Nigeria Data Protection Act, 2023: A Review

G. ELIAS

Introduction

Due to the rapid advancement of technology and the advent of artificial intelligence, there has been a growing global focus in personal data protection and privacy. However, it was not until 2019 that Nigeria had its first matter-specific regulation on personal data protection in the form of the Nigeria Data Protection Regulation (the "**NDPR**").[1] The NDPR Implementation Framework was subsequently issued in 2020 to provide more clarity on the NDPR provisions. There are also sector-specific rules on data protection items in the Central Bank of Nigeria ("**CBN**") Consumer Protection Framework, 2016,[2] Nigerian Communications Commission's Consumer Code of Practice Regulations, 2007 and other sundry acts and regulations. On June 13, 2023, the Nigeria Data Protection Act, 2023 (the "**Act**") was enacted to provide a more extensive regulatory framework for the protection of personal data in Nigeria.

This article aims to explain the changes made by the Act, highlight the key provisions of the Act and explore the impact of this Act on both businesses and individuals. We have structured this paper into twelve (12) rubrics namely: (a) key terms defined in the Act, (b) scope and applicability of the Act, (c) establishment of Nigeria Data Protection Commission, (d) principles and lawful basis for Data Processing, (e) necessity of consent (f) children and consent, (g) data privacy impact assessment, (h) Sensitive Personal Data, (i) Data Protection Officers, (j) the rights of a Data Subject, (k) cross-border transfer of Personal Data, and (l) sanctions and penalties.

It is pertinent to mention that the NDPR and its Implementation Framework has not been expressly repealed and as such, both regulations will remain valid and effective to the extent that they are not inconsistent with the Act.[3] Nevertheless, the Act provides that in the event of any inconsistency between the provisions of any law or regulation (NDPR and its Implementation Framework being inclusive) and this Act on Personal Data Processing, the provisions of Act shall prevail.[4]

Key Terms Defined

Before delving into the provisions of the Act, it is imperative to familiarize ourselves with certain key terms. Understanding these terms will aid comprehension of the discourse. The Act defines "Personal Data" as any information that can identify an individual. The "Data Subject" refers to an individual to whom Personal Data relates. A "Data Controller" is an entity or an individual responsible for determining the purpose and methods of processing Personal Data. A "Data Processor" is the entity or an individual that handles the processing of Personal Data on behalf of the Data Controller or at the direction of a Data Controller or another Data Processor. Under the Act, "Data Processing" encompasses any operation or set of operations that is performed on Personal Data including but not limited to collection, recording, organization, structuring, and storage whether through automated means or otherwise. The definition of "Data Processing" does not include the mere transit of data originating outside Nigeria through Nigeria.

Scope and Applicability of the Act

The Act generally applies to the processing of Personal Data whether it is conducted by automated means or not.[5] Section 2(2) of the Act identifies three exclusive instances where the Act will be applicable. First, the Act applies to a Data Controller or Data Processor who is domiciled in, resident in or operating in Nigeria. Second, the Act applies if the Data Processing takes place in Nigeria.[6] Finally,

[2] Rules 2.6 and 2.6.2, CBN Consumer Protection Framework, 2016
[3] S.64(2)(f), the Act
[4] S. 63, the Act.
[5] S. 2(1), the Act.
[6] S. 2(2)(b), the Act.

the Act applies to a Data Controller or Data Processor who does not reside or operate in Nigeria but processes the Personal Data of a Data Subject in Nigeria.[7]

However, the Act does not apply if the processing of Personal Data is solely for personal or household purposes provided that such processing does not violate the fundamental right to privacy of the Data Subject.[8] The Act does not also apply where Personal Data is processed for the purposes of crime investigation, public health emergencies, national security, or the publication of matters in the public interest for journalism, educational or literary purposes,[9] or commencing or defending legal proceedings.[10]

Although the Act is inapplicable in these cases, section 3(2) provides that the Data Controller or Data Processor must consider the privacy rights safeguarded in the Constitution of the Federal Republic of Nigeria, 1999 (as amended), principles and lawful bases of Personal Data Processing and the requirement to appoint a Data Protection Officer.

Furthermore, the Act grants the regulator that it creates, i.e., the Commission (more on this shortly), the discretion to determine, by regulation, the types of Personal Data and processing that will not fall under the purview of the Act.[11]

Establishment of the Nigeria Data Protection Commission

The Act has replaced the Nigeria Data Protection Bureau (the "**Bureau**"), which was established by former President Mohammed Buhari in 2022 as the regulatory body to implement the NDPR. In its place, a new independent regulatory body known as the Nigeria Data Protection Commission (the "**Commission**") has been established. The Commission has the mandate to oversee the implementation of the Act and exercise regulatory oversight over personal data protection and privacy matters.[12]

The Commission is also empowered by the Act to prescribe fees for Data Controllers and Data Processors, issue rules, regulations and directives, prescribe the manner and procedure of compliance returns filings by Data Controllers and Data Processors, and investigate and impose penalties for any contravention of the Act or any subsidiary legislation made pursuant thereto.[13]

Under the Act, the Commission is entrusted with the responsibility of overseeing the accreditation, licensing, and registration of suitable entities to provide data protection compliance services.[14] The Commission is also mandated to promote awareness on the obligations of Data Controllers and Data Processors and sensitize the public about Personal Data protection, their rights and obligations and risks to their Personal Data.[15]

Furthermore, the Commission is tasked with the responsibility of determining whether regions, countries, corporate rules and contractual clauses have adequate Personal Data protection standards for cross border transfers.[16] The Commission is responsible for collecting and publishing information with respect to Personal Data protection, including Personal Data breaches.[17] The Commission can exercise its discretion to license a person (whether human or juristic) to monitor, audit and report on compliance by Data Controllers and Data Processors.[18]

[7] S. 2(2)(c), the Act.
[8] S. 3(1), the Act.
[9] S. 3(2), the Act.
[10] Ibid
[11] S. 3(3), the Act.
[12] Ss.4,5,6,64, the Act.
[13] S. 6, the Act.
[14] S. 5(c), the Act.
[15] S. 5(e) and (f), the Act.
[16] S. 5(k), the Act.
[17] S. 5(l), the Act.
[18] S.33, the Act.

Principles and Lawful Basis Governing Personal Data Processing

As recognised under the NDPR, the Act outlines six principles that should regulate how Personal Data is controlled and processed in Nigeria namely:

1. a Data Controller or Data Processor is required to process Personal Data in a fair, lawful and transparent manner.[19]
2. Personal Data should only be collected for specified, explicit and legitimate purposes and not used for other incompatible purposes.
3. a Data Controller or Data Processor shall ensure that Personal Data is adequate, relevant, and limited to the minimum necessary for the purposes for which the Personal Data was collected or further processed.
4. Personal Data should not be retained for a period longer than is necessary for the purposes for which it is processed.
5. Personal Data collected must be accurate, complete and up to date.
6. Personal Data should be processed in a manner that ensures the security of Personal Data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach.[20]

These principles closely mirror what is obtainable in the European Union General Data Protection Rules (the "**GDPR**").[21] These principles have been specifically designed to protect the privacy of individuals and to ensure that their Personal Data is used fairly and responsibly.

The Act establishes six (6) lawful bases for the processing of Personal Data namely: consent, contractual necessity, legal obligation, vital interests, public interest and legitimate interests of the Data Controller or Data Processor.[22] Moreover, the interests of the Data Controller or Data Processor must not violate the fundamental rights of the Data Subject, and must not be incompatible with the other lawful bases of processing or extend the purpose for which the Data Subject agreed to.[23]

Necessity of Consent

Before Personal Data is collected or processed, the Data Controller or Data Processor must obtain the informed consent of the Data Subject. However, before the consent is granted, the Data Subject must be informed of their right to withdraw consent.[24] The Act provides that the withdrawal of consent does not invalidate previous Processing,[25] but it will affect subsequent Processing.

The Data Controller or Data Processor is tasked with supplying the following information to the Data Subject: the identity or residence of the Data Controller, lawful basis and purposes of processing, Data Subject rights, retention period for the Personal Data, right to lodge complaint and the existence of automated decision-making.[26] These information items should be contained in a privacy policy.[27]

The Act provides that requests for consent must be communicated clearly and simply, allowing the Data Subject to provide the affirmative consent without any pre-selected options.[28] Silence or

[19] S.24(1), the Act.
[20] S. 24 (1)(f) of the Act.
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.
[22] S. 25(1), the Act.
[23] S.25(2), the Act.
[24] S. 26(2), the Act.
[25] S.26(5), the Act.
[26] S. 27(1), the Act.
[27] S. 27(3), the Act.
[28] S. 26(6) & (7)(a), the Act.

inactivity of the Data Subject cannot be construed as consent.[29] The Data Subject may give consent in writing, orally or through an electronic means.[30]

Children and Consent

Under the Act, children and persons lacking the legal capacity to consent, such as a lunatic, cannot grant consent for the processing of their personal data. In these cases, the Act directs the Data Controller to obtain consent from their parents or guardians instead.[31] The Act also mandates the Data Controller to utilize available technology to verify the consent and age of the Data Subject, which includes the presentation of any government-approved identification documents.[32]

However, this restriction does not apply where the processing is necessary to protect the vital interests of the child or person lacking legal capacity to consent.[33] It also does not apply in cases pertaining to the educational, medical or social care of the child or person lacking legal capacity or for court proceeding relating to the Data Subject.[34] The Act further requires the Commission to make regulations in accordance with the objectives of the Act to govern the processing of the Personal Data of children who (a) are at least thirteen (13) years old and (b) request the provision of information and services by electronic means.[35]

Under the NDPR and its Implementation Framework, there were few provisions regarding the Personal Data Processing of a child.[36] Notably, the Implementation Framework clearly defined a child as any person under thirteen (13) years.[37] The Implementation Framework directed the data controllers and processors to formulate their privacy policies in a "child-friendly form" to ensure children and their parents understand the Data Processing activity before granting consent.[38] However, the Implementation Framework does not define “child-friendly form.”

It is important to note that, unlike the Act, the NDPR and its Implementation Framework did not mention any other category of persons that enjoy comparable privileges and protection like children. In contrast, the Act explicitly categorized these persons as persons lacking the legal capacity to consent.

Data Privacy Impact Assessment

The Act requires the Data Controller to conduct a data privacy impact assessment (the “**DPIA**”) if there is a likelihood that processing of Personal Data may adversely impact the rights and freedoms of the Data Subjects.[39] In the event that the DPIA indicates that the processing of the Personal Data could affect Data Subjects’ rights, the Data Controller is required to consult with the Commission.[40] The Act vests power on the Commission to issue regulations or directives specifying the categories of processing and persons subject to the requirement for the conduct of a DPIA.[41]

The DPIA is expected to contain the following information: (a) a systematic description of the Data Processing and its purpose; (b) an assessment of the necessity and proportionality of the processing in relation to the purpose of processing; (c) assessment of the risks and freedoms of a data subject; and (d) measures to mitigate the identified risks.[42]

---

[29] S.26(3), the Act.
[30] S. 26(7)(b), THE ACT.
[31] S. 31(1), the Act.
[32] S. 31(2) and (3), the Act.
[33] S. 31(4)(a), the Act.
[34] S. 31(4)(b), the Act.
[35] S. 31(5)(b), the Act.
[36] Art. 3,1 NDPR and Para 5.5, NDPR Implementation Framework
[37] Para 5.5, NDPR Implementation Framework
[38] Ibid
[39] S. 28(1), the Act.
[40] S. 28(2), the Act.
[41] S.28(3), the Act.
[42] S. 28(4), the Act.

The NDPR and its Implementation Framework also require Data Controllers to conduct DPIA in order to enhance compliance and minimise data protection risks.[43] The NDPR provides that a DPIA may be required for the following types of Data Processing: (a) evaluation or scoring; (b) automated decision-making with legal or similar significant effect; (c) systematic monitoring; (d) the processing of sensitive or highly Personal Data; (e) the processing of the Personal Data of vulnerable or differently-abled Data Subjects; and (f) when considering the deployment of innovative processes or application of new technological or organizational solutions.[44]

Sensitive Personal Data

The Act defines sensitive Personal Data as "*Personal Data relating to an individual's :(a) genetic and biometric data, for the purpose of uniquely identifying a natural person; (b) race or ethnic origin; (c) religious or similar beliefs, such as those reflecting conscience or philosophy; (d) health status; (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; or (h) other information prescribed by the Commission*."[45]

The processing of sensitive Personal Data is generally prohibited for Data Controllers or Data Processors except where:[46]

1. the explicit consent of Data Subject is obtained and has not been withdrawn;
2. the Data Controller requires the data to perform its obligations or to exercise the Data Subject rights under employment;
3. it is necessary to protect the vital interests of the Data Subjects or of another person where the Data Subject is incapable of giving consent;
4. the Data Controller is a non-profit organization and the data being processed is about its members or former members;
5. the data is necessary for the establishment, exercise or defence of legal claims;
6. the data is processed for public interest purposes;
7. the data is processed for medical purposes or community welfare;
8. the data is processed for public health reasons; or
9. the data is processed for archiving, scientific or historical research purposes.

Data Protection Officers

The Act introduced a new category of entities known as "Data Controllers or Data Processors of Major Importance". The Act mandates them to appoint a Data Protection Officer (the "**DPO**") who must possess expertise in data protection laws and practices.[47] The DPO is responsible for providing advice to the Data Controller and ensuring that the Data Controller complies with the Act.[48] Additionally, the DPO is the contact point for the Commission on Data Processing issues.[49]

A Data Controller or Data Processor of Major Importance is defined under the Act as *"a Data Controller or Data Processor that is domiciled, resident in or operating in Nigeria and (a) processes the Personal Data of a substantial number of Data Subjects who are within Nigeria, as the Commission may prescribe, or (b) processes Personal Data that is important to the economy, society or security of*

[43] Para. 3.2 (viii), the Implementation Framework
[44] Art. 4.2, the NDPR.
[45] S. 65, the Act.
[46] S. 30, the Act.
[47] S. 32(1) and (2), the Act.
[48] S. 32(3)(a), the Act.
[49] S. 32(3)(b), the Act.

Nigeria, as the Commission may designate."[50] Data Controllers and Data Processors of Major Importance are obligated to register with the Commission within six months after the commencement of the Act or on becoming a Data Controller or Data Processor.[51]

Unlike the Act, the Implementation Framework imposes the obligation to appoint a DPO on the following categories of Data Controllers/Data Processors: (a) government ministries, department and agencies; (b) organizations processing at least ten thousand (10,000) Data Subjects yearly; (c) organizations processing Sensitive Personal Data in their regular course of business; and (d) organizations possessing critical national information infrastructure with Personal Data.[52] The Implementation Framework also extends this obligation to the Nigerian subsidiary of a multinational company falling within these categories.

In light of the saving provision in the Act that preserves the Implementation Framework and all other regulation issued by the Bureau, it would appear that there is a conflict regarding persons who are required to appoint a DPO. To reconcile it, it is our considered view that provisions of both the NDPR and its Implementation Framework should be read conjunctively. Consequently, in addition to Data Controller of Major Importance, any entity that falls in the above-mentioned categories in the Implementation Framework will be equally mandated to appoint a DPO.

Rights of a Data Subject

A Data Subject has the right to obtain a confirmation as to whether his/her Personal Data is being stored or processed.[53] Upon such confirmation, the Data Subject will be entitled to know the following information and has the following rights: purposes of processing, categories of Personal Data concerned, recipients of the Personal Data, retention period, right to demand erasure of data and right to lodge complaint with the Commission.[54]

The Data Subject is entitled to a copy of the Data Subject's Personal Data in an electronic format.[55] The Data Subject can also demand the correction or deletion of Personal Data where the Personal Data is inaccurate, incomplete, outdated, or misleading.[56] The Data Subject can even demand the erasure of their Personal Data. The Data Subject can restrict the processing of their Data Processing. They have powers to object to the processing of their Personal Data.[57]

Cross-Border Transfer of Personal Data

Prior to enactment of the Act, the NDPR and its Implementation Framework had extensive provisions on cross-border transfer of Personal Data. The NDPR and its Implementation Framework both permitted such transfer subject to the supervision of the Honourable Attorney General of the Federation (the "**AGF**").[58] The Implementation Framework provided that requests for cross border transfer of Personal Data should be forwarded to the AGF.[59] Though the Act does not expressly mention this requirement, it is our position that, unless there is a provision to the contrary, the AGF will continue to provide oversight over cross border transfer of Personal Data.

Under the Act, cross-border transfers of Personal Data are permissible only in specific circumstances.[60] These special circumstances are similar to what is provided in the NDPR.[61] Under the Act, such

[50] S.65, the Act.
[51] S.44, the Act.
[52] Para 3.4.1, NDPR Implementation Framework 2020
[53] S. 34(1)(a), the Act.
[54] Ibid
[55] S. 34(1)(b), the Act.
[56] S. 34(1)(c), the Act.
[57] S. 36, the Act.
[58] Art 2.11, NDPR 2019
[59] Para 7.2, NDPR Implementation Framework 2020.
[60] S. 41(1), the Act
[61] Art 2.12, NDPR 2019

transfers may be permissible if the recipient of the Personal Data is subject to a law, binding corporate rules, contractual clauses or code of conduct that affords an adequate level of protection with respect to the Personal Data.[62] In the absence of an adequate level of protection, a transfer can still occur if any of the following conditions are satisfied:

a. where the Data Subject has consented to the transfer;

b. the transfer is necessary to perform a contract or fulfil the request of a Data Subject;

c. the transfer is necessary in the public interest;

d. the transfer is necessary for resolving legal claims;

e. the transfer is necessary to protect the vital interests of a Data Subject or of other persons that are incapable of giving consent;

f. the transfer is for the sole benefit of the Data Subject and securing the consent of the Data Subject is impractical but likely to be given if possible. [63]

The Data Controller or Data Processor is also responsible for recording the basis for every transfer of Personal Data to another country and the adequacy of protection in that foreign country. [64] Section 42 of the Act stipulates that a level of protection is deemed adequate if it upholds principles that are substantially similar to the conditions for the processing of the Personal Data provided for in the Act.[65]

Sanctions and Penalties

The Act introduced strict sanctions and penalties to deter Data Controllers and Data Processors. Under the Act, the Commission can issue "compliance" and other orders with content such as providing warning, requiring compliance with the Act or commanding persons to cease and desist from engaging in specified conduct. Non-compliance with such orders may attract a sentence of 1 year imprisonment or a fine as set out below, or both.[66]

Upon investigation, the Commission has powers to issue enforcement orders to require remediation, compensation, account for profits realized from the violation, or the payment of penalties/remedial fees of the higher of (a) ₦2,000,000 or 2% of the annual gross revenue in the preceding year for Data Controllers or Data Processors not of Major Importance or (b) ₦10,000,000 or 2% of the annual gross revenue in the preceding year for Data Controllers or Data Processors of Major Importance.[67] Dissatisfied Data Controllers/processors can seek judicial review within 30 days.[68]

The Act also provides that a body corporate or firm who commits an offence, as well as principal officers of the body corporate, shall be jointly liable unless the principal officers prove that the offence was committed without their consent or connivance and they exercised diligence to prevent the commission of the offence.[69] A Data Controller and Data Processor shall be vicariously liable for the acts or omissions of its agent or employee in so far as the acts or omissions relate to its business.

Finally, aggrieved Data Subjects retain the right to seek damages through civil proceedings against erring Data Controllers or Data Processors.[70]

Conclusion

[62] S. 41, the Act.
[63] S. 43, the Act.
[64] S. 41(2), the Act.
[65] Annexure C of the Implementation Framework lists jurisdictions that are deemed to have adequate data protection laws.
[66] S. 49, the Act.
[67] S. 48(2), the Act.
[68] S. 50, the Act.
[69] S. 53, the Act.
[70] S. 51, the Act.

We see the Act as being very largely a rational and most welcome attempt to modernize and give detail to the law on a matter of great importance. The Act creates a robust data protection framework that ensures the responsible handling of Personal Data, protection of individuals' privacy rights, and promotion of trust in the digital economy. We believe that the Act will strengthen the protection of Personal Data through the guidelines established for its lawful collection, transfer, processing and storage.

Authors

Ebimobowei Jikenghan
Senior Associate
ebi.jikenghan@gelias.com

Justice Uka-Ofor
Associate
justice.uka-ofor@gelias.com

Ayomide Abiodun
Associate
ayomide.abiodun@gelias.com

LOCATIONS

LAGOS OFFICE
6 Broad Street
Lagos, Nigeria

T: +234 (1) 460 7890
E: gelias@gelias.com

ABUJA OFFICE
2nd Floor, Abia House,
Plot 979, First Avenue,
Central Business District
F.C.T, Abuja.

T: +234 (1) 888 8881

Practices ● Arbitration ● Banking ● Capital Markets ● Competition ● Compliance ● Corporate ● Data Protection ● Derivatives ● Employment ● Environmental ● Fintech ● Foreign Investment ● Intellectual Property ● Litigation ● Mergers and Acquisitions ● Tax ● ”White Collar” Sanctions ●

Sectors ● Agribusiness ● Commercial Banks ● Commodities ● Construction ● Distributors ● Development Finance ● Electric Power ● Entertainment ● External Trade ● Fintech ● Healthcare ● Infrastructure ● Insurance ● Investment Banks ● Manufacturing ● Media ● Mining ● Oil and Gas ● Pension Managers ● Private Equity ● Real Estate ● Services ● Technology ● Telecommunications ● Transport ●

www.gelias.com