KPMG

The Nigeria Data Protection Act, 2023

A Review of the Key Compliance Provisions and their Implications for Nigerian Businesses

September 2023

home.kpmg/ng

Contents

On 12 June 2023, President Bola Ahmed Tinubu, GCFR, signed the Nigeria Data Protection Bill, 2023 into law as Nigeria Data Protection Act, 2023 ("the Act" or "NDPA"). The Act establishes the legal framework for the regulation of personal data in Nigeria and replaces the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019 issued under the National Information Technology Development Agency (NITDA) Act.

The key provision of the Act is the establishment of the Nigeria Data Protection Commission (NDPC or "the Commission") and a Governing Council ("the Council") of the Commission. The Commission will superintend the implementation and enforcement of rules and regulations set out in the Act, regulate the processing of personal information and other related matters, while the Council is charged with formulation and provision of overall policy direction of the affairs of the NDPC.

This Newsletter analyses the implications of the NDPA for businesses operating within and outside Nigeria, including best practices for compliance.

1. Objective of the Act

In today's interconnected world, data plays a pivotal role in shaping decisions and driving actions. Safeguarding information has become very important to governments and regulators due to its significant likelihood of containing personal data, and to ensure that it is not misused. As a result, many countries have enacted laws that ensures data protection is a fundamental human right, and Nigeria is no exception. The nation's commitment to individual privacy and security is evident in Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) ("the 1999 Constitution"), which explicitly guarantees citizens right to privacy. This provides the foundation for Nigeria's legal framework on data privacy and protection.

Based on the above, the key objectives of the Act include:

i. safeguarding the fundamental rights and freedoms and the interests of data subjects[1] as guaranteed under the 1999 Constitution;

ii. regulating the processing of personal data;

iii. promoting data processing best practices that safeguard the security of personal data and the privacy of data subjects;

iv. protecting the rights of data subjects and providing means of recourse and remedies, in the event of the breach of the data subjects' rights;

v. ensuring that data controllers/ processors[2] fulfil their obligations to data subjects;

vi. strengthening the legal foundations of the national digital economy, and

vii. guaranteeing Nigeria's participation in regional and global economies through beneficial and trusted use of personal data.

[1] The NDPA defines a "data subject" as anyone to whom personal data relates to, or that can be identified through the personal data.

[2] The NDPA defines a "data controller" as 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. It also defines a "data processor' as 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 processor.

2. Scope and Application

The scope of the Act is centred on data controllers and data processors engaged in the processing of personal data of subjects within Nigeria; and applies to entities domiciled, resident, or operating within Nigeria. The Act also covers data controllers or data processors outside Nigeria who process personal data of Nigerian data subjects. This provision differs from the NDPR 2019 Regulations and Implementation Framework which focused on individuals residing in Nigeria or Nigerians residing outside Nigeria.

However, the Act does not apply to processing of personal data by individuals exclusively for personal or household purposes, provided that such processing for personal or household purpose does not violate the fundamental right to privacy of the data subject.

Further, subject to the rights and freedom under the 1999 Constitution, a data controller or data processor is precluded from the provisions of the Act if the personal data processing is:

i. carried out by a competent authority for the purposes of prevention, investigation, detection, prosecution, or adjudication of criminal offence or the execution of a criminal penalty; or control of national public health emergencies; or national security.

ii. for public interest publications (such as journalism, education, art, literature) to the extent it conflicts with obligations and rights of data subjects, or

iii. necessary for establishing, exercising, or defending legal claims in court, administrative, or out-of-court proceedings.

The Act also empowers the NDPC to issue regulations to establish further exemptions where necessary.

3. Impact Analysis

We have analysed below, how the Act may apply to businesses that control and/or process personal data of Nigerian subjects.

3.1 Part V – Principles and Lawful Basis of Processing Personal Data

3.1.1 Principles of personal data processing

The Act provides the following six (6) key principles for the processing of personal data by data controller and data processor:

i. personal data must be processed in a fair, lawful, and transparent manner. This means that businesses must communicate clearly with data subjects about the purposes and their methods of data processing.

ii. collection of data must be for specific, explicit, and legitimate purposes, and not be further processed in any way that is inconsistent with the original intent. This principle requires businesses to be more precise and transparent about their data collection practices. Therefore, affected companies may need to revise their existing data processing procedures to ensure that they comply with the provisions of the Act.

iii. personal data should be adequate, relevant, and limited to the minimum necessary for the purposes for which it was collected or processed. Consequently, businesses will need to ensure that they collect only the data required for the stated purpose, limiting the risk of holding unnecessary and potentially sensitive information. To ensure compliance, businesses must adopt a more targeted and streamlined approach in their data collection strategies to ensure that they only collect the needed data.

iv. the retention period for personal data should not be longer than necessary to achieve its lawful purposes. The implication of the retention principle is that businesses will need to establish clear data retention and deletion policies to ensure that they delete or anonymize data once it is no longer needed.

v. data must be kept complete, not misleading, and up to date. For businesses, this necessitates the implementation of data validation processes and periodic reviews of stored information to ensure its accuracy and completeness.

vi. consistent with the central objective of the Act, businesses are required to process data in a manner that ensures appropriate protection against unauthorized or unlawful processing, access, loss, destruction, damage, or data breaches. This would require data controllers and data processors to adopt robust security measures, including encryption, access controls, and other data protection mechanisms to ensure absolute security of data collected and/ or processed.

3.1.2 Legal basis for processing personal data

Businesses must carefully determine the applicable basis for their data processing and ensure valid legal justification. The Act provides several options regarding the lawful basis for data processing, including consent, contract performance, legal compliance, protection of vital interests, public interest, and notably, legitimate interest[3] which is a newly introduced legal basis for processing data.

However, the Act specifies that an interest will not be considered legitimate where the fundamental rights and freedom of a data subject override such interest, or where such legitimate interest is incompatible with 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.

Key considerations for processing of personal data.

a. Consent

Gaining valid consent from data subjects is another vital aspect of data protection specified in the Act. The Act stipulates that consent must be freely given, specific, informed, and clear. Consent should be affirmative and not based on pre-selected confirmations. It can be provided in writing, orally, or electronically, but it cannot be assumed from silence or inactivity. Therefore, businesses must re-evaluate their consent-gathering methods to ensure that they obtain explicit, unambiguous consent from the data subjects.

Given the digital landscape where most activities occur online, the Act prohibits the automation of decision-making in terms of obtaining consent. It, therefore, demands that each data subject shall have the right to accept or reject the provision of consent and shall have the right not to be subject to a decision based solely on the automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject.

The Act also addresses obtaining consent from children and/ or individuals that lack legal capacity. Specifically, the Act provides that where a data subject is a child or lacks legal capacity, the data controller must obtain consent from a parent or legal guardian. The data controller must employ suitable methods to verify age and consent, using available technology. Notably, the Act elevates child protection by raising the age defining a "child" to 18 years, in line with the Nigeria Child Rights Act. This contrasts with the NDPR Implementation Framework, which designates a child as under 13 years old.

[3] According to the General Data Protection Regulation issued by the European Union, in determining legitimate interest, the controller must demonstrate a valid purpose for data processing, ensure it is necessary for achieving that purpose, and assess whether the individual's fundamental rights and freedoms outweigh the controller's interests.

b. *Data Protection Impact Assessment*

The Act introduces the concept of Data Protection Impact Assessment (DPIA), a process designed to identify the risks and impact of processing personal data. This may involve systematically describing the envisaged processing and its purpose, assessing the necessity and proportionality of the processing in relation to the purpose, evaluating the risks to the rights and freedoms of a data subject; and outlining measures to mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data. The DPIA is crucial where the processing of personal data appears likely to result in a high risk to the rights and freedoms of data subjects by virtue of its nature.

Based on the Act, where a DPIA indicates that processing data would pose a high risk to the rights and freedoms of data subjects, the data controller must consult the NDPC before proceeding with the processing. This provision underscores the legislators' commitment to data protection and privacy rights. The DPIA is not a new concept under data protections laws. For example, Kenya Data Protection Act requires a DPIA to be conducted 60 days prior to the processing of personal data. Unfortunately, the NDPA does not specify a timeframe for conducting a DPIA prior to processing Nigerian data subjects. Therefore, we expect that this clarification will be provided in the Regulations to be issued by the Commission.

c. *Data Protection Officers/ Data Protection Compliance Experts*

The Act mandates data controllers of major importance who are domiciled, resident, or operating in Nigeria to appoint a Data Protection Officer (DPO) who has expert knowledge of data protection law and practices. The DPO will be responsible for providing expert opinion and guidance to the organisation on data protection matters and shall act as a contact point with the regulators.

The Act also empowers the NDPC to license individuals with expertise in data protection to monitor, audit, and report on compliance by data controllers and data processors with the provisions of the NDPA. This is to ensure continuous regulatory oversight and may lead to more frequent audits and inspections of businesses by the Commission.

3.2 Part VI – Rights of a Data subject

The Act establishes the data subject's right of access, ensuring their ability to request for and obtain information about the processing of their personal data. Consequently, data controllers are obligated to promptly and comprehensively respond to such request for access, and provide details about the processing purposes, data recipients, and the rights to rectify, erase, or limit data. The implication of the provision is that businesses may need to invest in efficient data management systems that can efficiently handle and process such requests by data subjects.

Although the Act provides for the right of access of data subjects, it did not define any comprehensive mechanisms for implementing these rights, such as the parameters and modalities to respond to data subjects requests. The Act, however, provides that *"a controller should ensure that it is as easy for the data subject to withdraw consent, as it is to give consent."* In the event of any breach of the rights of a data subject by data controller or data processor, data subjects can seek redress by filing complaints with the NDPC or initiating legal proceedings against the company.

Section 35 of the Act grants data subjects the right to revoke their consent to the processing of their personal data at any time. Similarly, Section 36 of the Act allows data subjects to contest processing of their data, particularly for direct marketing purposes. When consent is withdrawn by a data subject, businesses must halt data processing unless they can demonstrate overriding legitimate grounds.

The Act also provides for right to data portability. The nature and importance of data today makes it a tool of information that data controllers may often share with one another to further process data. Hence, the data portability right allows for a data subject to receive personal data concerning them from a data controller and transmit it to another controller, or for the data to be directly transferred from one controller to another. However, implementing data portability could pose technical and logistical challenges for businesses in terms of data format standardization and secure data transfers. A major importance of this right, given Nigeria's thriving Fintech ecosystem, has seen the Central Bank of Nigeria issue operational guidelines within the context of open banking accounts.

The Act further empowers the NDPC to prescribe the circumstances and conditions in which the data subject may exercise the afforded right, and the obligations it would impose on a data controller or data processor in enforcing such right. The Act places significance on the rights of data subjects such that data processors/controllers who in any way impinge on either of these rights, could face potential consequences, including financial penalties, civil lawsuits, or even the revocation of their license to collect personal data from the public. With the introduction of the NDPA and the statutory obligation placed on the NDPC to uphold citizens' data protection, there is a likelihood that its regulatory stance will become increasingly stringent.

3.2.1 Automated Decision Making

The Act also introduces the concept of Automated Decision Making (ADM), considering advancements such as machine learning, artificial intelligence, internet of things among others which have the ability to identify and simulate the data subject's digital footprints, and replicate

same. Based on clarification provided by the UK Government on data protection, ADM includes any process of making a decision by automated means without any human involvement. The decisions could be based on factual data, digitally created profiles or inferred data.

The NDPA has rightly recognised this form of data collection in this digital era where more people are seeking to generate traffic to their websites or products. The Act explicitly provides that a data subject shall have the right not to be subject to a decision based solely on ADM, including profiling, which produces legal or similar significant effects concerning the data subject. The Act further precludes data controller or data processor from collecting and/ or processing data obtained through ADM.

3.3 Part VII – Data Security

Part VII of the Act introduces crucial provisions concerning data security, which will significantly impact how businesses manage personal data of subjects. The Act emphasises the responsibility of data controllers and data processors to implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data. Therefore, businesses must consider the sensitivity and volume of data they handle and adopt measures that will mitigate potential harm to data subjects in the event of a breach. Such security measures include encryption, pseudonymization, regular risk assessments, and testing of security protocols to address evolving risks. Compliance with these provisions will necessitate significant investments in robust cybersecurity infrastructure and staff training to maintain data security effectively.

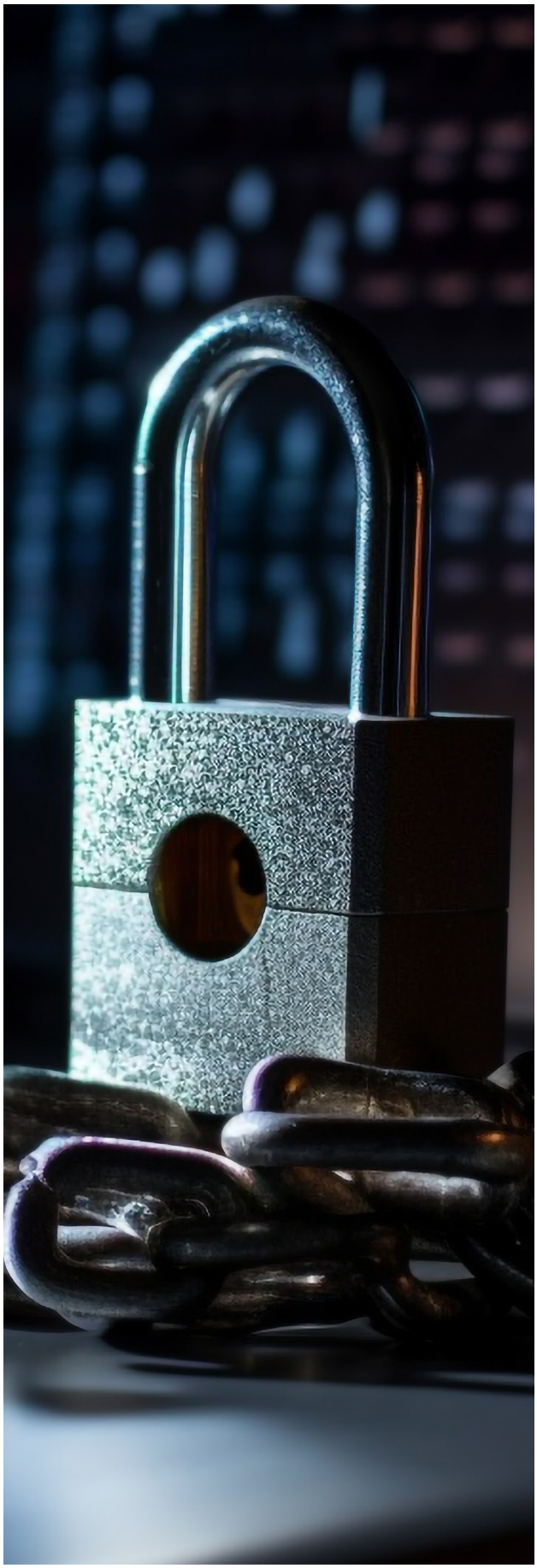
In the unlikely event of personal data breach, the Act provides stringent requirements that businesses must follow in addressing such breach. For example, data processors are required to promptly notify the data controller of any breach and provide necessary information to comply with data breach obligations. In turn, data controllers must report significant breaches that pose risks to individuals' rights and freedoms to the NDPC within 72 hours of the incident. Where a breach is deemed high risk, the data subjects must be informed immediately.

The implications of data breaches, such as reputational damage, legal penalties, financial risks and loss of client's trust, require that businesses must prioritize investments in robust cybersecurity infrastructure, encryption tools and data breach response plans, staff training, and awareness initiatives to foster a sturdy data security culture within the organization.

3.4 Part VIII – Cross border transfers of personal data.

The Act establishes guidelines for businesses in Nigeria regarding cross-border transfer of personal data. The provision prohibits data controllers and data processors from transferring personal data of Nigerian subjects to other countries unless the recipient country has adequate data protection laws, binding corporate rules, contractual clauses, a code of conduct, or certification mechanisms that align with the data protection principles stipulated in the Act.

Businesses will also need to obtain explicit consent from data subjects when transferring personal data to countries without adequate protection.



This requirement includes informing data subjects regarding the potential risks associated with such transfers. For data transfers based on other legal grounds, businesses must maintain transparent documentation and evidence to justify their compliance with the Act.

Section 43 of the Act outlines various other bases for transferring personal data outside Nigeria in the absence of adequate protection. These include obtaining explicit consent from the data subject after informing them of the potential risks, transferring data for the performance of a contract or at the data subject's request before entering into a contract, transferring data for the sole benefit of a data subject where obtaining consent is not practically feasible but likely if possible, transferring data for important public interests, for the establishment, exercise, or defence of legal claims, and transferring data to protect vital interests of data subjects or other individuals who are physically or legally incapable of giving consent.

This provision of the Act significantly affects entities with international operations. Therefore, multinational companies that handle personal data of Nigerian subjects will have to conduct thorough assessments of the data protection regulations in the recipient country before transferring any data. This may involve engaging the services of a licensed data protection expert, complex negotiations and implementing additional compliance measures to safeguard the security and privacy of the data. Maintaining detailed records of the basis for data transfers and the adequacy of protection in the recipient country will be crucial to demonstrating compliance with the Act.

Further, the Act empowers the NDPC to designate specific categories of personal data to stricter transfer restrictions based on their nature and potential risks to data subjects. This dynamic designation

may change over time, requiring businesses to remain vigilant and adapt their data transfer practices accordingly. There is also a risk that the evolving data protection regulatory landscape may lead to additional costs and administrative burdens for multinational companies engaged in cross-border data transfers.

3.5 Part IX – Registration and fees for data controllers and data processors of major importance

The Act introduces a concept of data controllers and data processors of *'major importance'* who are mandated to register with the NDPC within six months of the commencement of the Act or upon becoming a data controller or data processor of major importance. These include 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, as will be determined by the NDPC, of data subjects who are within Nigeria. The registration process involves providing details of the names and addresses of the entity and data protection officer, description of the personal data being processed, categories and number of data subjects, data processing purposes, intended recipients of the data, details of any data processor operating on its behalf, the country to which data transfer is intended, and a general description of the safeguards and security measures in place for data protection. The NDPC is required to publish and maintain a public register of the registered data controllers and data processors of major importance to ensure transparency and accountability.

This registration requirement bears significant implications for businesses utilising data, particularly those who will be classified as data controllers or data processors of major importance. Failure to register with the NDPC or provide misleading information will result in penalties and damage to a company's reputation. The Act also emphasises the importance of ongoing compliance, as data controllers and data processors of major importance must promptly inform the NDPC of any significant changes to the information submitted during registration.

The Act allows the NDPC to exempt certain persons from being classified as data controllers/ processors of major importance. In addition, the Act empowers the Commission to prescribe fees or levies to be paid by data controllers and data processors of major importance.

Unfortunately, the Act does not define the metrics for classifying a data controller or data processor as one of major importance. Therefore, it is expected that the NDPC will issue a circular/ regulation to provide guidelines to companies on the relevant metrics for the classification and the applicable fees or levies.

3.6 Part X – Enforcement

This aspect of the Act introduces robust enforcement mechanisms to ensure data protection compliance among businesses. It establishes a complaint system, allowing data subjects to report violations to the NDPC. The NDPC is authorised to investigate these complaints and initiate inquiries independently when suspecting violations to ensure transparency and accountability for businesses handling personal data.

The penalties for the violation of the provisions of the Act or any subsidiary regulations vary depending on the importance of the data controllers or data processors, indicating that entities that process larger amounts of personal data will be held to higher data protection standards and accountability. Specifically, the maximum fine for data controller or data processor of major importance may be the greater of ₦10,000,000 and 2% of the annual gross revenue in the preceding financial year while for data controllers or processors not of major importance, the maximum fine may be the greater of ₦2,000,000 and 2% of their annual gross revenue in the preceding financial year.

The penalties provided in the Act appears stiffer than the penalties stipulated in the NDPR 2019 which provides for a fine of 2% of the annual gross revenue of the preceding year or ₦10million where the breach involved more than 10,000 data subjects, and 1% of the annual gross revenue of the preceding year or ₦2million where the breach involves less than 10,000 data subjects.

Commentary

The introduction of the NDPA is a laudable milestone, aligning Nigeria's digital economy and technological advancement with global best practices. The Act introduces several pivotal changes to the operations of data controllers and processors, creating the need for businesses to familiarise themselves with the key changes and seek expert guidance on how to navigate the evolving Nigerian data protection framework to ensure compliance, mitigate potential penalties for non-compliance, protect the privacy of data subjects, and deepen trust in an increasingly data-centric business environment.

We expect the NDPC to issue the relevant regulations and guidelines to harmonize the NDPR, and clarify other compliance requirements provided in the Act, such as the metrics for classifying data controller or data processor of major importance, the frequency of filing and content of compliance returns by such data controllers and data processors of major importance, and steps to be taken by a data controller to adequately inform data subjects of a personal data breach. It is also important that the NDPC provide in the regulations, stricter requirements with respect to the individual who is appointed as the Data Protection Officer (DPO) to ensure that the DPO has the requisite experience and competence in the organisation to drive compliance with the provisions of the Act. This will also ensure that issues of data protection are treated with utmost importance in Nigeria.

Given the changes introduced in the Act, businesses must assess their compliance status and strategies on evolving data protection policies. It becomes an even more murky pathway for technology companies who are adopting newer forms of technology such as machine learning, artificial intelligence, among others, into their business operations. These companies will need to ensure that such technology does not walk on the borderline of implying consent or impinge on any of the compliance requirements stipulated in the Act.

In the meantime, pending the issuance of the regulations by the Commission, affected businesses should proactively seek professional opinion to review and assess their current data processing framework for relevance and suitability to the compliance and other obligations specified in the Act to avoid any potential penalties for non-compliance.

kpmg.com/socialmedia

kpmg.com/app