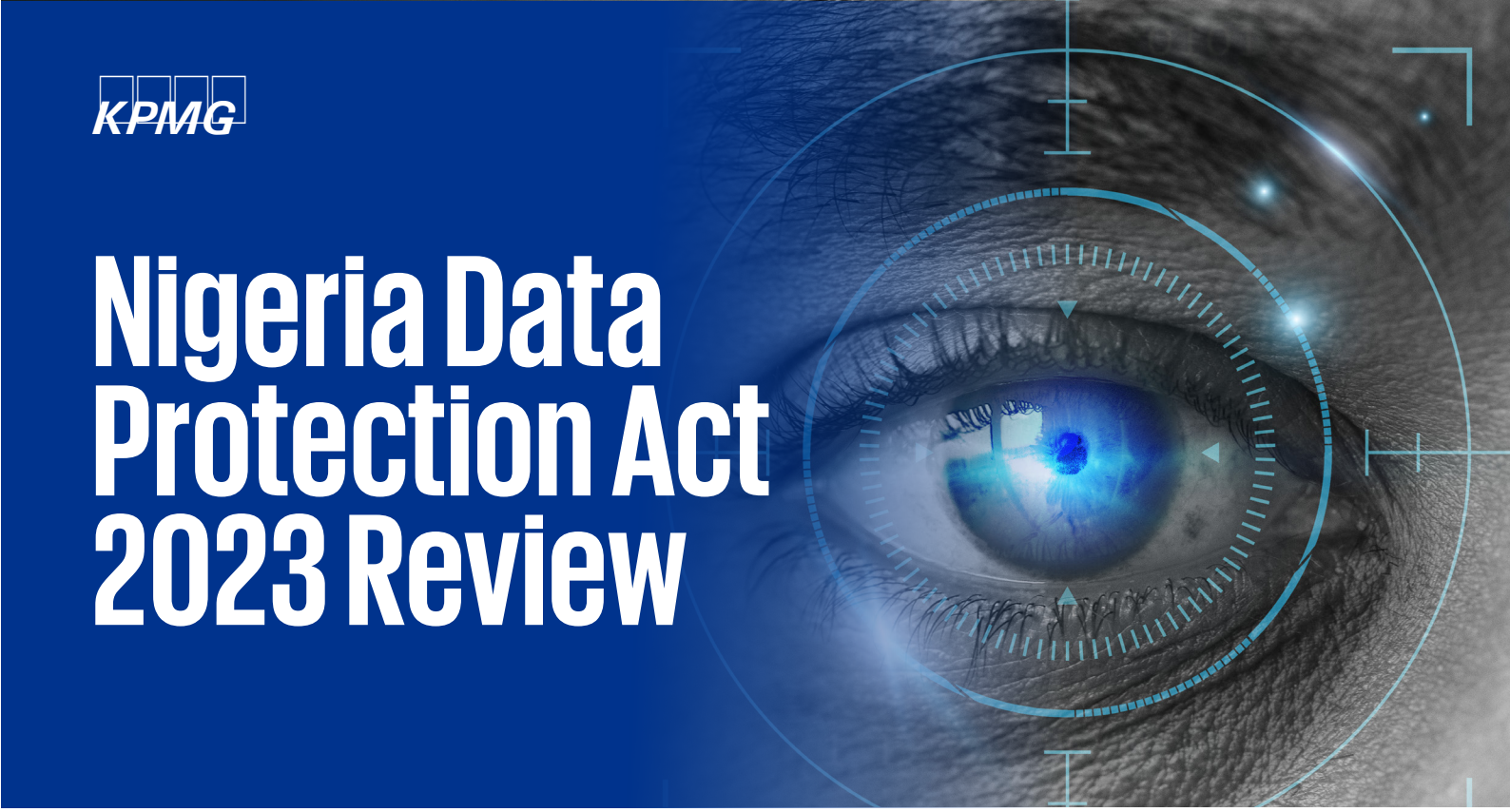
KPMG

Nigeria Data Protection Act 2023 Review



Overview

The need for strong data protection measures has never been more pressing in an age where personal data has replaced oil as the new currency. Significant accomplishments and steadfast efforts have distinguished Nigeria's progress toward comprehensive data protection regulation. The Nigeria Data Protection Regulation (NDPR) which was published in 2019 and the Nigeria Data Protection Bureau (NDPB) which was established in 2022 were significant advances in this direction. To address the issues with the developing data protection and privacy landscape, stakeholders have long called for more comprehensive and enforceable legislation.

On 14 June 2023, President Bola Ahmed Tinubu signed into law, the Data Protection Act, 2023. The objective of the Act, amongst others, is to safeguard the fundamental rights and freedoms and the interests of data subjects as guaranteed under the 1999 Constitution of Nigeria. The Act establishes the Nigeria Data Protection Commission (NDPC), also referred to as the "Commission", to replace the Nigeria Data Protection Bureau (NDPB) established by former President Muhammadu Buhari.

Unveiling The Nigeria Data Protection Act 2023

The Act comprises twelve (12) parts, i.e., Part I to Part XII. The first four (4) parts focus on the details of the Commission and its structure, and Part V to Part VIII emphasize the Data Protection Principles and relevant implementation requirements. Part IX highlights the Registration of Data controllers and data processors of major importance, while Part X and XI focus on Enforcement and Legal Proceedings. Finally, Part XII highlights the miscellaneous provisions of the Act.

This review highlights the different focus areas of the Act and draws comparison with the NDPR where applicable. We have also provided our points of views on certain aspects of the Act, particularly where data controllers and processors may need to look out for additional regulatory guidelines from the Commission.

Key provisions of the Act and its potential impact on data controllers, processors, and subjects.

Application of the Nigeria Data Protection Act, 2023

The Act applies to Data Controllers and Data Processors domiciled, ordinarily resident or ordinarily operating in Nigeria, or where the processing of personal data occurs within Nigeria. The Act also applies to data controllers or data processors not domiciled, ordinarily resident or ordinarily operating in Nigeria, so long as they are processing personal data of data subjects in Nigeria. This is unlike the NDPR which focuses on natural persons residing in Nigeria or Nigerians residing outside Nigeria.

In addition, the Act provides the boundaries of applicability by exempting activities carried out solely for personal or household purposes and various activities carried out by competent authorities. The Act also empowers the Commission to create further exemptions by regulation.

Lawful Bases for Processing Personal Data

Section 25 of the Act highlights the necessary conditions for the lawful processing of personal data. A notable provision of the Act is the addition of **legitimate interest** as a basis for processing personal data. This implies that Data Controllers or Data Processors can justify the processing on grounds of legitimate interest e.g., data

processing for fraud prevention. It is important to note that Legitimate Interest will not be lawful when:

- they override the fundamental rights, freedoms, and interests of the data subject,
- they are incompatible with other lawful bases of processing,
- the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

Data Privacy Impact Assessment (DPIA)

The Act has made significant improvements on the NDPR regarding the performance of a DPIA. The Act mandates the Data Controller to consult the Commission prior to the processing, if, notwithstanding the adoption of relevant measures, the outcome of the DPIA indicates that the processing of the data would result in a high risk to the rights and freedoms of data subjects.

Sensitive Personal Data

The Act defines sensitive personal data as data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records, or any other sensitive personal information. Unlike the NDPR, the Act further sets out several criteria for processing sensitive personal data. It says without prejudice to the principles set out in the Act, a data controller or data processor shall not process, or permit a data processor to process on its behalf, sensitive personal data unless the:

(a) data subject has given and not withdrawn consent to the processing for the specific purpose or purposes for which it will be processed;
(b) processing is necessary for the purposes of performing the obligations of the data controller or exercising the rights of the data subject under employment or social security laws or any other similar laws.

The Act also states that the Commission may issue directives prescribing further categories of personal data that may be classified as sensitive personal data.

Children Rights

The NDPR and NDPR Implementation Framework established that a child shall be any person below thirteen (13) years. They also mandated that Data Controllers or Processors whose processing activity targets children shall ensure their privacy policy is made in a child-friendly form with the aim of making children and their guardians a clear understanding of the data processing activity before granting consent. On matters relating to Children's Rights, Section 31 of the Act states that where a data subject is a child or a person lacking the legal capacity to consent, a data controller shall obtain the consent of the parent or legal guardian, as applicable. The Act also mandates Data Controllers to apply appropriate mechanisms to verify the age and consent as the case may be.

Data Security

Section 2.6 of the NDPR emphasizes the need for Data Controllers and Data Processors to protect personal data processed. While the Regulation highlighted some general measures that could be adopted, the Act takes it further by expanding on these measures for ensuring data security (Section 39 (2)). These include processes for timely restoration of data in the event of an incident, periodic risk assessment of systems and services, regular testing, assessment and evaluation of effectiveness of measures against current and evolving risks, amongst others.

Rights of a Data Subject

The NDPR had made provisions concerning the rights data subjects could exercise over their personal data (Section 3.1). An example of such is the right of data subjects to data portability, where a data subject had the right to request a transfer of personal data from one data controller to another.

In the NDPR, this right was not formally established. Specifically, in Section 38 of the Act, the Commission has clarified that regulations may be developed in the future which would establish this right and define the modalities upon which data subjects can invoke this right and the obligations of data controllers as well.

Data Breach Reporting/Communication

For personal data breaches, while the requirements to report breaches to the Commission within 72 hours from discovery have been maintained in the Act (Section 40 (2)(3)), the Commission now has the authority to make a public communication about a personal data breach where it considers the steps taken by the data controller to inform data subjects inadequate (Section 40 (5)).

Data Controllers and Data Processors of Major Importance

Unlike the NDPR, the Act has defined a new category of Data Controllers and Data Processors, called "Data Controllers and Data Processors of Major Importance" as defined in Section 65. The Act emphasizes that the class of personal data processed by such Data Controller or Data Processor must be of significant value to the economy, society, or security of Nigeria. Organizations that do not fall under this category are called "data controllers or data processors not of major importance".

In addition, the Act has mandated that Data Controllers and Data Processors of major importance register with the Commission within six (6) months of the Commencement of the Act, as stated in Section 44 (1). If there are any significant changes to the information submitted during registration, the Commission should be notified within 60 days of such change. Organizations under this category should also note that the Commission may prescribe fees or levies to be paid.

Furthermore, the Act mentions that the Commission shall maintain and publish on its website, a register of duly registered Data Controllers and Data Processors of major importance.

Enforcement

The Commission may initiate an investigation of its own accord where it has reason to believe a Data Controller or Data Processor has violated the Act, as stated in section 46(3). The Act also emphasizes comprehensively, the rights of a data subject. For instance, a data subject who suffers injury, loss, or harm as a result of a violation of this Act by a Data Controller or Data Processor, may recover damages from such data controller or data processor in civil proceedings as stated in section 51. Similarly, an enforcement order may be imposed on the data controller or data processor to pay compensation to a data subject who has suffered injury, loss or harm as a result of a violation.

In addition, penalties for breach of the Act have been broken down for Data controllers of major importance and Data Controllers not of major importance. as follows:

- Whichever is greater between **₦10,000,000** and **2%** of the Revenue of the Preceding Year- for Data Controllers or Data Processors of **major importance**
- Whichever is greater between **₦2,000,000** and **2%** of the Revenue of the Preceding Year- for Data Controllers or Data Processors **not of major importance.**

In addition to the fine above, the data controller or processor may face imprisonment for a term not more than one year or both.

Provision of Information to Data Subjects

Section 2.5 of the NDPR outlines the relevant information that data subjects should be provided with, typically through a privacy policy, before their personal data is obtained.
The Act expands on the NDPR requirement by mentioning more specific information that should be included in the privacy policy presented to the data subject such as the:

- Identity and Residence of business (of a data controller)
- Means of communication with the data controller and its representatives, where necessary;
- Recipients or categories of recipients of the personal data, if any.

Data Transfer to a Foreign Country

The Regulation (Sections 2.11,2.12) and the Act (Sections 41-43) largely align on the conditions for transferring personal data to a foreign country.

However, the Act (Section 41(2)) requires that the Data Controller records the basis relied upon to transfer personal data outside the country.

Further regulations may also be released by the Commission that would require data controllers and data processors to notify the Commission of the bases relied upon to transfer personal data.
Additionally, regulations that identify certain categories of personal data where additional specified restrictions would be enforced, based on their nature and possible risks to data subjects, may also be released by the Commission.

The Implementation Framework of the Regulation makes a special mention of 'whitelisted' countries which were adjudged to have adequate data protection laws (Annexure C). However, the Act is silent on these whitelisted countries but only mentions the presence of an adequate data protection regulation as part of the criteria for assessing the adequacy of protection (Section 42(2)(d)). We await further guidance from the Commission on the viability of the whitelisted countries in the Implementation Framework of the Regulation.

Commentaries

The establishment of the Nigeria Data Protection Act 2023 demonstrates the new posture of the Federal Government to hit the next gear in relation to ensuring all organizations in the scope of the Act, obtain and process personal data in line with best practices.
The Commission is also now fully vested with the authority to enforce compliance with this Act. This emphasizes the need to take compliance with this Act very seriously to reduce the exposure of attracting fines, sanctions, convictions, etc. Organisations should endeavour to review the Act carefully to better understand and comply with it.

In conclusion, here are other key points to consider:

- Section 64(f) of the Act states that all orders, rules, regulations, decisions, directions, licenses, authorizations, certificates, consents, approvals, declarations, permits, registrations, rates, or other documents that are in effect before the coming into effect of the Act and that are made or issued by the National Information Technology Development Agency (NITDA) or the NDPB shall continue in effect as if they were made or issued by the Commission until they expire or are repealed, replaced, reassembled or altered. This implies that the NDPR mandated **annual data protection audit** which Data Controllers and Data Processors are expected to undergo, is to continue except the Commission issues regulations that state otherwise.

- As stated in the Act, further guidelines may be established or released for some of the principles of data protection. For example, the Act does not explicitly state organisations that are data controllers and data processors of major importance. However, emphasis was laid on the **significant** number of data subjects processed, as it relates to the Nigerian population which could be associated with certain public sector organisations and private organisations such as leading Telecommunications companies and top-tier commercial banks.

- We advise that the measures of data security stated in Section 39(2) of the Act are taken as minimum requirements and should not be adopted as a boundary to efforts in protecting personal data.

- While oral consent appears valid under the Act, it should be noted that the Act emphasizes that the burden of proof lies with the Data Controller. Hence, the approach and mechanism of obtaining and documenting oral consent should be carefully considered.

For feedback and enquiries, please contact:

John Anyanwu
Partner & Head, Cyber & Privacy
KPMG in Nigeria
T: +234 803 975 4061
E: john.anyanwu@ng.kpmg.com

Olaoluwa Agbaje
Senior Manager, Cyber & Privacy,
KPMG in Nigeria
T: +234 805 032 8055
E: olaoluwa.agbaje@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia

Download KPMG NIgeria Tax Mobile App: