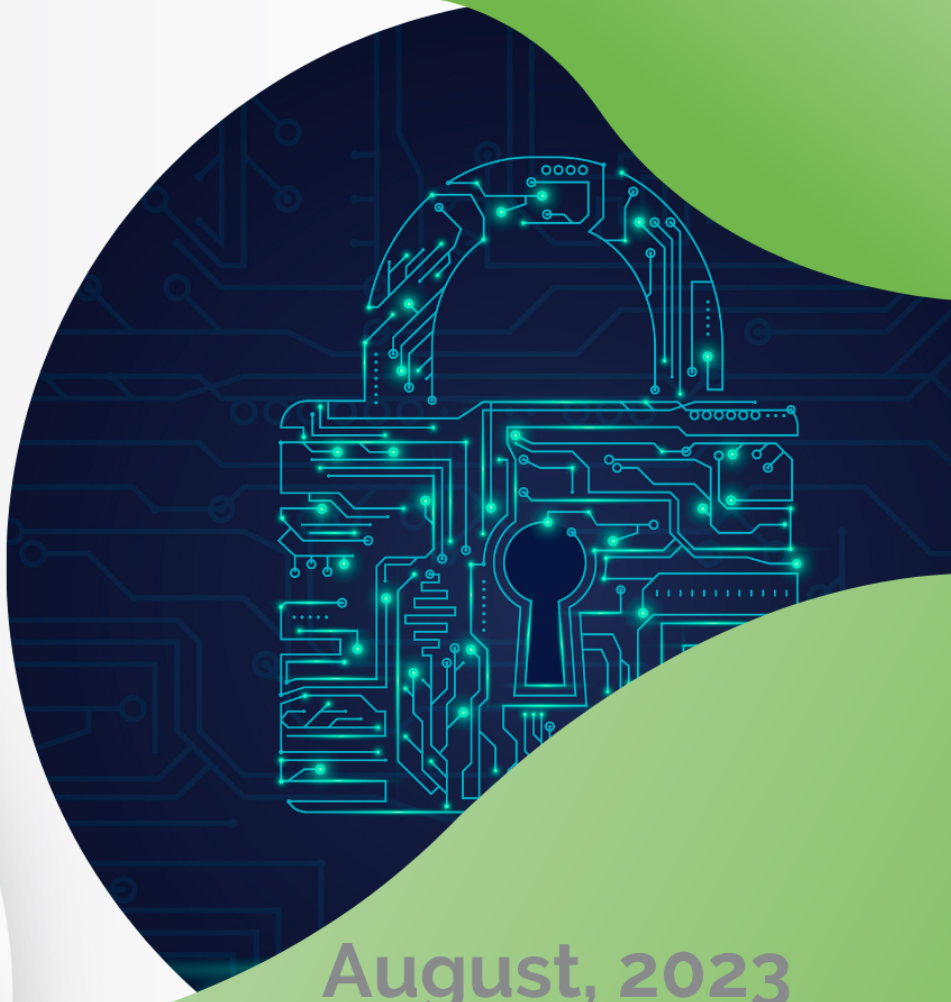
TLP ADVISORY

The Nigeria Data Protection Act, 2023



Client Briefing Note

August, 2023

TLP ADVISORY

Table of Content

Overview

On 14 June 2023, Nigeria passed the Data Protection Bill into law. With the enactment of the Data Protection Act 2023 (the "Act"), Nigeria joins the list of African Countries with substantive legislation focused on data protection. Prior to the Act, the handling and processing of personal data in Nigeria was governed by the Nigerian Data Protection Regulation (NDPR), which had limited provisions, a reflection of the fact that it was not an act of the National Assembly but a subsidiary legislation largely informed by the establishment act of the Nigerian Information Technology Development Agency (NITDA).

Since its enactment, the Act has been received with enthusiasm, particularly by data experts and other affected organisations, who predict that it will clarify the grey areas that the NDPR could not address, make Nigerian businesses more attractive to foreign investors, and strengthen the country's position in the global economy.

This Briefing Note provides insights into the changes the Act makes to the data protection ecosystem that you should be aware of and comply with when handling personal data in Nigeria.

Who Does The Act Apply To?

The Act generally applies to data controllers (organisations or individuals that determine the process or purpose of processing personal data), data processors (organisations or individuals that process data on behalf of a data controller or another data processor), and data subjects (individuals to whom personal data relates). Nevertheless, the following questions will help determine whether you have obligations under the Act:

a. Are you or your organisation resident or domiciled in Nigeria?
b. Are you or your organisation resident or domiciled abroad, but the data subjects reside within Nigeria?
c. Is the data processing done within Nigeria?

If the answer to any of the above questions is “Yes”, then the data processor must comply with the provisions of the Act. The Act will, however, not apply where personal data is being collected or processed by individuals for personal or domestic purposes that do not violate the data subject's fundamental rights to privacy, e.g. a guest list for a family event.

Is There a New Regulator?

YES! The Act establishes the Data Protection Commission (the “Commission”), which replaces the National Data Protection Bureau and takes on its functions. The Commission is responsible for implementing the provisions of the Act as well as monitoring and supervising data controllers and data processors in the country. The administrative and regulatory processes, including reporting, filings, applications, payments, et al., will now be made to the Commission.

The Commission is empowered to receive complaints from data subjects, investigate the activities of data controllers and data processors, and impose sanctions on defaulting parties.

What Else is New?

Registration of data controllers and processors (Section 44)

The Act provides that all existing data controllers and data processors of major importance must register with the Commission within six months of the commencement of the Act, i.e., by or before 31 December 2023.

The Act defines data controllers and processors of major importance as those who are resident, domiciled, or operating in Nigeria and who process the data of a certain number of subjects exceeding an amount to be determined by the Commission or who process a class of personal data that the Commission may regard as being of ‘particular value’ or ‘significance’ to the economy, society, and security of Nigeria.

The omission of a specific threshold in the Act is a prominent departure from the NDPR, which had varying compliance obligations for data controllers that handled the personal data of more than 1,000 data subjects and for data controllers that processed the personal data of less than 2,000 data subjects. The NDPR also based its sanctions on the amount of personal data processed by the data controller. Data controllers who handled the personal data of more than 10,000 data subjects were, in the event of default, liable to different penalties than

data controllers who handled the personal data of fewer than 10,000 data subjects.

Under the Act, potential data processors and controllers also have the obligation to register with the Commission within six months of the commencement of business operations as a data controller or data processor of major importance.

As part of the registration requirements, data controllers and processors are required to disclose to the Commission the nature, purpose, and number of personal data being processed, etc. Additionally, the data processors or controllers of major importance also have the obligation to notify the Commission of any subsequent changes to the information submitted during registration within 60 days of the change.

Processing the Data of Children and Special Persons (Section 31)

Similar to its predecessor, the Act contains ample provisions on the processing of data on children and persons unable to provide legal consent. Section 31 of the Act states explicitly that, except in particular circumstances, when processing the personal data of a child or a person without the capacity to give consent, the controller or processor must obtain the permission of their parent or legal guardian.

In the course of handling the data of children, data processors and controllers are required to use the available technology to provide and implement age verification and consent collection mechanisms.

Section 31 (4) of the Act provides that data controllers and processors are exempted from the obligation to procure the consent of a parent or guardian where the data is being processed for any of the following reasons:

- The protection of the vital interests of the data subject
- The provision of educational, medical, or social care services by a professional or service provider with a duty of confidentiality
- Proceedings before a court that involve the data subject

Section 31(5) provides that the provisions that cater to the processing of the personal data of children and persons incapable of giving consent are non-expansive as the Commission will issue further regulation on the subject, especially with regard to the processing of the personal data of a child aged at

least 13 in relation to the digital provision of information and services at the request of the child.

Legitimate interest (Section 25)

Section 25 of the Act makes a prominent change to the data processing ecosystem with the introduction of legitimate interest as a basis for data processing. Legitimate interest was conspicuously absent from the NDPR.

With the introduction of legitimate interests, data processors and controllers (and third parties acting on their behalf) are permitted to process data if the processing is necessary to carry out tasks related to their business activity.

For instance, if data needs to be processed to prevent fraudulent or criminal activity, such data may be processed on the basis of legitimate interest. However, data processors and controllers are not given blanket permission to process personal data for the purpose of legitimate interest. Such processing is not permitted where the processing:

- conflict with the fundamental rights, freedoms and interests of the data subject,
- Is incompatible with other lawful bases of processing,
- could not have been reasonably expected by the data subject.

Reporting Obligations

Unlike the NDPR, the Act provides that in the event of a breach, data processors and controllers have the obligation to notify the Commission of the breach and provide, as much as is feasible, details of the nature of the breach, including the categories and number of data subjects and personal data records impacted.

Penalties

The Act introduces very robust provisions for non-compliance. The most prominent of these are the higher penalty thresholds for defaulting data processors and controllers. Unlike the NDPR, which pegged the penalties to be paid to the extent of default, the Act provides that the penalties to be paid by the errant data controller or processor will be based on its qualification as a controller or processor of “major importance” or otherwise.

According to Section 48(2), an errant data controller or processor of major importance would be required to pay a penalty of ₦10,000,000 (Ten Million Naira) or 2% of its annual gross revenue in the preceding financial year, whichever is higher. Other data controllers or processors would pay a penalty

of ₦2,000,000 (Two Million Naira), or 2% of the annual gross revenue in the preceding financial year.

The penalty provisions are a significant departure from the NDPR, as these provisions introduce upwardly reviewed percentages and grant data subjects the right to sue non-compliant data controllers or processors for damages.

Non-compliant data processors and controllers may also be subjected to judicial proceedings and sentenced to a prison term of not more than 1 year in addition to the payment of the penalties.

Vicarious Liability for Data Processors and Data Controllers

The Act saddles data controllers or processors who engage the services of third-party data processors with the obligation of ensuring that the engaged data processor complies with the obligations that the data controller or engaging processor is bound by under the Act.

The Act also mandates that the engaging data processor or data controller and engaged party execute a written agreement that reflects the full extent of the recruiters' compliance obligations under the Act.

Data Protection Officers (Section 32)

The Act creates a range of obligations for data controllers of major importance. A significant obligation is the requirement to engage the services of a Data Protection Officer (the "Officer"). Data controllers are required to engage an Officer with expert knowledge of data protection legislation and practices as well as the ability to ensure compliance with statutory obligations.

The Act also states that the Officer has to be engaged under a contract of employment or service contract. The Act also goes beyond this to define the functions of the Officer. The duties of the Officer include the following:

- Advising the data controller or the data processor and their employee on the extent of their obligations under the Act
- Monitoring compliance with the act and related policies
- Interfacing with the Commission on behalf of the data processor or controller.

The Officer is required to have robust knowledge of data protection legislation and practices as well as the ability to carry out the compliance obligations created by the provisions of the Act.

Additional Rights of Data Subjects

Data subjects under the Act now have the right to object to the processing of their data, mainly where it is processed for direct marketing purposes; they are also entitled to file complaints against a processor of their data at the Commission.

Data subjects can now request that the data processor deliver, transfer, or transmit their data in a structured and machine-readable form to themselves or another data processor without delay.

Data Privacy Impact Assessment

Considering the sensitive nature of personal data, the Act provides safeguards that cater to the sensitive nature of personal data. The Act provides that where a data controller suspects that the processing of certain personal data would likely result in a high risk to the rights and freedoms of a data subject, a data privacy impact assessment has to be carried out before the personal data is processed.

The assessment is tailored to the relevant risk and elements such as the purpose for which the personal data is to be processed, the legitimate interest pursued by the processor, the necessity of the processing relative to the purpose for which the data will be processed, the proposed measures to address the risks to data subject rights, etc.

After the impact assessment is completed, if the results indicate that the processing would threaten the rights of data subjects, then the data controller must consult the Commission before processing.

International Data Transfers (Sections 41 and 42)

The Act has eliminated the pre-transfer obligation of obtaining the consent of the Attorney General of the Federation prior to the cross-border transfer of personal data.

The Act generally prohibits the transfer of personal data abroad unless the recipient has binding corporate rules, contracts, codes of conduct, or certification mechanisms in place that would ensure that the data receives an equal or better level of protection than the Act provides; the Act describes this safeguard as “Adequate Protection”.

Data controllers and processors are also required to document the basis or purpose of transferring the data to a foreign country and assess the data protection framework in the receiving country.

For a transfer to occur without fulfilling the Adequate Protection condition, the controller or processor must obtain informed and unwithdrawn consent from the data subject, or a contract requiring such a transfer must exist between the controller or processor and the data subject. The Act lists other grounds for transferring personal data abroad, including transferring in the public interest, in the data subject's interest, and where obtaining the subject's data is reasonably impracticable.

Processing Data Not Obtained Directly

Before a data controller obtains the data of a subject in a way other than directly from the subject, the controller must notify them of certain information, including the controller's identity and place of business, the recipient of the personal data, their right to lodge a complaint against the controller, any automated decision-making and profiling, etc.

Sensitive Personal Data

Sensitive personal data includes all data relating to a person's race or ethnicity, biometrics or genetics, religious beliefs and psychology, health, sexuality, political opinions and affiliations, etc.

The Act has taken a firmer stance than previous data protection laws on the standard of care for the sensitive personal data of data subjects by providing that sensitive personal data must not be processed unless the data subject gives unwithdrawn and purposeful consent or under other explicit exceptions provided within the Act.

Data Retention Policy

Data controllers and data processors are now required to have a data retention policy that states the period in which the personal data collected and processed will be retained and must communicate the same to the data subjects before collecting their data. This can be made as a separate policy from a data processor's privacy notice or integrated into the notice.

Conclusion

The Data Protection Act makes significant changes to the data protection landscape. The ripple effect of these changes creates a range of obligations and rights for data subjects, processors, and controllers.

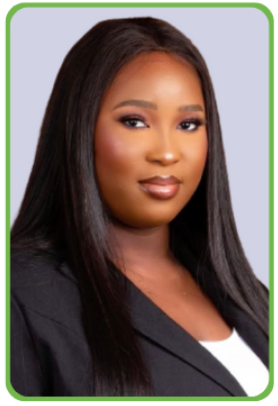
Unarguably, the Data Protection Act expands on the limited provisions of the NDPR and makes much-needed changes to the data protection ecosystem, especially with its focus on the actions and activities of data controllers and processors.

The transitional provisions of the Act provide for the continuation of the provisions of the NDPR. In view of the scope of changes introduced by the Act, the co-existence of the NDPR and the Act may result in ambiguity and conflict in the months ahead. We believe the Commission will issue explanatory circulars and regulations to resolve these discrepancies.

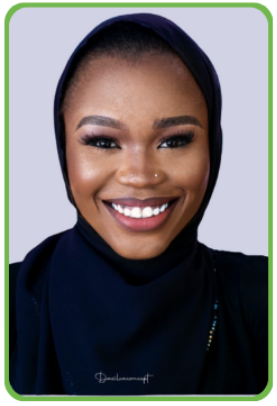
We, at TLP Advisory, are able to address any questions or concerns you may have, as well as help you and your business understand and navigate the changes introduced by the Data Protection Act. We can be reached via email at **info@tlpadvisory.com** and look forward to hearing from you.

TLP ADVISORY

The Authors



Emmanuella Boluwatife Keshinro
Associate
TLP Advisory



Maryam Oluwatoyin Jimoh
Associate
TLP Advisory

Daniel Igiekhumhe
Associate
TLP Advisory