



ALLEN & MARYLEBONE LAW FIRM

A REVIEW OF THE NIGERIAN DATA PROTECTION ACT 2023 IN THE LIGHT OF NIGERIA'S RACE TO CREATE A DIGITAL ECONOMY



1.1 INTRODUCTION

In the European Union, as a rule, the provisions of the General Data Protection Regulation must be complied with while in Nigeria the Data Protection Act just passed around June 2023 must now be complied with in the processing of personal data. Insecurity is a big deal all over the world but even more critical in Nigeria. As the giant of Africa, Nigeria has joined the league of both developed and developing nations that have enacted domestic legislations to protect the incorporeal rights and creativity of its citizens against any undue infringement. This is clearly seen through the enactment by the Nigerian National Assembly of several Intellectual Property regulatory laws such as the Copyright Act 2023 and the Patents and Design Act 2004. However, for long the populous black nation failed to enact an exclusive legislation regulating personal data or personal information of private citizens, even though section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) enshrined the right to privacy it does not suffice in a digital economy. This paper evaluates the new Nigerian Data Protection Act 2023 enacted by the Nigerian National Assembly and assented to in June 2023 by President Bola Tinubu, with occasional reference to the European Union (EU) General Data Protection Regulation (GDPR) 2016 to ascertain what is obtainable under the new Act. The purpose of this analysis is to ensure we briefly capture the spirit and purpose of the Nigerian Data Protection Act 2023 assessing its relevance in a digital economy while giving heads up to stakeholders and practitioners on key provisions worthy of note. Reference is made to the European Union (EU) General Data Protection Regulation 2016 and the UK Data Protection Act as we break down the issues.

KEY PHRASES: Digital Economy, Nigerian Data Protection Act 2023, European Union (EU) GDPR 2016, Facial recognition technology (FRT), Biometric data, Data Controllers, Data Subject, Data Protection,

1.2 Precursor to the Enactment of the Nigerian Data Protection Act 2023

The Constitution of the Federal Republic of Nigeria in section 37 provides for the right to privacy giving the right to every Nigerian not to have his privacy infringed upon without his consent. The Court of Appeal confirms this position in *Federal Republic of Nigeria v Daniel* where the justices declared that undoubtedly, by virtue of the provision of section 37 of the 1999 Constitution (as amended), the privacy of every Nigerian Citizen, their homes, correspondences, telephone and other telegraphic communications are cherishingly guaranteed

In Nigeria privacy regulations have always existed all drawing inspiration from chapter four (IV) of the CFRN 1999 particularly section 37 afore cited. The Freedom of Information (FOI) Act 2011 in its preamble provides that it is: ‘An Act to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences or disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and; for related matters’. From the preamble of the FOI Act 2011, it is clear that the FOI Act 2011 which was set to revolutionize the face of information acquisition and privacy in Nigeria, that the Act sought to regulate privacy of information or data. Section 14 of the FOI Act 2011 goes on to exempt production of personal information by providing inter alia that a public institution must deny an application for information that contains personal information. This provision is specifically geared towards privacy regulation. Such disclosure is only subject to the owner’s consent or where disclosure is necessary for public interest reasons if the public interest reason for disclosure of such information clearly outweighs the protection of the privacy of the individual to whom such information relates.

In 2016 the EU GDPR took off revolutionizing the handling of processing of personal data in the EU and back then also in the UK before Brexit. The regulation was welcomed because it placed more responsibility on companies that process data and ensured that they took extra care in handling personal information of consumers and customers described as data controllers. The EU GDPR further bolstered the provision in the European Convention on Human Rights (ECHR) that the right to having one's personal data protected is fundamental correlated to the right to privacy which is also recognized in section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended). In 2018 the Data Protection Act 2018 was enacted in the UK by the British Parliament following the wind of personal data protection the UK not wanting to leave data protection to chance. The UK being Nigeria's colonial overlord with the large African giant always copying trends from the UK, it was expected that sooner than later the Nigerian scene would also welcome a data protection legislation. Unfortunately, while the National Assembly was indecisive as to passing data protection legislation, the National Information Technology and Development Agency (NITDA) proactively released the Nigerian Data Protection Regulation (NDPR) 2019. Since the regulation put out by NITDA was not a legislation of the National Assembly it lacked the much needed efficacy and publicity even though major firms were already being coerced into upholding provisions of the NDPR. On a continental level the African Union Convention on Cyber security and Data Protection, 2014 and the Economic Community of West African States (ECOWAS) Data Protection Act 2010 had been put in place to, inter alia, provide a common framework for data protection among member states, including Nigeria. However, neither of them is operational in Nigeria at the moment; having not been domesticated. The Nigerian Data Protection Act 2023 now having scaled through sealed with the Presidential assent making it official a keen mind in fact an officious observer would be interested in what the legislation has to say. But particularly it is interesting to see what the legislation says with regard to facial recognition. In the next part it is crucial to consider the EU GDPR which predates the UK Data Protection Act 2018 and the Nigerian Data Protection Act 2023 which is still fresh off the legislative kitchen.

1.3 Highlights of the Nigerian Data Protection Act 2023

Section 37 of the 1999 Constitution (As Amended) is the foundation upon which personal data protection within the Nigerian legal framework is built. The section specifically provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected. Indeed, the right to a private life is connected and intertwined with human dignity, personal autonomy and the right to be left alone. Unfortunately, section 37 falls short of covering the field; hence the need for proper legislation exclusive to the protection of personal data.

(a) Rights under the NDPA 2023

The rights of a data subject under the Act are contained in Part VI (Sections 34 – Section 38). The right to request information from data controllers is provided in section 34 (1). The implication therefore is that anyone can request their data from telecommunications companies or public authorities in so far as such data qualifies as personal data pursuant to section 65 of the Nigerian Data Protection Act which defines personal data as information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, psychological, genetic, cultural, social, or economic identity of that individual. The data subject's consent is at the center of processing and can be withdrawn at any time without reason. The data subject is also allowed the right to object to data processing. Section 37 provides inter alia that a data subject shall not be subject to a decision solely based on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject. Exceptions are provided for in section 37 (2). Thus, automated processing is allowed where the decision is necessary for entering into or the performance of a contract between the data controller and the data subject, also where it is pursuant to written law although the law must ensure fundamental rights are protected and there are safeguards. Also, where the data subject consents, automated decision making is allowed.

(b) Regulatory Framework and Enforcement

The NDPA 2023 establishes the Nigerian Data Protection Commission consisting of a National Commissioner and other staff of the Commission. Importantly, the functions of the Commission and the powers of the Commission are enumerated in section 5 of the Act to wit;

- i. regulation of deployment of technological and organizational measures to enhance personal data protection;
- ii. fostering the development of personal data protection technologies, in accordance with recognized international best practices and applicable international law;
- iii. accredit, license, and register suitable persons to provide data protection compliance services;
- iv. registration of data controllers and data provisions of major importance;
- v. promotion of awareness on the obligation of data controllers and data processors under the NDPA 2023;
- vi. promotion of awareness to the public of personal data protection, rights and obligations, and possible risks, helping the public understand better the rights under the NDPA 2023;
- vii. handling complaints associated with violations of the NDPA or other subsidiary legislation made under the Act,
- viii. inter agency collaboration;
- ix. ensuring compliance with natural and international best practices and obligations over personal data protection;
- x. collaboration with other national and regional data protection authorities, etc.

The Commission is to also oversee cross border transfer of personal data; collection and publication of information on personal data protection and personal data breaches; advising government on policy issues relating to data protection and privacy; submitting legislative proposals to the Minister of Information and Communication for strengthening personal data protection in Nigeria. A perusal of the provisions of the Act on the functions of the Commission shows that the Commission is the primary enforcer of the legislation with the responsibility to oversee compliance. The crucial question then is whether the compliance role would not clash with the role already being played by NITDA pursuant to the NITDA Act?

It appears that 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.

(c) Data Controller of ‘Major Importance’

Section 5 (d) jumps at a curious reader; it states that the Commission shall play the function to ‘register data controllers and data processors of major importance’. Who decides or what parameters would be used to determine which company or institution is a data controller of importance? Would it be the volume of personal data collected, stored, or processed? Would it be the share capital might of the company? Would it be the sector of operation of the company? In other words, what is the profile of a company described as a data controller or processor of major importance? If these questions were left unanswered by the Act, it would have been a draftsman blunder but section 65 of the NDPA 2023 did define what a data controller or processor of major importance means. Section 65 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. On the other hand, a data processor is 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 data processor. This leads us to inquire what processing now means. Processing by section 65 consist of any operation or combination of operations performed on personal data whether by automated means or not and may consist of collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use disclosure by transmission, dissemination, or otherwise making available a ligament combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria. There are many things to unpack from the definition of processing. However, let us not lose focus on the original query of knowing what data controller of major importance means. According to section 65 ‘data controller of major importance’ means

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 circumstances may designate.

The foregoing definition is quite unsatisfactory because it still leaves the parameters open to be decided subsequently by the Commission. This automatically places a responsibility on the Commission to come up with an explanatory memorandum or subsidiary legislation clarifying the position on who a data controller of major importance is. Any such explanatory memo would tell us the amount of data to be controlled or processed to make one a data controller of major importance or what nature of data affecting the economy, security, or society that bestows the title of major importance on the data controller.

(d) Powers of the Nigerian Data Commission

The Powers of the commission are enumerated in section 6(a) – (h) and while all the powers are of importance what could be described as the major powers are in sections 6(a) – (g). Thus, the commission is empowered to oversee implementation of the NDPA 2023; prescribe fees payable by Data Processors and Controllers; prescribe frequency, content and manner of filing compliance of returns by data controllers and data processors of major importance; investigate violations and violators of the Act. The Commission purports to be independent in the performance of its functions, another seeming impossibility considering what the INEC and the Judiciary currently suffers within the Nigerian nation from lack of fiscal independence even though on paper total autonomy is what was promised.

(e) The Council of the National Data Protection Commission

A governing Council consists of about seven members who run the commission as part time members except the National Commissioner. The Chairman of the Council is a part time member and must be a retired Judge working collaboratively with the National Commissioner. The Council is the functional working machinery of the commission. Other important provisions on the activities of the Council are in Part II of the Act. Art III provides for the appointment of the National Commissioner and other staff of the Commission. The National Commissioner is appointed by the President on the recommendation of the Minister of Information and Communication. The National Commissioner is the chief executive and accounting officer of the Commission responsible for execution of policies and administration of the affairs of the commission. Section 14 to section 17 speaks to the tenure, qualification and role of the National Commissioner in the Council.

(f) Lawful Processing – CONSENT

The requirement of consent stands as one of the foremost safeguards provided by all the personal data legislations and regulations the world over and the Nigerian Data Protection Act 2023 is no different. Under EU and UK law, consent as a basis for lawful data processing is fully established in Article 6 of the General Data Protection Regulation (GDPR) 2016 and is also explicitly referred to in Article 8 of the EU Charter on Human Rights. Section 26 of the NDPA 2023 is all about consent of the data subject placing the onus of proof of consent on the data controller. So for example if I assert that I did not grant consent to say MTN to use my personal information to run adverts the onus is not on me but on MTN to show that MTN duly and validly obtained my consent. Consent has to be freely given not coerced or incurred via undue influence. Consent must also be informed expressing right to affirm or withdraw at any time. Silence or inactivity does not constitute consent or allow room for presumption of valid consent, rather consent must be either oral, written or through electronic means.

(g) Principles and Safeguards under the Nigerian Data Protection Act

Principles and safeguards refer to certain fundamental guide which data controllers and data processors must take in handling personal data to ensure there is no breach. These are contained in section 24 of the NDPA Act 2023 consisting of principles of lawfulness, data minimization, purpose limitation, transparency, consent, pseudonymization, data protection by design, etc. These basic principles provided by the NDPA Act 2023 serve to protect data subjects. One safeguard that can provide protection against the abuse of personal data by data controllers is pseudonymization. According to Section 65 of the NDPA 2023 Pseudonymization is the substitution of direct identifiers in a way that data can no longer be attributed to a specific data subject without the use of additional information. principles of data minimization and purpose limitation are also safeguards guaranteed under the NDPA 2023. The principles of data minimization require personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Note that, big data analytics truncates this very principle and becomes an antithesis of data minimization as it requires more and more data, often for unspecified purpose. On the other hand, purpose limitation requires that data must be processed for specified aims and cannot be used for purposes incompatible with the initial purpose of collection, unless such processing is based on a legal ground such as, but not limited to, consent of data subject. The principles of transparency in processing and accuracy also form safeguards to protect personal data from being exploited negatively. The safeguards so far highlighted are effective and if adhered to by data controllers would ensure a secure regime of personal data processing.

1.4 Overview of the Digital Economy and Role of the Nigerian Data Protection Act 2023

Digital Economy best describes a series of economic activities that integrate, analyze, add value and trade digital resources with digital information as the source of value, virtual platform as the operating carrier and information technology as the innovative means. The migration from traditional economy to digital economy has been swift, cataclysmic and disruptive all at once. The quick transition has also been global with every country quickly transforming or seeking to transform every activity from brick and mortar structure to digitalized structure. The digital economy has played and continues to play a stabilizing role in the global economic fluctuation. Consequently, even during the Covid-19 pandemic rather than take a halt there has been expansion. In the Far East China, the digital economy has become the key driving force for stable economic development especially between 2015 and 2020. The global digital economy has increased from 40.3% of GDP in 2018 to 41.5% of GDP in 2019 with both developed and developing countries enjoying varying degrees of growth in the digital economy. In China, the growth rate is 9% with the added value in 2020 exceeding 39 trillion Yuan, rising from 27% to 38.6% and becoming an important part of China's economic system. Worldwide, tax authorities have realized that tax knowledge and good forward thinking policies will lead to better tax compliance in the digital economy. The entire digital economy is worth almost 22% of world GDP and is growing at an unprecedented rate mainly because the digital drive maximizes the web as much as every available gadget and internet enabled medium. The web is universal and the profits generated seem to flow to a limited number of operators who have established their dominant presence in the world market. It appears that the seamless infrastructure of global business allows for easy access to utilizing of personal data in the digital economy. Nigeria's best bet to positioning for maximizing the digitization of everything is through passing the right type of legislation to meet emerging trends. The Nigerian Data Protection Act 2023 is actually late to the party but it is better late than never. The Act can play the role of being the go to guide to industry stakeholders and regulators but it must be strictly enforced fairly across board.

1.6 Conclusion and Recommendation

After a review of the Nigerian Data Protection Act 2023, it is clear that the Act seeks to protect the rights of citizens and has provided safeguards such as the requirement of conducting lawful and transparent processing; conducting Data Protection Impact Assessment (DPIA), requirement of consent, data minimization, purpose limitation, pseudonymization etc. Since the mid-1990's, the digital economy has evolved rapidly, first into the internet economy, then the data-driven economy and now the algorithmic economy in which the ability to use artificial intelligence is higher than it has ever been in history. In a data driven economy personal data and big data are two inextricable sides to the same coin. AI's ability to work with data analytics is the primary reason why artificial intelligence and big data are now seemingly inseparable. So personal data have assumed economic value and corporations by repurposing personal data via the components of A.I. and Big Data seek to maximize profit. This is why the NDPA 2023 is so crucial to building a digital economy in Nigeria. The safeguards provided under the Act seeks to ensure there remains some semblance of sanity as more and more corporations play in the area of Big Data analytics. The way forward is for data controllers to immediately seek expert knowledge on compliance with this legislation. In fact, there should be a rush for Data Protection Officers because the consequences for running afoul of the Act are dire. Lawyers are also given a great area of specialization to hone their skills and expand their portfolio as data protection officers or practitioners. We shall observe to see how implementation of the Act fares because it is one thing to pass a robust law such as this; the implementation is a different ball game entirely.

Bibliography

Primary Sources

Statute (s)

1. **Charter of Fundamental Rights of the European Union [2012] O J C326/391**
2. **Constitution of the Federal Republic of Nigeria 1999 (As Amended 2018), Cap C23 Laws of the Federation of Nigeria 2004 (Updated)**
3. **Copyright Act 2004 Cap C28 LFN 2004**
4. **Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms* 4 November 1950 ETS 5**
5. **Data Protection Act 2018, (signed on 23rd May 2018, commenced in May 2018)**
6. **Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA**
7. **Freedom of Information (FOI) Act 2011**
8. **Nigerian Data Protection Act 2023**
9. **National Information Technology Development Agency ('NITDA') Act 2007**
10. **Nigerian Data Protection Act 2023**
11. **Patents and Design Act 2004 Cap P2 LFN 2004**

12. Police and Criminal Evidence Act 1984

13. Regulation (EU) 2016/679 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 (General Data Protection Regulation) [2016] OJ L199/1

Case(s)

14. *Federal Republic of Nigeria v Daniel* [2011] LPELR – 4152 (CA)

Secondary Sources

15. Afolabi B, 'Tinubu Signs Data Bill into Law' (*The Punch Newspaper*, 14 June 2023) <<https://punchng.com/tinubu-signs-data-protection-bill-into-law/>> accessed 23 November 2023

16. African Union Convention on Cyber Security and Personal Data Protection (the Convention) 2014

17. Agh J, 'The Impact of the GDPR on Big Data' (*Tech GDPR*, 1 December, 2020) <<https://techgdpr.com/blog/impact-of-gdpr-on-big-data>> accessed 1 June 2022

18. Aina D, 'FG to Install Facial Recognition Technology at Airports' (*The Punch Newspaper*, 22 March 2023) <<https://punchng.com/fg-to-install-facial-recognition-technology-at-airports/>> accessed 23 November 2023

19. Article 29 Data Protection Working Party, *Opinion 02/2012 on facial Recognition in Online and Mobile services* (Article 29 Working Party, 22 March 2012) <https://ec.europa.eu/justice/data-protection/index_en.htm> accessed 11 November 2023

20. Boccia F, 'The Digital Economy and Fiscal Policy in the Age of E-Commerce' in Francesco Boccia & Robert Leonadi (eds); *The Challenge of Digital Economy: Markets Taxation and Appropriate Economic Models* (Springer International Publishers, 2017)
21. Bornman M and Wassermann M, 'Tax Knowledge for the digital economy' (2020) 13 (1) *Journal of Economic & Financial Sciences*
22. Bottis M and Bouchagiar G, 'Personal Data V Big Data; Challenges of Commodification of Personal Data' (2018) (8) 206 - 215 *Open Journal of Philosophy*. <<https://doi.org/10.4236/ojpp.2018.82015>> accessed 21 November, 2022
23. Chivot E and Castro D, 'The EU Needs TO Reform The GDPR To Remain Competitive In The Algorithmic Economy' (*Center for Data Innovation*, 13 May 2019) <<https://datainnovation.org/2019/05/the-eu-need-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>> accessed 20 November, 2023
24. European Union Agency for Fundamental Rights and Council of Europe (CoE) *Handbook on European Data Protection Law* (European Union Agency for Fundamental Rights and Council of Europe, 2018) 360
25. Faga P, 'Limits of copyright protection in contemporary Nigeria: re-examining the relevance of the Nigerian copyright act in today's digital and computer age' *Nnamdi Azikiwe Journal of International Law*, [2011] (2) 211-225, available at <<https://www.ajol.info/index.php/naujilj/article/view/82405>> accessed 20 November 2023
26. Kindt E J, *Transparency and Accountability Mechanisms for Facial Recognition* (GMF Policy Brief 2021)
27. Maryville University, 'Big Data and Artificial Intelligence: How They Work Together' (Maryville University, 2022) <<https://online.maryville.edu/blog/big-data-is-too-big-without-ai/>> accessed 10 June 2022

28. Olomjobi Y, 'Right to Privacy in Nigeria' (31 October, 2017) Available at SSRN: <<https://ssrn.com/abstract=3062603>> or <<http://dx.doi.org/10.2139/ssrn.3062603>> accessed 23 November, 2023
29. Tang Rui, 'Digital economy drives tourism development – empirical evidence based on the UK (2022) Economic Research – Ekonomska Istrazivanja DOI: <<https://doi.org/10./080/1331677X.2022.2094443> > accessed 27 November, 2023
30. Yang H, Lei Y, Shu Y, and Kan X, 'The Impact of Digital Economy on Tax Collection and Management system and its Counter Measures' (2022) (6) (2) *Frontiers in Business Economics and Mgt* 193

CONTRIBUTORS



OBINNA AKPUCHUKWU

Partner

+234(0) 906 715 8192.

o.akpuchukwu@allen-marylebone.com

CONTACT US

Abuja Office: Ventures Park, No 5 Kwaji Close, Maitama, Abuja.

Onitsha Office: No 9 Tasia Road, Off Awka Road by ABS Junction, Onitsha, Anambra State, Nigeria.

Telephone: +234 906 715 8192, +234 803 510 5706

Email: info@allen-marylebone.com

Website: www.allen-marylebone.com