequently, the NDPR Implementation Framework 2020

Further to the above, the Commission re-issued[4] a Guidance Notice on the Registration of Data Controllers and Data Processor of Major Importance – NDPC/H-Q/GN/VOL.03/B/24 (the **"Notice"**) classifying and outlining qualifying criteria for entities as ***Data Controllers/Processors of Major Importance***. The Notice has been incorporated as Schedule 7 of the GAID. The Notice, amongst other things, categorized DC/PMI based on the value and the number of data subject they process their personal data as follows:

a. **Ultra-High Level ("UHL"):** This level includes any organisation that processes amongst other personal data of ***over five thousand (5,000) data subjects***, through the means of technology under their technical control or indirectly via a service contract[5].

b. **Extra-High Level ("EHL")**: These are organisations that process amongst other personal data of over one thousand (1,000) data subjects but less than five thousand (5,000), whether directly through technology under their technical control or indirectly via a service contract[6].

c. **Ordinary High Level ("OHL"):** These are organisations that process amongst other personal data of over two hundred (200) data subjects but less than one thousand (1,000) within six (6) months, whether directly through technology under their technical control or indirectly via a service contract[7].

Additionally, the Notice acknowledges that there exists a category of data controllers or processors who may handle data whether in large or small volumes but are not classified as being of major importance[8], owing to the minimal risks their processing activities pose. These entities are considered low risk because they do not present significant economic, technological, or social threats.

While the overarching policy framework encourages ethical data privacy practices across board regardless of the size or scope of the data processor, it imposes stricter expectations on DC/PMIs due to the systemic relevance of their data security to critical industries, sectors, and the national economy. With this context in mind, it becomes imperative to critically examine the provisions of the GAID, particularly the requirement for the filing of CAR.

PRE GAID: FILINGS UNDER THE REPEALED NDPR

Prior to the enactment of the Act, Nigeria's data protection landscape was primarily governed by the NDPR and the NDPR Implementation Framework. Under the old regime, organizations that processed the personal data of Nigerian citizens or residents were required to conduct a comprehensive data protection audit within six (6) months of the regulation's commencement[9] and subsequently on an annual basis particularly where such processing exceed more than two thousand (2,000) data subjects.

These audits are to be carried out through licensed a Data Protection Compliance Organizations (**"DPCOs"**). Specifically, Data Controllers or Data Processor that processed the personal data of more than one thousand (1,000) data subjects within a six (6) month period were mandated to submit a soft copy of a summary audit report containing prescribed disclosures to the National Information Technology Development Agency (**"NITDA"**)[10], which then served as the primary regulatory authority for data protection. Furthermore, any Data Controller or Data Processor processing data of over two thousand (2,000) individuals in a twelve (12) month period was required to submit a summary of its data protection audit no later than March 15 of the subsequent year[11].

Where an organization failed to meet its annual filing obligations under the stipulated thresholds, such failure was deemed a breach of the NDPR, attracting fines as follows: two percent (2%) of the Annual Gross Revenue of the preceding year or Ten Million Naira (₦10,000,000.00), whichever is greater, with respect to a Data Controller that processes the Personal Data of more than ten thousand (10,000) Data Subjects[12] or the payment of the fine of one percent (1%) of the Annual Gross Revenue of the preceding year or the payment of the sum of Two Million Naira (₦2,000,000.00), whichever is greater, for a Data Controller that processes the Personal Data of less than ten thousand (10,000) Data Subjects.[13]

Although the concept of DC/PMI had not yet been formally introduced under the NDPR, the regime implicitly recognized the heightened obligations of entities whose processing activities had systemic relevance. In retrospect, the thresholds stipulated under the NDPR for audit filing effectively anticipated what is now captured under the EHL and UHL categories of DCPMIs in the GAID framework.

CAR FILING UNDER THE GAID; REGULATORY AMBIGUITY

As earlier expressed, the GAID was issued to provide further guide on the implementation of the Act whilst aiming to set additional streamlined and pertinent compliance provisions to Data Controllers and Data Processors in Nigeria. Specifically, we shall consider Articles 7 and 10 of the GAID which address the requirements for conducting and filing CAR. It is essential to state that upon close scrutiny, these provisions reveal a degree of ambiguity that warrants careful examination and subsequent call to action by the Commission.

The provisions of Article 7 of the GAID provide for compliance measures by Data Controllers and Data Processors, specifically outlining compliance obligations with a focus on Data Controllers and Data Processors of major importance. It mandates the registration of such entities with the Commission and requires them to conduct a compliance audit within fifteen (15) months of commencing business[14], with annual audits thereafter. Crucially, Article 7(c) of the GAID explicitly requires only Data Controllers and Data Processors of major importance categorized as UHL and EHL to file on an annual basis, CAR with the Commission by March 31 each year while Data Controller in the category of OHL is required to renew its registration with the Commission on an annual basis and is not required to file annual CAR upon renewal of its registration.

From the foregoing, it seems that the GAID vis-a-vis the above provisions simply focus on CAR filing obligations for UHL and EHL and annual renewal for OHL. However, subsequent consideration of Article 10 of the GAID introduces a grey area.

For better context, Article 10 (1) of the GAID presents a broader, more generalized mandate, providing that:

> *"A data controller or a data processor **shall carry out periodic compliance audit of its data processing activities** with a view to mitigating the risk of data breaches through appropriate technical and organizational measures"*

Also, Article 10 (9) of the GAID further provides that:

> *"Where a **data controller or data processor fails to file its CAR** as and when due, it shall pay, in addition to the stipulated filing fee, an administrative penalty, which shall be 50% of the stipulated CAR filing fee."*

4. On February 14, 2024, NDPC issued a Guidance Notice on the Registration of Data Controllers and Data Processor of Major Importance- NDPC/H-Q/GN/VOL/02/24. However, by virtue of the judgment of the Federal High Court in Suit No: FHC/KD/CS/34/2024, the NDPC had to reissue another guidance notice on the subject matter inorder for certain items in the Guidance Notice to be complainant with the ruling of the COurt

5. Paragraph 2(2)(e) of the Guidance Notice

6. Paragraph 3 (1) (d) of the Guidance Notice

7. Paragraph 3(1) (f) of the Guidance Notice

8. Paragraph 4 of the Guidance Notice

9. Paragraph 4.1(5) of the NDPR

10. Paragraph 4.1(6) of the NDPR

11. Paragraph 4.1(7) of the NDPR

12. Paragraph 2.10 (a) of the NDPR

13. Paragraph 2.10 (b) of the NDPR

14. Article 7(b) of the GAID

The combined interpretation of the above provisions is to the effect that all Data Controllers and Data Processors, whether of major importance or not, must carry out periodic compliance audits and also file CAR or otherwise be subject to penalty. This raises a series of questions, particularly as to the intent of the above provisions when placed side by side with the initial provisions of Article 7 treated in the preceding paragraph.

The language in Article 10(1) and (9) of the GAID implies that all Data Controllers and Data Processors, regardless of their classification, have audit and filing obligations which run directly contrary to the provisions of Article 7 of the GAID which have previously limited audit and filing obligations to UHL and EHL respectively.

This dichotomy raises critical questions. Does the GAID require all Data Controllers and Data Processors, major or otherwise to submit annual compliance audit returns? Or is this filing obligation reserved exclusively for EHL and UHL? The lack of clarity between these provisions creates uncertainty for Data Controllers and Data Processors, potentially leading to inconsistent compliance practices and enforcement challenges.

To further buttress the above, it is critical to consider Schedule 10 of the GAID which provides for CAR filing fees as follow:

S/N	DCPMI	Tier	FEE (N)
1	**Ultra-High Level – UHL**	A – 50,000 data subjects and above.	1,000,000
		B – 25,000-49,999 data subjects.	750,000
		C – below 25,000 data subjects.	500,000
2	**Extra-High Level – EHL**	A – 10,000 data subjects and above.	250,000
		B – 5,000-2,500 data subjects.	200,000
		C – below 2,500 data subjects.	100,000

A review of the above further shows the discrepancies between the provisions of article 7 and 10 (1 &9) of the GAID to the effect that while the intent of the Commission might have been to restrict annual CAR filings to EHL and UHL, the latter provisions reflect CAR filings for Data Controllers and Data Controllers which are not of major importance and does not provide for the CAR filling fee for Data Controller and Data Processor. Also, considering that the GAID has repealed the NDPR and the NDPR Implementation Framework, the GAID does not provide for threshold on the number of data subjects a Data Controller or Data Processor must process before it is required to file CAR.

Additionally, there are also discrepancies between the threshold of the number of data subjects for EHL. Per Paragraph 3 (1) (d) of the Notice, it suggests that the number of Data Subjects for EHL will be over one thousand (1,000) data subjects but less than five thousand (5,000). However, Schedule 10 of the GAID provides for the tier of data subjects under the EHL to be more than five thousand (5,000) data subjects.

CONCLUSION

The objective of the GAID is clear: to instill trust, foster accountability, and elevate Nigeria's data governance to global standards. However, regulatory objective must be matched with legislative clarity. The evident discrepancy in the provisions of the GAID, particularly concerning CAR filings, is a critical gap that could dilute the effectiveness of the framework designed to promote accountability. Hence, there is need to provide more clarity with respect to the CAR for Data Controllers and Data Processor (not of major importance).

For additional information on this article, please contact the Bloomfield LP Data Protection Team at dpo@bloomfield-law.ng or your usual Bloomfield LP contact.