TEMPLARS

15 November 2023

Key contacts

Sadiq Ilegieuno
Partner,
Dispute Resolution and Media, Technology, & Intellectual Property (METI)
sadiku.ilegieuno@templars-law.com

Lawal Kazeem
Associate,
Dispute Resolution
lawal.kazeem@templars-law.com

Victoria Oloni
Associate,
Media, Technology, & Intellectual Property (METI)
victoria.oloni@templars-law.com

TEMPLARS ThoughtLab

Navigating the Enforcement Framework under the Data Protection Act 2023

Introduction

In an era characterized by an upward trajectory in the use of digital technologies across several sectors of the economy, the importance of personal data has assumed a global relevance. This development, which has made personal data freely and easily available has also, unfortunately, resulted in the misuse of personal data by data controllers and/or processors and thus leading to the continued quest for data protection by many countries across the globe.

Nigeria is not left out in the quest for sustainable data protection policies and legal frameworks, and after several legislative efforts at enacting a robust substantive legal framework on the subject, the Nigerian Government eventually enacted the Data Protection Act of 2023 (the "**NDPA**" or the "**Act**") in June 2023. The NDPA represents a significant legislative milestone in the efforts by the Nigerian government to address data protection concerns associated with proliferation of data and digital transformation in the society. A key feature of the NDPA is its extensive enforcement regime, which comprises both administrative and judicial measures for addressing violations of data protection standards.

This article seeks to appraise the enforcement frameworks under the Act having regard to their possible efficacy and challenges.

The NDPA Enforcement Mechanisms

The NPDA establishes both administrative and judicial enforcement procedures against violations of the rights of data subjects by data controller or processor. Notably, these enforcement procedures can run simultaneously, as the Act does not explicitly make one procedure contingent on the other or require data subjects to complete one procedure before pursuing the other. In practical terms, this means that a data subject can file a complaint with the Nigeria Data Protection Commission ("**NDPC**") while simultaneously initiating a civil action for breach of personal data. It thus goes without saying that the NPDA

allows for flexibility in seeking remedies, enabling data subjects to explore multiple avenues for redress concurrently.

A. Administrative Approach

The Act permits data subjects who are aggrieved by the decision, action, or inaction of a data controller or data processor in a manner that violates or undermines the provisions of the Act, or any subsidiary legislation made under or preserved by the Act, to lodge complaints with the NDPC, who has been empowered by the NPDA to investigate such complaints, provided they are well founded.[1] Interestingly, the NDPC also has the powers to independently initiate investigations into the activities of data controllers or data subjects, even without a formal complaint being received from a data subject.[2]

By the nature its powers and functions under the Act, the NDPC doubles as an administrative tribunal. Specifically, the NDPC has both investigatory power and the power to compel the appearance of persons and the production of documents[3]. Perhaps, the most prominent of the powers assigned to the NDPC is its power to give or issue compliance orders and impose sanctions (in the form of monetary penalty) for violations of the law. These compliance orders include: (a) warnings, (b) mandating the data controller or data processor to adhere to the provisions of the Act, including complying with data subject's requests; (c) issuing cease-and-desist orders, requiring the data controller or data processor to halt actions that may be inconsistent with the Act, including the processing of personal data specified in the order[4] etc.

Regarding fines, the NDPC has the power to impose a higher maximum amount of penalty of Ten Million Naira (₦10,000,000) or 2% of a controller/processor's annual gross revenue in the previous financial year, whichever is higher, where the defaulting data controller is a Data Controller/Processor of Major Importance ("**DCMI/DPMI**"), or Two Million Naira (₦2,000,000) or 2% of the controller/processor's annual gross revenue in the previous financial year, whichever is higher, if the data controller is not a **DCMI/DPMI**.[5] The NDPA allows for judicial review within thirty (30) days if a data controller is dissatisfied with the decision of the NDPC.[6]

It is instructive to note and recognize the growing legal jurisprudence on judicial restriction on the powers of administrative or statutory bodies to impose administrative sanctions or penalties in Nigeria. Specifically, Nigerian courts have ruled that regulatory authorities lack the authority to impose sanctions to enforce regulatory compliance, as only the courts have the competence to do so[7].

However, this may not be the case with NDPC, because, as indicated above, it is an administrative tribunal in this context. All that it requires, however, is to ensure that data controllers/processors are afforded the opportunity to make necessary representations at the proceedings, before being punished by sanctions or penalties.

The caveat, however, is that in cases where the NDPC initiates investigation by itself, and still proceeds to sit as the tribunal, it may potentially be faced with the challenge of being labeled as acting as a judge in its own cause.[8]

B. Judicial Approach

In addition to the administrative approach highlighted above, the NDPA permits recourse to the court by a data subject who has suffered harm or loss for the recovery of damages. In our view, this is the most functional provision of the NDPA because it encourages and tends to facilitate restorative justice to data subjects.

Meanwhile, the failure of a data controller or processor to comply with an order of the NDPC is treated as a criminal offence for which a data controller or processor may be liable, upon conviction, to fines or imprisonment for a term not more than one (1) year or both.[9] Further, the court may also make an order of forfeiture against a convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act 2022.[10] This forfeiture order is most likely to apply when the data controller or processor profits from their breach of the provisions of the Act.

In terms of liability, it is worth noting that principal officers of any defaulting data controllers/processors may also be deemed culpable unless they can show that: (i) the offence was committed without their consent or connivance; and (ii) they exercised reasonable diligence to prevent the commission of the offence.[11] Furthermore, the Act establishes vicarious liability for data controllers and processors concerning the actions or omissions of their agents or employees, as long as these actions or omissions are related to the organization's business operations.[12]

Challenges of Enforcement under the NDPA

A. Jurisdiction

The issue of jurisdiction within the NDPA raises concerns as the Act does not explicitly designate a specific court with jurisdiction but rather defines "court" as any court of competent jurisdiction. This broad definition leaves room for varying interpretations as to the appropriate court to handle data protection matters.

[1] Section 46 (1) & (2) of the NDPA
[2] Section 46 (3) of the NDPA
[3] Section 46 (4) of the NDPA
[4] Section 47 (1) & (2) of the NDPA
[5] A DCMI/DPMI is defined under the NDPA as 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
[6] Section 50 of the NDPA
[7] National Oil Spill Detection and Response Agency (NOSDRA) v. Mobil Producing Nigeria Unlimited (Exxonmobil) (2018) 13 NWLR (pt. 1636)334, and Shell (Nig) Exploration and Production Co Ltd v. NOSDRA (2021) LPELR-53068 (CA).
[8] This principle is encapsulated in the Latin maxim: nemo judex in causa sua which is one of the twin pillars of fair hearing, which the law holds sacrosanct. Thus, anything or act done or omitted to be done in negation of the principle cannot stand or be legally sustained. See the case of Yanawo v. State (2021) LPELR-56441(CA).
[9] Section 49 (1) of the NDPA
[10] The court shall make a forfeiture order where it finds on a balance of probabilities that the property concerned is reasonably suspected to— (a) be proceeds of unlawful activity; (b) represent whether directly or indirectly the proceeds of unlawful activity; (c) be involved in the facilitation of unlawful activity ; or (d) be intentionally used for unlawful activity.
[11] Section 53 (1) of the NDPA
[12] Section 53 (2) of the NDPA

In time past, data protection cases have been brought before various courts, including the State and Federal High Courts, and the National Industrial Court. However, a case was recently filed against the Attorney General of the Federation and the National Assembly[13] to challenge the absence of provisions specifying courts with jurisdiction over data protection in the NDPA.[14] This suit is a pointer to the fact that the issue of jurisdiction is uncertain, and this lack of clarity may pose challenges for data subjects and the NDPC when seeking legal recourse against data controllers and processors.

B. Parallel Enforcement Mechanisms

Another challenge to enforcement of the provisions of the Act is the existence of parallel enforcement procedures under the Nigeria Data Protection Regulation ("**NDPR**"). The NDPA did not repeal the provisions of the NDPR; instead, it treats specific provisions of the NDPR as void only when these provisions are inconsistent with the NDPA. The NDPR has its own enforcement regime, which does not overtly conflict with the NDPA.

Specifically, under the NDPR, the NITDA (now the NDPC) was empowered to create an administrative redress panel (the "**ARP**") for investigating allegations of breach and issuing administrative orders.[15] We note that the ARP was not established under the NDPA enforcement regime. However, its coexistence with NDPC remains uncertain. This becomes particularly significant due to past disputes over the ARP's role. For example, the Federal High Court of Nigeria ruled in the case of ***Incorporated Trustees of Digital Rights Lawyers Initiative v Unity Bank Plc***[16] that lodging a complaint with the ARP is a necessary precondition for pursuing legal action in court. If one argues that the NDPA's silence on the ARP implies its discontinuation, it raises questions about the fate of other NDPR provisions not explicitly mentioned in the NDPA, such as audit filing requirements.[17]

C. Cross Border Enforcement

Enforcing the NDPA against foreign entities presents another significant challenge. The NDPA'S extraterritorial application, as outlined in Section 2 thereof, means that foreign entities processing the data of Nigerian residents fall within the ambit of the NDPA. However, the practicality of enforcing the NDPA against non-resident entities in Nigeria remains unclear.

To improve the NDPA's extraterritorial reach, the NDPC may consider collaborating with other data protection regulators, particularly within Africa, to leverage existing networks and establish effective cross-border enforcement mechanisms.

[13] https://punchng.com/lawyer-challenges-data-protection-act/
[14] https://thenigerialawyer.com/lawyer-challenges-data-protection-act-2023-in-court-over-jurisdiction/
[15] Article 4.2 of the NDPR
[16] (Unreported) Suit No FHC/AB/CS/85/2020.
[17] However, it's important to note that the NDPC is reportedly developing an implementation framework that may address these complexities.

D. Data Controllers/Processors of Major Importance

The provision of the NDPA on fines and penalties as well as registration with the NDPC have generated debates regarding their operational status. This debate stems from the classification of penalties and registration on the basis of "importance." However, a key challenge arises from the fact that the NDPC has not yet issued regulations to define the criteria for identifying who qualifies as a DCMI/DPMI.

As a result, the said provisions seem to be in a state of limbo, lacking operational clarity. Data controllers and processors are left in uncertainty, as they do not know with certainty if they fall into the DCMI/DPMI category and, consequently, what penalties might apply to them and whether they are required to register with the NDPC.

The absence of clear criteria for determining DCMI/DPMI status creates ambiguity and hampers effective enforcement. To address this issue, the NDPC needs, as a matter of priority, to develop and publish precise guidelines and criteria for classifying organizations as DCMI/DPMIs, providing much-needed clarity to data controllers and processors operating under the Act.

Conclusion

The enforcement mechanisms of the NDPA are robust and commendable. Save for the challenges that we have identified; they represent a massive improvement on the previous legal and institutional frameworks for the enforcement of data protection. If the NDPA's enforcement mechanism are optimally utilized, they will help advance Nigeria's quest for efficient personal data protection.

However, the challenges of the NDPA's enforcement mechanism that we have identified above make it evident that further clarity and guidance is needed to facilitate a smooth and effective implementation of the NDPA's objectives. To this end, we urge the NDPC to take proactive steps in issuing clear and detailed regulations. These regulations should aim to provide clear and precise guidelines on various aspects of the NDPA, including the criteria for identifying DCMI/DPMI, and procedural requirements for lodging complaints, the scope and limits of NDPC investigations.

Clarity in regulations will promote consistency and transparency in enforcement actions, benefiting both data subjects and data controllers. Additionally, the regulations should also offer practical guidance to data controllers on how to prevent or mitigate breaches under the Act. This guidance can include best practices for data handling, security, and compliance, as well as strategies for addressing potential violations. By equipping data controllers with proactive measures, the NDPC can foster a culture of compliance and reduce the likelihood of enforcement actions.