Sep 2023

Nigeria: Highlights of the Data Protection Act, 2023

On June 12, 2023, the Nigeria Data Protection Bill was signed into law by President Bola Ahmed Tinubu. Tiwalola Osazuwa, Peretimi Pere, Nenjom Asuk, and Ifeoluwa Ebiseni, from Aelex Partners, look at the key provisions of the Act, including its scope and applicability and penalties for non-compliance.

James Enyi / Essentials collection / istockphoto.com

The long-awaited Bill had scaled through the legislative process at both houses of the National Assembly and was forwarded to the immediate past President, Gen. Muhammadu Buhari, for assent. However, it was not assented until the Tinubu-led administration was sworn in.

The Nigeria Data Protection Act, 2023 (the Act) is the first comprehensive legislation on data protection in Nigeria, replacing the Nigeria Data Protection Regulations 2019 (NDPR) as the primary instrument on data protection in Nigeria[1]. The Act is a welcome development as its provisions reflect a technological and commercial consciousness in respect of data and its use. Whilst the Act did not repeal its predecessors[2], it contains noteworthy provisions that differ from the pre-existing regime.

This article examines the provisions of the Act, *vis-à-vis* the provisions of the NDPR, highlighting its key provisions and how they affect new and existing businesses in Nigeria.

Key provisions of the Act

Scope and applicability of the Act

The Act is currently the primary legislation on data protection in Nigeria, superseding the NDPR. Whilst the NDPR and all previous regulations made by the National Information Technology Development Agency (NITDA) and the Nigeria Data Protection Bureau (NDPB) are preserved under the Act, the provisions of the Act will prevail in the event of any conflict with the provisions of any of the other regulations.

In terms of the applicability of the Act, the Act governs the processing of personal data, whether by automated means or not. The implication is that businesses that process personal data through manual/non-automated means are also caught within the scope of the Act and must comply accordingly. It is important to note that the definition of processing, just as under the NDPR, is extensive and would include various activities in respect of personal data, including collection of the information[3]. As such, it is imperative that small businesses, vendors, and other data controllers or processors ensure that their processing activities are in compliance with the law.

Additionally, the Act shifts focus from the residence and domicile of the data subject, as obtainable under the NDPR, to the processing activity and the controller/processor. Accordingly, the Act applies where: (i) the data controller or data processor is domiciled or resident or operating in Nigeria; (ii) the processing of personal data occurs within Nigeria; or (iii) where the data controller or data processor is not domiciled or resident or operating in Nigeria but is processing personal data of a data subject that is in Nigeria.

Establishment of the Nigeria Data Protection Commission

The Act establishes the Nigeria Data Protection Commission (NDPC) as the independent governing body for data protection and regulation in Nigeria. The NDPC, unlike its predecessor, is an independent body with perpetual succession and a common seal. The NDPC replaces the NDPB which was instituted in February 2022 by the former president of the Federal Republic of Nigeria as a specialized body to regulate data protection in Nigeria[4]. However, given the transitional provisions of the Act[5], it would appear that there has only been a nomenclature change to the status of the regulator, as the Act retains all the NDPB's officers, properties, proceedings and causes of action, contracts, certifications, and regulations, etc., which are now vested in the NDPC[6].

Notwithstanding, we anticipate that the NDPC in exercising its powers under the law will put in place robust regulations and guidelines that will further strengthen data protection compliance in Nigeria. It is thus important for businesses that process personal data (both small and large scale) to keep an eye on developments in this regard.

Processing of Sensitive Personal Data

The Act defines 'sensitive personal data' in similar terms as the NDPR but replaces the term 'sexual orientation' with 'sex life.' The rationale for the change is unclear.

The Act currently defines sensitive personal data[7] as personal data relating to an individual's: genetic and biometric data, for the purpose of uniquely identifying a natural person; race or ethnic origin; religious or similar beliefs, such as those reflecting conscience or philosophy; health status; sex life; political opinions or affiliations; and trade union memberships. The Act empowers the NDPC to prescribe further categories of 'sensitive personal data'[8].

The Act also highlights detailed but specific grounds for the processing of 'sensitive personal data.' These include: where consent has been given and not withdrawn for the specific purpose; where processing is necessary for carrying out obligations/exercising rights under social security or employment laws; to protect vital interests of the data subject or another person; where it is necessary for establishment, exercise, or defense of a legal claim; for medical care or community welfare; and for reasons of public health, etc[9].

It is important for data controllers and processors who operate in sectors that require handling sensitive personal data to understand these grounds and ensure that their basis lies within these grounds. The NDPC is empowered by the Act to make regulations setting out further grounds and applicable safeguards. Also, business owners, in line with the principles of processing personal data, should minimize the data collected and avoid processing unrequired sensitive personal data, as these would require an additional layer of protection, as may be prescribed by the regulator.

Registration requirement: data controllers and data processors of major importance

Section 44 of the Act introduces a new classification of controllers/processors - data controllers or processors of major importance - and defines them 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.'

Data controllers or processors of major importance are subject to higher obligations and penalties and are required to register with the NDPC six months after the commencement of the Act or upon attaining this status[10].

It is anticipated that the NDPC will release a guide or regulation for data controllers or processors of major importance[11] as the Act merely lays the framework for this new class of data controllers and processors, without more.

Inclusion of legitimate interest as a lawful basis for processing personal data

The inclusion of legitimate interest as a justification for processing personal data in the Act is a noteworthy addition. Under the NDPR, legitimate interest was not considered as a lawful basis for the processing of personal data. A lot of stakeholders believed there was a need for its recognition given that most businesses had legitimate reasons for the processing of personal data which the erstwhile scope did not cover.

Although the Act did not define legitimate interests, it sets down the rules for interests that will not be deemed legitimate. These include where: (i) such interests override fundamental rights, freedoms, and the interests of the data subjects; (ii) such interests are incompatible with other lawful bases for processing data under the Act; and (iii) the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged[12].

It is thus important for data controllers to take cognizance of this rule in relying on this basis for processing personal data.

Processing of data of children and individuals lacking legal capacity

One of the key issues settled by this Act in respect to the processing of children's personal data is the definition of a child under the Act. The Act adopts the definition of a child under the Child's Rights Act 2003. It also extends the rules for processing the personal data of children and those categories of people who lack legal capacity. Specifically, it provides that where the data subject is a child or person lacking the ability to consent, such consent can only be validly obtained from a parent or guardian of the data subject[13].

The Act mandates a data controller to employ appropriate mechanisms to verify age and consent, taking available technology into cognizance. It further stipulates a government-approved identification as an appropriate mechanism for verifying age and consent.

The Act, however, lays down the circumstances where consent of a child or a person who lacks legal capacity may be waived[14]:

- where the processing is necessary to protect the vital interests of the child;
- where it is carried out for purposes of education, medical or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or
- where it is necessary for proceedings before a court relating to the individual.

The Act also provides that where a child who is 13 years of age and above specifically requests the processing of their personal data in relation to the provision of information and services by electronic means, the NDPC shall make regulations for such processing in accordance with the objectives of the Act[15].

It is thus important that companies, particularly technology companies, put in place the appropriate measures to comply with the above. It is also expected that the NDPC will put in place practicable guidelines and rules on the subject, given the advancement of technology and the realities of the digital world[16].

Cross-border data transfers

Whilst the provisions of the Act on cross-border transfer is similar to the NDPR, the Act slightly modifies the rules pertaining to cross-border transfer of personal data. The Act sets out two conditions for cross-border transfer of data.

First, it restricts cross-border transfer to entities that are subject to a law, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms that afford an adequate level of protection with the Act.

Adequacy of protection is defined by the Act as a level of protection or system which upholds principles that are substantially similar to the conditions contained in the Act. The Act sets out factors to be taken into consideration in determining adequacy and empowers the NDPC to issue guidelines on the assessment of adequacy.

Secondly, in the absence of adequacy of protection as provided under the Act, a data controller or processor may only transfer data where;

- the data subject consents to the transfer and does not revoke such consent after being informed of the associated risks inherent in the transfer in the absence of adequacy of protection;
- transfer is necessary for the performance of a contract to which the data subject is a party in order to take steps at the request of the data subject, prior to entering into a contract;
- the transfer is for the sole benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject, and if it were reasonably practicable to obtain such consent, the data sub-

ject would likely give it;

- transfer is necessary for important reasons of public interest;
- transfer is necessary for the establishment, exercise, or defense of legal claims; or
- transfer is necessary to protect the vital interests of a data subject or of other persons who are physically or legally incapable of giving consent.

Given the transitional provisions of the NDPC and its mandate to issue guidelines on the subject, it will appear that the Whitelist issued under the previous regime is still in force and the countries listed are deemed to have adequate level of protection, pending any further guidelines by the regulator. Multinationals or other companies transferring or intending to transfer personal data are to take note of these conditions and comply accordingly.

Penalties for non-compliance

The Act empowers the NDPC to issue written compliance orders against defaulting data controllers or processors. Such orders include warnings, demands, and cease and desists. The orders will also specify the measures to be taken to avoid or remediate the violation, the period for implementation, and a right to judicial review.

The NDPC also has the power to investigate complaints made to it by data subjects in respect of the actions and inactions of a data controller or processor. The NDPC may, in addition to applicable criminal sanctions, issue enforcement orders against the defaulter. Such enforcement order may include a remedial fee of: (i) the higher amount between NGN 10,000,000 (approx. $13,200) or 2% of the controller/processor's annual gross revenue in the preceding financial year for data controllers or processors of major importance; and (b) the higher amount between NGN 2,000,000 (approx. $2,640) or 2% of the controller/processor's annual gross revenue in the preceding financial year for data controllers or processors not of major importance.

Conclusion

The Act contains some very important provisions that are vital to enable the NDPC to catch up with technological advancement and to play a supervisory role over data controllers and processors. It is noteworthy that the transitional provisions of the Act preserve all orders, rules, regulations, decisions, directions, licenses, and other documents that were in effect before the enactment of the Act, to the extent that they do not conflict with the provisions of the Act.

In any event, there are a number of clarifications required in terms of the provisions of the Act. It is anticipated that the NDPC will issue guidelines to resolve these ambiguities and vague provisions, to further achieve the objectives of the Act.

Tiwalola Osazuwa Partner

tosazuwa@aelex.com

Peretimi Pere Senior Associate

ppere@aelex.com

Nenjom Asuk Associate

nasuk@aelex.com

Ifeoluwa Ebiseni Associate

iebiseni@aelex.com

Aelex Partners, Lagos

---

1. The Act contains transitional and savings provisions that retain the provisions of existing regulations and instruments that are not in conflict with the Act.
2. Ibid.
3. Processing is defined under Section 65 of the Act as 'any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria.'
4. Prior to the establishment of the NDPB, NITDA was responsible for implementing the NDPR, which itself was issued pursuant to the NITDA Act.
5. Section 64 of the Act.
6. Id.
7. Section 65 of the Act.
8. Section 30(2) of the Act.
9. Section 30(1) of the Act.
10. Section 44(1) of the Act.
11. It is uncertain what kind of controller or processor will fall within this bracket, and as such, it is impracticable for businesses to comply with the deadline set by the Act.
12. Section 25(2) of the Act.
13. Section 31 of the Act.
14. Section 31(4) of the Act.
15. Section 31(5) Data Protection Act, 2023.
16. It is imperative that these guidelines are set, given the boundaryless nature of the internet.