Infusion Lawyers

your partner in innovation

Understanding the Nigeria Data Protection Act 2023: Obligations of Digital Platforms and Businesses

www.infusionlawyers.com

Infusion Lawyers is a virtual technology and intellectual property law firm for the knowledge economy and the digital age. With our innovative legal services, consider us *your partner in innovation*.

Infusion Lawyers

your partner in innovation

Understanding the Nigeria Data Protection Act 2023: Obligations of Digital Platforms and Businesses

3 August 2023

Gabriel Eze, *Associate*

gabriel@infusionlawyers.com

Introduction

On 12 June 2023, the Federal Government of Nigeria passed the Nigeria Data Protection Bill into law—Nigeria Data Protection Act 2023 (NDPA). The NDPA comes on the heels of the Nigeria Data Protection Regulation (the "NDPR", or the "Regulation") issued by the National Information Technology Development Agency (NITDA) on 25 January 2019. Before the NDPR, there was the Guidelines on Data Protection 2013 (the "Guidelines") also issued by NITDA. Up until it was repealed, the Guidelines was crippled by lack of any enforcement mechanism and uncertainty about its legal status. A major shortcoming of the NDPR is that it is a subsidiary legislation. Also, it lacks certain vital provisions expected in a substantive statute. For instance, NITDA lacked the statutory authority to establish a commission with wide powers to deal with data privacy issues in Nigeria. And this may be why under the NDPR, "Relevant Authorities", which is defined to mean NITDA "or any other statutory body or establishment having government's mandate to deal solely or partly with matters relating to Personal Data", are recognized.

Consequently, the NDPA has been enacted as the principal data legislation in Nigeria. The NDPA provides a legal framework for the protection of personal information and establishes the Nigeria Data Protection Commission (NDPC) for the regulation of the processing of personal information. Notably, priority is given to the NDPA over any other legislation relating to the processing of personal data—directly or indirectly—in Nigeria. Effectively, where the provisions of any other legislation, apart from the Constitution of the Federal Republic of Nigeria, 1999 (the Constitution), are inconsistent with any of the provisions of the NDPA, the latter shall prevail.

The objective of this article is to provide a general understanding of the NDPA, highlighting its provisions from five perspectives, namely constitutional, legal & regulatory, administrative, technical/organizational, and economic perspectives. I also point out the NDPA's relationship with previous and other similar legislation. Finally, I outline obligations digital platforms and businesses must comply with in order to safely do business in Nigeria's growing digital economy.

Scope and applicability of the NDPA

The NDPA applies to the processing of personal data by a data controller or data processor—whether by automated means or not—belonging to data subjects in Nigeria. Specifically, the NDPA provides instances of mandatory application. These instances are "where the —

(a) data controller or data processor is domiciled in, resident in, or operating in Nigeria;

(b) processing of personal data occurs within Nigeria; or

(c) the data controller or the data processor is not domiciled in, resident in, or operating in Nigeria, but is processing personal data of a data subject in Nigeria."[1]

Essentially, it will not matter that a data controller or data processor is not domiciled or operating in Nigeria. As long as personal data of data subjects in Nigeria are being processed, the NDPA applies.

The NDPA does not offer protection to Nigerian citizens residing outside Nigeria.

Noticeably, there is a significant distinction in scope and applicability between the NDPA and the NDPR (including the NDPR Implementation Framework 2020). While the NDPA applies to the personal information of a data subject in Nigeria only, the NDPR applies to the personal information of data subjects residing in Nigeria or *residing outside Nigeria who are citizens of Nigeria*.[2] This creates two specific implications: (1) the personal data of Nigerians abroad do not enjoy protection, except the data controller or data processor is domiciled in, resident in, or operating in Nigeria; and (2) the personal data of both Nigerians and non-Nigerians in Nigeria enjoy protection. This is similar to the provisions on territorial scope under the General Data Protection Regulation (GDPR).[3]

The NDPR—to the extent of its consistency with the NDPA—is now to be treated as a regulation issued by the NDPC established under the NDPA. It is understandable because the NDPC has statutory powers to make regulations. Presently, the NDPR coexists with the NDPA subject to when (or if) the National Commissioner replaces it.

Application Limits of the NDPA

The NDPA will not apply "to the processing of personal data carried out by one or more persons solely for personal or household purposes" as long as such processing does not violate the fundamental right to privacy of a data subject.[4]

Other exceptions include the processing of personal data carried out by a competent authority, or of national health emergency, or of natural security, or in respect of a publication of public interest.

Accordingly, the NDPA will not apply to a data controller or data processor if the processing of personal data is carried out by

[1] Section 2 (1) (2) (a), (b), (c) NDPA

[2] Article 1.2 (b) NDPR

[3] Article 3 GDPR

[4] Section 3 (1) NDPA

a competent authority for any of the following purposes:

- the prevention, investigation, detection, prosecution, or adjudication of a criminal offense or to execute a criminal penalty in accordance with any applicable law;
- to prevent or control a national public health emergency;
- as is necessary for national security;
- in respect of publication in the public interest, for journalism, educational, artistic and literary purposes to the extent that such obligations and rights are incompatible with such purposes; or
- necessary to establish, exercise, or defend legal claims, whether in court proceedings, or in an administrative or out-of-court procedure.[5]

The above exception applies as long as two things are considered. First, the rights and freedoms under the Constitution are guaranteed alongside its limitations. And second, obligations relating to the principles of data processing, lawful basis for personal data processing, and personal data breaches are not violated.

Understanding the NDPA from Five Perspectives

A holistic understanding of the NDPA flows from five perspectives. These could be gleaned from the objectives of the NDPA as follows:

1. Constitutional

The first perspective is to "safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution"[6]. This is deeply rooted in the right to private and family life under section 37 of the Constitution. Section 37 guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. Digital platforms and businesses that control and/or process personal data of Nigerian citizens within Nigeria must recognize that personal data and privacy matters are fundamental rights.

2. Legal & Regulatory

The second perspective is to ensure that personal data is processed in a fair, lawful and accountable manner. To protect data subjects' rights, and provide means of recourse and remedies in the event of a breach.[7] To provide regulation for the processing of personal data and ensure that data controllers and data processors fulfill their obligations to data subjects.[8]

Digital platforms and businesses in Nigeria are obligated to meet the legal and regulatory requirements under the NDPA or face sanctions. An example of this is the abuse of privacy rights by digital loan platforms such as Soko Loan.

In February 2023, it was reported that the Nigeria Data Protection Bureau (NDPB) investigated four banks, one telecommunications firm, consulting firms, and a large number of loan sharks for various alleged data breaches. Briefing some journalists in Lagos, the National Commissioner of the NDPC, Dr. Vincent Olatunji, particularly condemned the activities of loan sharks and the pains they cause to Nigerians. "Loan Sharks" are alternative lending platforms that perpetuate illegal and unethical practices including violating consumer privacy,

[5] Section 3 (2) (a) – (e) NDPA

[6] Section 1 (1) (a) NDPA
[7] Section 1 (1) (d), (e) NDPA
[8] Section 1 (1) (b), (f) NDPA

ethical loan repayment/recovery practices, fair lending terms, and consumer rights. According to Dr. Olatunji, NDPB was investigating over 110 data controllers and data processors for various degrees of data privacy and protection breaches.

Digital platforms and businesses in Nigeria should adopt a privacy-by-design model.

To hold information securely and prevent unauthorized access to data subjects' information, digital platforms and businesses should adopt a privacy-by-design model.

Privacy-by-design model simply means that digital platforms and businesses must consider privacy and data protection concerns and integrate requisite measures in building digital products and services. They must ensure that their platforms including software Applications (Apps) are directly or indirectly built in accordance with and meet legal/regulatory requirements of the NDPA.

Other key provisions

(a) Children or persons lacking legal capacity to consent are protected.

Where a data subject is a child or a person lacking the legal capacity to consent, a data controller must obtain the consent of the parent or legal guardian. The data controller must apply appropriate mechanisms to verify age and consent, taking into consideration available technology.[9]

However, there is an inconsistency in the NDPA concerning who a child is. While section 31(5) provides that a child that is below 13 years is not capable of giving consent for processing activities, section 65 applies the same meaning of a "child" as ascribed under the Child's Rights Act, 2003. Under the Child Rights Act, a child is a person below the age of 18 years.[10]

(b) Data controllers and data processors owe data subjects a duty of care.

Data controllers or data processors owe a duty of care in respect of personal data processing. They must demonstrate accountability relating to the principles and lawful basis for processing personal data. They must ensure that personal data is processed in a fair, lawful, and transparent manner. And personal data must be collected for specified, explicit, and legitimate purposes.

The personal data collected must not be further processed in a way incompatible with these purposes. They must be adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed. They must be retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed.[11]

Digital platforms and businesses that control or process personal data of data subjects in Nigeria are generally not permitted to further process personal data of data subjects. Especially if it is for a purpose different from which it was originally collected. For instance, a bank or Fintech platform cannot use customers' personal information in its database to process automated teller machine (ATM) cards for them if it had not first informed and obtained customers' consent. To proceed with such further processing, customers must be provided with all relevant

[9] Section 31 (1) & (2) NDPA

[10] Section 227, Child Rights Act, 2003

[11] Section 24 (1) NDPA

information to enable them to decide accordingly.

(c) Automated decision-making is generally prohibited under NDPA.

Under Section 37(1) of the NDPA, a data subject has the right not to be subject to a decision based solely on automated processing of personal data. This includes profiling, which produces legal or similar significant effects concerning the data subject.

By prohibiting robots from determining rights and liabilities of a data subject, it ensures that human will is not vitiated in obtaining consent and that fundamental rights of data subjects remain safeguarded.

However, the NDPA provides exceptions to automated decision-making. Automated decision-making will not apply where it is:

(i) necessary for entering into or for the performance of a contract between the data subject and a data controller;

(ii) authorized by a written law, which establishes suitable measures to safeguard the fundamental rights and freedoms;

(iii) in the interest of the data subject; or

(iv) authorized by the consent of the data subject.

3. Technical/Organizational

The third perspective is to "promote data processing practices that safeguard the security of personal data and privacy of data subjects."[12]

[12] Section 1 (1) (c) NDPA

Digital platforms and businesses operating in Nigeria must implement appropriate technical and organizational measures. This is to ensure the security, integrity, and confidentiality of personal data in their possession or under their control. It involves having relevant policies on data retention periods. Data security measures, such as encryption, or the insertion of consent and withdrawal of consent functionalities in data subject-facing applications with regard to security should be implemented.

Flutterwave and MTN's MoMo PSB

In April 2023, it was reported that Flutterwave, Nigeria's Fintech unicorn, allegedly lost about $6.4 Million in a hack. Though Flutterwave has since denied the allegations and reports of any hack on its security system, the point is that technical/organizational standards on data protection are critical to cybersecurity.

Also, in May 2022, MTN's Momo Payment Service Bank (PSB) in Nigeria was reportedly hacked. According to the reports, it suffered a breach and lost about 22 Billion Naira. However, MoMo's PSB CEO posited that no customers' funds were lost and that all customer data remains secure.

The above incidents support why digital platforms and businesses must ensure continuous improvement of their information security architecture to prevent possible data breaches. Strong controls and security safeguards at technical and operational levels must be in place to prevent hacking. Digital platforms and businesses must ensure protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, or access. This is a requirement under the NDPA.

In carrying out this statutory function, the following must be taken into consideration:

(i) the amount and sensitivity of the personal data;

(ii) the nature, degree and likelihood of harm to a data subject that could result from the loss, disclosure, or other misuse of the personal data;

(iii) the extent of the processing;

(iv) the period of data retention; and

(v) the availability and cost of any technologies, tools, or other measures to be implemented, relative to the size of the data controller or data processor.[13]

The more reason also digital platforms and businesses must have internal mechanisms for cybersecurity measures.

4. Administrative

The fourth perspective is to "establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors."[14]

For the first time in Nigeria, there is the establishment of a sole data protection and regulatory authority—the NDPC. The NDPC is an independent body with wide powers[15] to oversee the implementation of the provisions of the NDPA, and issue regulations, rules, directives, and guidance.[16]

In a presentation on "Data Protection in Emerging Technologies", Dr. Olatunji stated that the NDPA is designed to address the challenges that may arise with the deployment of emerging technologies in Nigeria and that *"strong data protection laws are needed for responsible AI development and deployment ..."*[17] Affirmatively, the NDPA provides for regulating the deployment of technological and organizational measures to enhance personal data protection, foster the development of personal data protection technologies, in accordance with recognized international best practices and applicable laws globally, etc.[18] Of course, this does not suggest that the NDPC will not also address challenges that arise in data protection and privacy outside the deployment of emerging technologies in Nigeria.

The NDPA recognizes other competent authorities other than the NDPC in Nigeria.

Similarly, the NDPA also recognizes other competent authorities such statutory bodies or establishments having the government's mandate to deal solely or partly with matters relating to personal data. Under section 65 of the NDPA, it defines "competent authority" to include:

(a) the Government of the Federal Republic of Nigeria or any foreign government; or

(b) any state government, statutory authority, government authority, institution, agency, department, board, commission, or organization within or outside Nigeria, exercising executive, legislative, judicial, investigative, regulatory, or administrative functions.

For instance, the Federal Competition and Consumers Protection Commission (FCCPC), in conjunction with other relevant

[13] Section 39 (1)(a)–(e) NDPA
[14] Section 1 (1) (g) NDPA
[15] Section 7 NDPA
[16] Section 6 NDPA

[17] Dr Vincent Olatunji, 'Nigeria Data Protection Act To Address Technological Challenges', VON, July 12, 2023, https://von.gov.ng/nigeria-data-protection-act-to-address-technological-challenges/
[18] Section 5(a)–(b) NDPA

regulatory authorities, introduced the Limited Interim Regulatory/Registration Framework and Guidelines for Digital Money Lending 2022 (the FCCPC Framework). The FCCPC Framework was issued to curb illegal and unethical practices of loan sharks.

Also, the Nigeria Communications Commission (the NCC) recently published some draft regulatory instruments. These include the Data Protection (Communications Services) Regulations 2023, and the Draft Guidelines on Corporate Governance. The proposed regulatory frameworks are for the protection and privacy of data in the communications sector.

Reason a new Commission has been established in Nigeria when the Country already has the NDPB

Indeed, before the enactment of the NDPA, the Federal Government of Nigeria had created the NDPB in February 2022. This, amongst other things, is to further numerous municipal and international instruments on the fundamental right to privacy. Part of the NDPB's mandate is to oversee the implementation and achieve the objectives of the NDPR. Its functions include to safeguard the rights of natural persons to data privacy, and foster safe conduct of transactions involving the exchange of personal data. The NDPB is mandated to also ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.[19]

The NDPA consolidates the NDPB and the NDPC as one entity.

The NDPA makes copious provisions relating to the NDPB in order to curb the duplicity that often results in avoidable regulatory frictions and tensions. Effectively, under the NDPA, any reference to the NDPB or a document issued in the name of the NDPB, shall be read as a reference to the Commission, and all persons engaged by the Commission shall have the same rights, powers, and remedies as they existed in the NDPB before its commencement.

Also, all other existing agreements and contracts currently in effect by the NDPB relating to the provisions of the NDPA will continue. This includes all orders, rules, decisions, directions, licenses, authorizations, certificates, consents, approvals, declarations, permits, registrations, rates, or other documents that were in effect before the enactment of the NDPA and that are made or issued by NITDA or the NDPB. They will continue to be in effect as if they were made or issued by the Commission until they expire or are repealed, replaced, reassembled, or altered.[20]

This smooth transition, with statutory backing, is commendable.

5. Economic

The fifth objective of the NDPA is to "strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data."[21]

If the news on fines and sanctions by the NDPC is anything to go by, then it is clear

[19] https://ndpb.gov.ng/Home/about#, accessed 20 July 2023

[20] Section 64 (1) and (2) (a)–(f) NDPA

[21] Section 1 (1) (h) NDPA

that Nigeria is determined to strongly protect the personal data of Nigerians in the Country. According to Senator Ihenyen, "by having a stronger protective regime for data privacy, in tune with global best practices, Nigeria hopes to help boost international trade and commerce. At a time when transactions increasingly involve personal data processing, one of the objectives … is to ensure that there are adequate safeguards in place. Also, the economic advantage to data protection is not lost ... The scope of the [NDPA] and its penalties demonstrate this consciousness."[22]

Accordingly, the Nation newspaper has reported that no fewer than seven banks and other institutions had paid over 200 Million Naira to the Federal Government for violating data privacy of Nigerians. The instances for the 200 Million Naira-fine include cases where citizens' personal data being wrongly captured by banks making affected customers unable to access funds in their bank accounts. And cases where some customers' funds were wiped off from their bank accounts due to personal data breaches.

The NDPA generally prohibits cross-border transfer of personal data.

Under the NDPA, Digital platforms and businesses whose data processing activity may extend beyond Nigeria are barred from transferring or permitting personal data to be transferred from Nigeria to another country. They are only allowed to do so where the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism with similar level of protection that the NDPA provides.[23]

[22] Senator Ihenyen, 'Nigeria: New Regulation Demonstrates a Serious Approach to Data Protection', Data Protection Leader, Vol. 1, Issue 4, September 2019, 18

[23] Section 41 (1) NDPA

Obligations of Digital Platforms and Businesses Processing Personal Data

There are a number of obligations digital platforms and businesses processing personal data must comply with under the NDPA. Here are some of them:

1. **Compliance with the NDPA:** digital platforms and businesses that control or process personal data must ensure they comply with the principles and obligations set out in NDPA as applicable to them.[24]

2. **Registration of data controllers and data processors of major importance:** Data controllers and data processors of major importance must register with the Commission within six months after the commencement of the NDPA or on becoming a data controller or data processor of major importance.[25] The NDPA defines "a data controller of major importance" in two disjunctive ways:

   (i) one 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*

   (ii) 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.

   Considering how far and wide the above qualifications are, the NDPA has given very wide discretion to the NPDC to exercise, particularly under the second paragraph above. This is a potential problem. Advisedly, the

[24] Section 29 NDPA

[25] Section 44 NDPA

NDPC may consider issuing further guidance in this respect. Also, since the NDPA has given life to all previous orders, rules, regulations to coexist side by side, it may be right to say that the thresholds for filing data audits as stipulated by the NDPR for data controllers processing of personal data apply under 2(i) above. A period of 12 months for businesses or organizations processing personal data of more than 2,000 data subjects.

3. **Designation of Data Protection Officer (DPO):** A data controller of major importance shall designate a DPO with expert knowledge of data protection law and practices. The DPO is required to have the ability to carry out the tasks prescribed under the NDPA and subsidiary legislation made under it.

   The DPO may be an employee of a data controller or engaged by a service contract.[26]

Conclusion

The enactment of the NDPA is a welcome development, particularly for Nigeria's growing digital economy. By having a principal data legislation, Nigeria has demonstrated that it recognizes the place of personal data in driving a data-driven global economy. Although there are certain inconsistencies that require further clarifications by the NDPC, the NDPA will further engender growth and innovation in Nigeria. But it does not come without its implications on digital platforms and businesses.

Data controllers and data processors should consult with their lawyers to ensure full compliance and avoid exposure to liabilities for non-compliance. Similarly, data subjects should be aware of their rights, ensuring that data controllers and data processors are held accountable for any violations.

Data controllers and data processors should consult with their lawyers to ensure full compliance and avoid exposure to liabilities for non-compliance. Similarly, data subjects should be aware of their rights, ensuring that data controllers and data processors are held accountable for any violations. Assisting organizations and individuals to safely navigate the data protection and privacy landscape remains one of the areas Infusion Lawyers is always available for.

[26] Section 32 (1) and (2) NDPA

A&D FORENSICS

Infusion Lawyers

Our Certified Cryptocurrency Compliance Specialist Course (3CS)

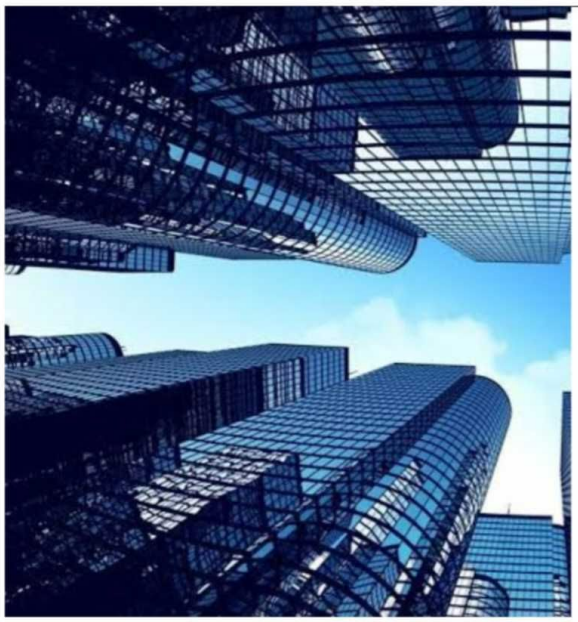
is tailored-made for:

- Compliance Officers of Banks, Cryptocurrency Exchanges & Financial Institutions.
- Lawyers
- Tax Specialists
- Forensic Accountants / Auditors
- Certified Fraud Examiners
- OTC Traders
- Investigators

Join us this **September** in **Lagos** by enrolling here:

Register here: https://adforensics.com.ng/training/

Training Materials and Catered Lunches are available for Participants.



Infusion Lawyers
your partner in innovation

Contact us:

LAGOS

23 Water Corporation Drive
Victoria Island, Lagos, Nigeria

ABUJA

Ventures Park, 5 Kwaji Close
Maitama, Abuja, FCT, Nigeria

Telephone: +234806 735 1417
Email: info@infusionlawyers.com
Website: www.infusionlawyers.com

Infusion Lawyers
your partner in innovation