



A REVIEW OF THE NIGERIAN DATA PROTECTION ACT 2023: HIGHLIGHTS AND LIMITATIONS



A REVIEW OF THE NIGERIAN DATA PROTECTION ACT 2023: HIGHLIGHTS AND LIMITATIONS

INTRODUCTION

On the 12th of June 2023, President Bola Ahmed Tinubu assented to the Nigerian Data Protection Bill 2022. The Bill thereon immediately took effect as the Nigerian Data Protection Act, 2023 ("The Act").

The Act provides a comprehensive and far-reaching legal framework for the protection of personal information, safeguards the fundamental rights and

freedoms and the interests of data subjects as guaranteed under the Constitution and the practice of data protection in Nigeria.

This article reviews the key provisions of the NDPA, its amendments to existing legislation and shortcomings.

BACKGROUND AND SCOPE

The objective of the Act, amongst others, is to primarily safeguard the fundamental

rights and freedoms and the interests of data subjects as guaranteed under the Constitution.

The NDPA is made up of 66 sections divided into 12 parts and a schedule. These parts provides for the following- the objectives and application of the Act; the establishment of the Commission and its Governing Council; the financing of the Commission; principles and lawful basis governing the processing of personal data; rights of a data subject; data security; cross-border transfer of personal data; registration of controller/processors and penalties for violations of the Act; enforcement provisions of the Act; legal proceeding on matters covered by the Act; and Miscellaneous provisions.

establishes the Nigeria Data Protection Commission ("the Commission") as the primary regulatory body for data protection in Nigeria, thus, replacing and absorbing the responsibilities, rights, powers, and liabilities of the Nigeria Data Protection Bureau. The Commission, by virtue of section 5 of the Act, is vested with independent power to oversee the full implementation of the Act, and this is expressed through the following functions:

- a. Regulation of the deployment of technological and organisational measures to enhance personal data protection;



HIGHLIGHTS OF THE NIGERIAN DATA PROTECTION ACT 2023

1. Establishment of the Nigeria Data Protection Commission: The Act

- b. Fostering the development of personal data protection technologies, in accordance with recognised international best practices and law;

- c. Accrediting, licensing, and registering suitable persons to provide data protection compliance services;
- d. Registration of data controllers and data processors of major importance;
- e. Promoting awareness of data controllers and data processors' obligation under the Act;
- f. Promoting public awareness and understanding of personal data protection, rights and obligations imposed under this Act, as well as the risks to personal data;
- g. Receival of complaints relating to violations of this Act or subsidiary legislation made under the Act.

Notably, the Act has a transitional provision under section 64, which entails that all powers and duties of the NDPB (Nigeria Data Protection Bureau) are to be transferred to the Commission. It is our opinion that the establishment of the Commission as an independent and effective regulatory commission to oversee data protection

and privacy issues in Nigeria is a significant achievement.

However, a closer look at the composition of the governing council of the Commission reveals a loophole on its 'independence status.' This is seen in the fact that the appointment and removal of the Council members lies solely under the President's prerogative, which indicates heavy reliance on the executive arm of government.


Furthermore, the Commission is required to submit legislative proposals to the Minister of Communication and Digital Economy, including amendments to existing laws, to strengthen personal data protection in Nigeria. The Commission can also make regulations on any matter that the Minister considers necessary. This setup implies that the President, the Minister, and therefore the executive arm of government, have considerable influence over the Commission's decision-making process. This situation undoubtedly casts doubt on the independence of the Commission.

2. **Applicability of the Act to Data Subjects resident in Nigeria:** Section 2 of the Act states that it will only apply where:

- The data controller or data processor is domiciled, resident, or operating in Nigeria;
- The processing of personal data occurs within Nigeria; or
- The data controller or the processor is not domiciled, resident or operating in Nigeria, but is processing personal data of a data subject in Nigeria.

or operation in Nigeria or the residency of the data subject in Nigeria. However, the Act does not define the terms used. The test to determine whether a controller or processor is domiciled, resident or operating in Nigeria is unknown.

Summarily, the Act applies if a data controller or processor resides or conducts business operations in Nigeria, processes data within Nigeria, or processes personal data of data subjects in Nigeria while



" the Act does not define the terms used. The test to determine whether a controller or processor is domiciled, resident or operating in Nigeria is unknown..."

The scope of applicability of the NDPA manifestly differs from that of the Nigerian Data Protection Regulation (NDPR). Whereas the NDPR is based on the citizenship and residency of the data subject, the NDPA is based on the controller or processor's domicile, residency,

residing or operating abroad. It appears that Nigerians living abroad are excluded from the scope of application of the Act.

3. **Legitimate Interest as a basis for processing Personal Data:** The NDPA, under section 25 sub-

section 1(b)(v) introduces 'legitimate interest' as a basis for processing personal data, in addition to the five existing legal bases under the NDPR- Consent, Contractual obligation, Legal obligation, Vital Interest and Public interest. Thus, the Act has ensured some harmonisation around the legality of data processing in the country. Previously, there existed an uncertainty as to whether "legitimate interest" was a valid lawful basis since it was not provided for in the NDPR, but in the Implementation Framework. However, this uncertainty has been laid to rest because of this provision. Legitimate interest will however not be a basis for processing personal data where the fundamental rights and freedom of a data subject overrides such interest, or where the interest is incompatible with the other lawful bases or where the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

The introduction of legitimate interest as a ground for processing data will provide a lawful alternative for data controllers to process personal data. Although the Act establishes legitimate interest as a basis for processing

data, it does not define the phrase. It is therefore unclear what the scope of legitimate interest will be to invoke its applicability.

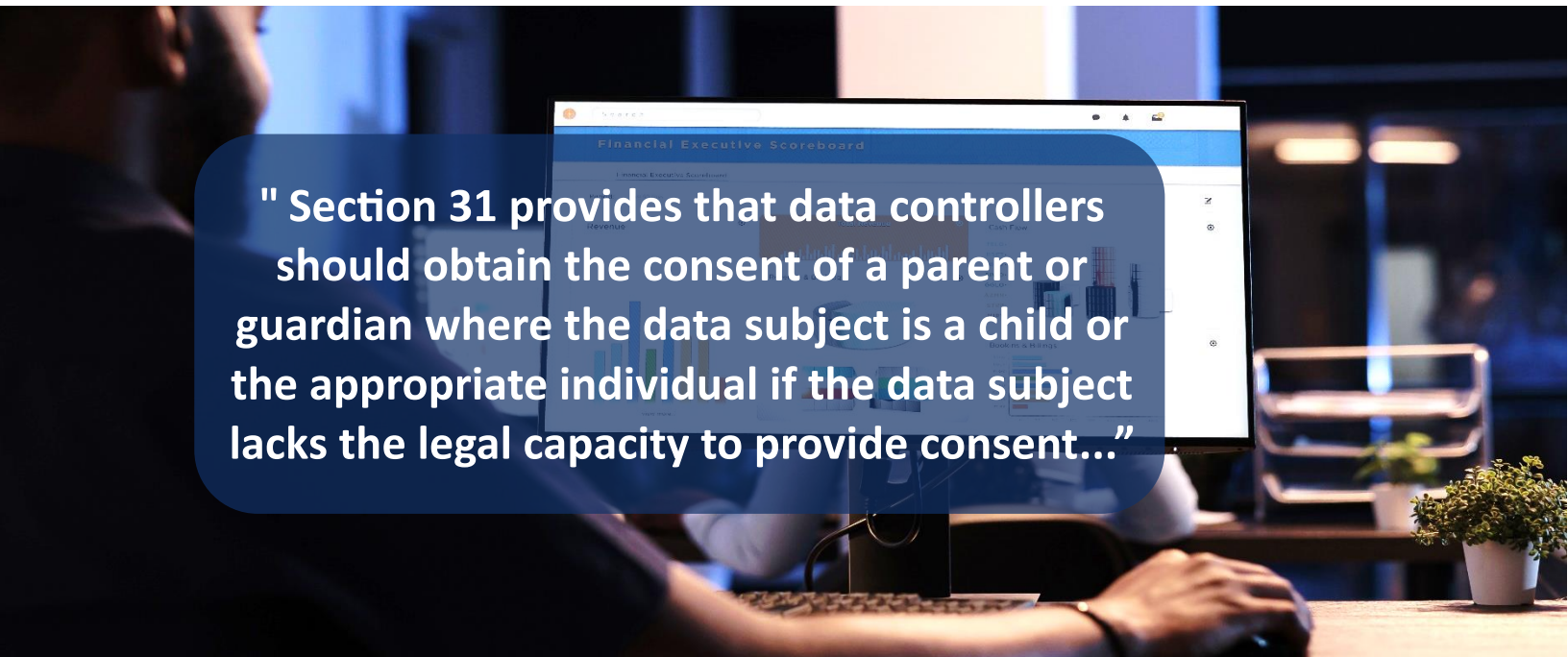
4. **Data Protection Impact Assessment:**

The Act, under section 28, makes provision for Data Protection Impact Assessment ("DPIA"). As an improvement on the former regime, the Act requires data controllers to conduct a DPIA prior to processing personal data that may result in high risk to data subjects' rights and freedom. The assessment must identify risks and impact, assess necessity and proportionality, and outline measures to address risks and protect personal data. The Commission may issue regulations or directives on this section. This is a more elaborate provision on DPIA as opposed to the provisions of the NDPR and its Implementation Framework.

5. **Sensitive Personal Data:** The Act provides rules on the processing of sensitive personal data. This is an improvement on the provisions of the NDPR which merely provides for the definition of the term. By the provision of section 30 of the Act, sensitive personal data can only be processed under certain conditions, such as explicit and informed consent of the data

subject, necessary obligations, vital interests of the data subject, non-profit organizations' activities, legal claims, public interest, medical care, public health, and archiving purposes.

consent. Section 31 provides that data controllers should obtain the consent of a parent or guardian where the data subject is a child or the appropriate individual if the data subject lacks the legal capacity to provide consent.



" Section 31 provides that data controllers should obtain the consent of a parent or guardian where the data subject is a child or the appropriate individual if the data subject lacks the legal capacity to provide consent..."

The Act empowers the Commission to issue regulations or directives for further classifications, grounds, and safeguards of sensitive personal data. Also, the Commission must consider the risk of significant harm, confidentiality, and protection of sensitive personal data in making such regulations or directives.

However, this right is limited where the processing is necessary to protect the vital interests of the child or individual lacking the legal capacity to consent or the processing is carried out for purposes of medical or social care and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality.

6. Protection of Minors: Unlike the NDPR, the NDPA makes clear and precise provisions on consent to process the data of a child or a person lacking the capacity to give

7. Data Security: Part 7 of the Act expands on Regulation 2.6 of the NDPR 2019, by introducing

provisions that emphasize appropriate technical and organizational measures for data security. It specifically addresses considerations such as the amount and sensitivity of data, potential harm to data subjects, processing extent, retention period, and available technologies. Also, the Act makes adequate provision for steps to be taken by organisations in the event of a personal data breach including personal data breach notification by data processors to the data controller either directly or publicly, prompt response by the processor involved to requests of the data controller or data processor that engaged it; and notification of the Commission within 72 hours of a breach likely to result in risks to individuals' rights and freedoms.

The Act in this part also provides for record-keeping and verification of compliance. In comparison, the Nigeria Data Protection Regulation, 2019, provision on data security only focuses on general security measures, organizational policies, and staff capacity building.

8. **Cross-Border Transfer of Personal Data:** The Act, in Part 8, provides elaborately for cross-border data transfer regulation in Nigeria. Unlike

the provisions of the NDPR, the Act focuses on adequate level of protection to be determined upon examination by the processor/controller, upon the determination, the Commission may approve such binding rules, codes of conduct or certification mechanisms (in proof of adequate level of protection) proposed to it by a data controller. Also, the Act does away with the provision for the approval of the Attorney-General of the Federation in order to transfer data. The Act also attempts to provide for safeguards to transfer of data in the absence of an adequate level of protection and expands on the exceptions for transfer, which includes explicit consent, contract performance, public interest, legal claims, and vital interests.

The NDPA further provides that the Commission is required to make guidelines and regulations that will determine the adequacy of the recipient, as well as determine from time to time whether any country, region or specified sector.

9. **Registration of Data Controllers and Data Processors of Major importance:** By the provision of section 44 of the NDPA, data controllers and data processors of

Major Importance are required to register with the Commission within six months of the Act being passed into law. Although the Act does not clearly define or specify the amount of data processed to qualify as a data controller or processor of major importance, it gives the Commission the power to determine the amount of data processed to qualify for a data processor/controller of major importance. The Commission will also consider classes of data controllers or processors that process personal data that is of specific importance to the economy, society, or security of Nigeria.

To register, data controllers and processors of Major Importance must provide a description of the Data Protection Officer (DPO)'s personal information, the categories and number of data subjects, the purposes for which the personal data is processed, and any country to which the data controller or processor intends to transfer the data. Regular updates must be provided to the Commission within 60 days of significant changes to the information provided. The Commission will exempt a class of data controllers and processors from the registration requirement if it considers it unnecessary.

" ...Regular updates must be provided to the Commission within 60 days of significant changes to the information provided..."



It should be noted that data controllers and processors of Major Importance may be required to pay prescribed fees or levies as determined by the Commission, and duly the Commission shall maintain and publish on its website a register of duly registered data controllers and processors of Major Importance.

10. **Provision Relating to Enforcement:**

Part 10 of the Act introduces provisions for enforcement and penalties. Data subjects who are aggrieved by violations of the Act can lodge complaints with the Commission. The Commission can issue compliance orders, impose sanctions, and enforce penalties based on the severity of the offense. The Act also establishes a Unit within the Commission to receive and follow up on complaints and conduct investigations.

The penalties the Commission may enforce are substantial. The fines are classified into Higher Maximum Amount (in the case of a data processor/controller of Major Importance) and Standard Maximum Amount in the case of a data processor/controller not of Major Importance). The fine of Higher Maximum Amount is the

greater of #10,000,000 (Ten Million Naira) and 2% of its annual revenue in the preceding financial year, while the fine of the Standard Maximum Amount is the greater of #2,000,000 (Two Million Naira) and 2% of its annual revenue in the preceding financial year.

A data controller/processor who is not satisfied with the Commission's orders has its right to judicial review reserved in section 50. Also, data subjects who suffer harm due to violations of the Act can seek damages through civil proceedings. In cases where a data controller or individual is convicted of an offense, the court can order the forfeiture of assets under relevant laws.

In contrast, the NDPR does not have specific provisions related to enforcement. It primarily focuses on penalties for breaches of data privacy rights, based on the number of data subjects involved and the annual gross revenue of the data controller. The Nigerian Data Protection Regulation Implementation framework, however, provides in Reg 10.0 for various forms of enforcement such as surveillance, compliant filing, investigation, a notice of enforcement/; administrative

penalties, and criminal prosecution for defaulting organizations pursuant to Article 4.2 of the NDPR 2019 and section 17(1) and (3) of the NITDA Act 2007.

11. Provisions on Legal Proceedings: Part

12 of the NDPA provides clearer guidelines for legal proceedings, enforcement actions, investigation powers, and representation in civil proceedings, as opposed to the NDPR. The NDPA makes provision for a limitation period of 3 months, from the date of any act, neglect or default, to institute an action against the Commission, a member of Council or its Staff. The Act also provides that actions can only be instituted against the Commission, a member of Council or its staff, after a pre-action notice of 1 month has been issued. The Act also clarifies that notices and other documents can be served by delivering them to the National Commissioner at the Commission's Head Office.

In terms of execution or attachment process, the Act specifies that no such process shall be issued against the property of the Commission in relation to an action or suit. Any awarded sum of money shall be paid from the Commission's Fund, and the

Commission is responsible for indemnifying its officers against losses incurred in the execution of their duties.

The Act empowers the Commission to apply for a warrant to obtain evidence in investigations related to the Act. A judge may issue a warrant based on grounds such as the commission or prevention of offenses, data security breaches, obtaining electronic evidence, or preparing to commit an offense.

The warrant grants the Commission powers to enter and search premises, stop, and search conveyances, seize, or detain evidence, use computer technology, and require the production of computers or electronic devices. As regards representation in civil proceedings, the Act allows a legal officer of the Commission, or a private legal practitioner engaged by the Commission to represent it in matters relating to its business or operations.

These provisions in the NDPA expand and provide clearer guidelines for legal proceedings, enforcement actions, investigation powers, and representation in civil

proceedings, which were not explicitly covered in the NDPR.

NOTABLE LIMITATIONS OF THE NIGERIA DATA PROTECTION ACT

1. **Unclear status of Nigeria Data Protection Regulation and the Nigeria Data Protection Regulation Implementation Framework:** Section 64(2)(f) preserves all current rules and regulations passed by NITDA and NDPB, as if they were passed by the NDPC. It is worth noting that certain provisions of the NDPR and the NDPA are in conflict. Thus, in a bid to provide for a transitional provision that adopts the acts, powers, liabilities etc., of the Nigeria Data Protection Bureau (NDPB) by the NDPC, the Act creates a confusion as to the status of the of the NDPR and does not clearly provide for an instance of conflict with existing laws or regulations.
2. **Definition of Terms:** The terminologies and concepts used in data protection are unique and do not always align with their common usage. Unfortunately, the Act does not provide definitions for many terms, such as anonymisation, cross-border transfer, data portability, DPCO, recipient, legitimate interest, genetic data, profiling, and third party. These omissions leave stakeholders to adopt various suitable definitions, thus affecting unanimity in certain interpretations of part of the law.
3. **Unclear Jurisdiction for Adjudicating Disputes in Data Protection Cases:** The issue of jurisdiction is commonly contested in our case law, and the lack of clarity in defining the court with jurisdiction to handle disputes arising from the Act is a potentially contentious issue. The word court in the Act is defined vaguely as "any court of competent jurisdiction". This confusion could have been avoided by explicitly defining the court as a specific court in Nigeria.
4. **Independence of Data Protection Officers (DPOs):** Section 32 of the Act requires data controllers of Major Importance, domiciled in Nigeria, to have a Data Protection Officer (DPO). The DPO can be an employee or engaged through a service contract. Questions may arise as to the independence of the DPO, as they are expected to report to the data controller while also being a contact point for the Commission.

It is suggested that the Act could have better safeguarded the status of the DPO by requiring Commission's approval/notice for DPO appointments/removal, thus safeguarding the role of the DPO, and avoiding unfair play from a data controller/processor. These safeguards would encourage companies to take the DPO role more seriously and ensure internal compliance.

CONCLUSION

Overall, the Nigerian Data Protection Act, 2023, provides more comprehensive provisions relating to data protection. Its provisions are more encompassing when compared with the Nigeria Data Protection Regulation, 2019, The Nigerian Data Protection implementation framework, and the provisions of the Nigerian Information Technology Development Agency (NITDA) Act of 2007.

It strengthens the legal framework for data protection in Nigeria, and contains provisions which enhance data protection practices, regulatory oversight, and transparency in Nigeria's data processing landscape. Furthermore, its provisions expand and provide clearer guidelines for legal proceedings, enforcement actions,

investigation powers, and representation in civil proceedings, which were not explicitly covered in the old Nigerian Data Protection Regulation, 2019.

Its enactment suggests an effort on the part of the government to adapt to the evolving challenges of data protection and align with international standards. It is, however, important that sufficient emphasis be placed on public awareness and education is made to ensure that individuals and organizations are made aware of their rights under the Act.

Finally, we look towards the successful implementation of the provisions of the Act and the regulations and guidelines to follow, from the Commission, in order to implement and provide directives as to the application of certain provisions of the Act.





AUTHORS



Christian Aniukwu
Managing Partner



Chizitereihe Oti
Associate



Ibitola Akanbi
Associate



Chidinma Anuforo
Associate

THE FIRM

Stren & Blan Partners is an innovative and dynamic law firm with a compelling blend of experienced lawyers and energetic talents. Our lawyers are available to provide you with guidance and innovative solutions on complex business and legal issues across a variety of sectors.

This is a publication of Stren and Blan Partners and it is for general information only. It should not be construed as legal advice under any circumstances. For more information about the firm and its practice areas, please visit www.strenandblan.com. You can also contact us via contact@strenandblan.com or call +234 (0) 702 558 0053.