AN ANALYSIS OF THE DATA PRIVACY AND PROTECTION LAWS IN NIGERIA

BY EMEKA EKWEOZOR ESQ.[1]

ABSTRACT

Data protection and reliability are top priority issues in this digital age. With the advent of new technologies, the need to protect one's privacy is becoming of ever greater importance. The advent of information technology has created an environment where personal and organizational data can easily be assessed by anyone if they are not properly protected[2]. Besides, the undeniable fact that people's lives are now becoming woven around continuous exchange of information, and streams of data, means that data protection is gaining importance and moving to the centre of the political and institutional system[3]. Thus, most countries have taken a stance on data protection in order to enforce laws, prevent crime and adopt in diplomatic relationship[4]. Moreover, the fundamental right to protection of personal data is recognised at the universal level in various human rights instruments adopted under the aegis of the UN[5], mostly as an extension of the right to privacy. It is an inalienable human right also guaranteed by the Nigerian. However, the growing subscription of customers to online services offered by the financial, trading and telecommunications companies in Nigeria, as well as the increasing rate of identity theft and other cyber misdemeanours have necessitated the need for data protection legislation that aligned to international standards .

LEGAL REGIME OF DATA PROTECTION IN NIGERIA

According to the Section 1.3 of the Nigerian Data Protection Regulation, 2019[6],

> **"Data" means characters, symbols and binary on which operations are performed by a computer. Which may be stored or transmitted in the form of electronic signals is stored in any format or any device;)**
>
> **"Database" means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases;**

---

[1] Emeka Ekweozor is a litigation and corporate law practitioner and an LLM Candidate based in Lagos. (accessible at emekaekweozor@gmail.com)

[2] Abubakar Sanni Aliyu , *The Nigeria Data Protection Bill: Appraisal, Issues, And Challenges*, The Innovative Issues and Approaches in Social Sciences Journal, Vol. 9, No. 1, 2016

[3] European Union Agency for Fundamental Rights (2010). *Data Protection in the European Union: The Role of National Data Protection Authorities*. Luxembourg: Publications Office of the European Union.

[4] Davoli, A. (2011). Personal Data Protection. Available online at http://www.europarl.europa.eu/ftu/pdf/en/FTU_4.12.8.pdf.

[5] See Article 12 of the Universal Declaration of Human Rights (UDHR) protects the right to private life.

[6] Hereinafter referred to as the NDPR

> **"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;**
>
> **"Personal Data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;**

Data protection is commonly defined[7] as the law designed to protect your personal data. In modern societies, in order to empower us to control our data and to protect us from abuses, it is essential that data protection laws restrain and shape the activities of companies and governments. These institutions have shown repeatedly that unless rules restricting their actions are in place, they will endeavour to collect it all, mine it all, keep it all, share it with others, while telling us nothing at all. There is presently no specific or comprehensive data privacy or protection law in Nigeria.[8] The only legislation that provides for the protection of the privacy of Nigerian citizens in general terms is the Constitution of the Federal Republic of Nigeria (Promulgation) Act.[9] Section 37 of the Constitution provides that:

> **"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected"[10].**

Other than this constitutional provision, there is no other law that sets out detailed provisions on the protection of the privacy of individuals in Nigeria. There are however, a few industry-specific and targeted laws and regulations that provide some additional privacy-related protections.

Nigeria does not have any omnibus data protection law that is comparable to that in operation in other countries like South Africa, Canada and countries in the European Union (EU). In other words, there is no single legislation focusing solely on data privacy regulations in Nigeria at the moment.[11] The closest that Nigeria has to a data protection regulation appears to be the Draft Guidelines on Data Protection published by the National Information Technology

---

[7] 7 UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, para 10.

[8] Akindele, Roland (2017) *"Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system," Journal of International Technology and Information Management:* Vol. 26 : Iss. 4 , Article 4. Available at: http://scholarworks.lib.csusb.edu/jitim/vol26/iss4/4

[9] Chapter C23, Laws of the Federation of Nigeria 2004 (as amended) (the "Constitution")

[10] In the context of communications services, this constitutional provision was asserted in Emerging Markets Telecommunication services LTD v. Barr. Godfrey Nya Eneye (2018) LPELR-46193 (CA), where the Plaintiff claimed that Etisalat's unauthorised disclosure of his mobile number to third parties, who subsequently sent a flood of unsolicited SMS' to his phone violated his right to privacy. In giving judgment against Etisalat, the court stated, "the innumerable text messages without [Plaintiff's] consent … is a violation of his fundamental right to privacy".

[11] Jovan Kurbalija. (2017). 'An Introduction to Internet Governance' https://www.diplomacy.edu/resources/books/introduction-internet-governance, p. 211.

Development Agency[12]. Clause 1.2 of the Guidelines provides that the authority for the Regulations is in accordance with the NITDA Act 2007 and that they are issued in pursuance to Sections 6, 17 and 18 of the NITDA Act. It should be noted that the guidelines can at best be described as soft codes as there are no mandatory provisions.[13]

THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY ("NITDA/THE AGENCY")

This was set up by the National Information Technology Development Agency Act 2007[14] as the statutory agency with the responsibility for planning, developing and promoting the use of information technology in Nigeria. The NITDA Act also empowers the Agency to do the following:

> **"Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information".**

It was further to the foregoing powers that on 28th January 2019, NITDA published its Data Protection Regulation ("the Regulation") which aims at protecting personal data of all Nigerians and non-Nigerian residents in Nigeria. The NITDA Guidelines define "personal data" as:

> **"any information relating to an identified or identifiable natural person (data subject); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address".**

The Regulation designates the NITDA as 'the Agency' to administer the Regulation[15], and gives it various powers, for example to licence Data Protection Compliance Organisations, to receive audit information, to make adequacy decisions in relation to foreign countries, and to develop and manage international cooperation mechanisms.

The Regulation applies to

> **"all transactions intended for the processing of personal data, to the processing of personal data notwithstanding the means by which the data**

[12] See also The Nigerian National Policy for Information Technology 2000. The IT Policy has as one of its general objectives the promotion of legislation (Bills & Acts) for the protection of online, business transactions, privacy and security.

[13] *Personal Data Protection In Nigeria*; World Wide Web Foundation (March 2018) accessible at http://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf

[14] ACT NO. 28 PUBLISHED IN THE FEDERAL REPUBLIC OF NIGERIA OFFICIAL GAZETTE NO. 99 VOL. 94 LAGOS 5TH OCTOBER 2007

[15] See the preamble to the NITDA Regulation

processing is being conducted or intended to be conducted in respect of natural persons in Nigeria" [16]

The Regulation defines the "Data Administrator as a person or an organization that processes data.[17] "Data Controller" is defined as a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for or the manner in which personal data is processed or is to be processed.[18]

Data Processing Principles:
Personal data shall be:
(a) "Collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject;
(b) Adequate, accurate and without prejudice to the dignity of the human person;
(c) Stored only for a period within which it is reasonably needed; and
(d) Secure against all foreseeable hazards and such as theft, cyber-attack, viral attack dissemination, manipulation of any kind, damage by rain, fire and exposure to other natural elements."[19]

Lawful processing of personal data requires
(1) consent of the data subject;
(2) for the performance of a contract;
(3) for compliance of a legal obligation;
(4) to protect the vital interests of the data subject; and
(5) for the performance of a task carried out in the public interest.[20]

The Regulation stipulates that organizations are responsible for the personal data that is in their custody or control. Organizations owe a duty of care to the Data Subject and also are accountable for all acts and omissions of data processing.[21]

13 3.3 Third-Party Contracts:
A Data Controller shall enter into a written contract with any third-party processing data on its behalf. In addition, if an organization engages a third party to handle personal data collected by the organization, the organization is also responsible for the third party's compliance with the Regulation.[22]

Organizations can contract with service providers, including cloud computing service providers to process and store client and employee personal information. The service providers can be located outside Nigeria. However, if an organization does use a foreign service provider, the

[16] NDPR, at Art. 1.2 (a)
[17] Ibid at Art. 1.3(ix).
[18] Ibid at Art. 1.3(x).
[19] Ibid Art. 2.1(1)(a – d).
[20] Ibid at Art. 2.2 (a-e).
[21] Ibid at Art. 2.1 (2 & 3).
[22] Ibid at Art. 2.7.

processing shall be subject to the Regulation and supervision of the Honourable Attorney General of the Federation ("HAGF").[23]

In addition, the organization must include in its policy the access (if any) of third parties to personal data and purpose of access.

3.4 Privacy Policy: Organizations must display a "simple and conspicuous" and easily understandable privacy policy that contains specified content. The Regulation requires the organizations to develop and follow privacy policies that are reasonable and as stipulated under regulation 2.5 (a–i), so that the organization meets its obligations under the Regulation.

3.5 Consent: There are specific requirements for obtaining consent. This is an important and crucial requirement of the Regulation. Section 2.1 of the Regulation stipulates that the "data subject" who is generally any identifiable person, must consent before any data is collected and that personal data must be collected and processed in a lawful manner. Organizations may only collect, process and disclose personal data for purposes that are reasonable and only to the extent that it is reasonable for meeting the purposes for which the information was collected.[24] Data Controllers may also only process the collected personal information for the purposes for which the information was originally collected.[25]

3.6 Data Security: Article 2.1(d) of the Regulation stipulates that personal data shall be:

> **"secured against all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements".**

The breach of data security amounts to a loss of privacy. Hence, Article 2.6 stipulates measures to protect personal data. The Data Controller is to ensure the security of personal data collected. We would advise that the Data Controller should establish security measures that reflect the sensitivity of the personal data it collects and handles. Highly sensitive personal data would require the most security, while anonymous data would require the least amount of protection. Individuals that suffer loss of privacy may use the Regulation to initiate proceedings against organizations that disclose personal information without authorization due to a security breach. However, the Regulation does not provide a procedure to follow where there is a breach. One would expect that an organization that suffers a security breach would notify the NITDA of an incident that involves the loss of, unauthorized access to, or disclosure of personal data that may pose a real risk of significant harm to individuals. The organization should also notify the affected individuals and organizations may do so under their own initiative. Furthermore, it is advisable for organizations to notify data subjects of available remedies in the event of a breach of their privacy policy and the time frame for the remedy.

3.7 Implementation: The Regulation sets out specific provisions for implementation for both public and private organizations and they include the following:

[23] Ibid at reg. 2.11
[24] Ibid at reg. 2.2.
[25] Ibid at reg. 2.3.

i. All organizations that control personal data shall within 3 months of the issuance of the Regulation, release to the public their data protection policies, which shall conform with these Regulations;[26]
ii. There shall be a Data Protection Officer, to ensure compliance with the Regulations;[27]
iii. Within 6 months after the date of issuance of the Regulations, an Organization must conduct an audit of its privacy and data protection services;[28]
iv. Where a Data Controller processes the personal data of more than 1000 data subjects in a period of 6 months, it shall submit a soft copy of the summary of the audit to the Agency;[29]
v. Where a Data Controller processes the personal data of more than 2000 Data Subjects in a period of 12 months, it shall submit a summary of its data protection audit to the Agency.[30]

FREEDOM OF INFORMATION ACT

The Freedom of Information[31] enables public access to public records and information, prevents a public institution from disclosing personal information to the public unless the individual involved consents to the disclosure. The provisions of the Freedom of Information[32] also impacts on the protection of the information of individuals in Nigeria. Although the FOI Act was promulgated to, amongst other things, make public records and information more freely available and to provide for public access to public records and information, the FOI Act limits this right of access to information in certain circumstances. Under section 14 of the FOI Act, a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Personal information is defined as "any official information held about an identifiable person but does not include information that bears on the public duties of public employees and officials". Section 16 of the FOI Act also provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege and journalism confidentiality privilege). In addition to the foregoing, the Nigerian Courts have also provided some guidance on this matter.

In the case of **Habib Nigeria Bank Limited v. Fathudeen Syed M. Koya**[33] which involved an alleged disclosure by a bank of a customer's transactional information, the Court of Appeal held that it is elementary knowledge that the bank owed its customer a duty of care and secrecy. This case indicates that other than the statutory protection afforded to information provided to lawyers, doctors and journalists, certain persons (such as banks) owe a duty to maintain confidentiality to their clients - even though such duty is not expressly prescribed by law. One concern that often arises for employers, in the absence of specific data protection legislation, is in relation to the collection, storage, processing, management and treatment of personal

[26] Ibid at reg.4.1(1).
[27] Ibid at reg. 4.1(2).
[28] Ibid at reg. 4.1(5).
[29] Ibid at reg. 4.1(6).
[30] Ibid at reg.4.1(7).
[31] Act No. 4 of 2011
[32] (the "FOI Act")
[33] (1992) 7 NWLR Pt.251 P43 at 57 and 58)

information of employees. This concern, which is common amongst multi-national corporations that usually have a centralised data-base where the employees' personal details are retained, arises from the fact that the language of section 37 of the Constitution is very wide and could be breached in circumstances where it can be established that personal information such as the names, telephone numbers and addresses of employees who are Nigerian nationals have been published or disseminated without the consent of such individuals. In the absence of specific protections under the law, it appears that the only protection available to employers is contractual and as such employers are usually advised to ensure that the terms of each employee's contract of employment (which in Nigeria has been held to include the employees/staff manual) contains a provision pursuant to which an employee consents to the purpose, the treatment and the use by the employer, of any personal information provided by the employee to the employer in the context of the employment relationship.

CYBER-CRIMES ACT

The Cybercrimes Act 2011 prevents the interception of electronic communications and imposes data retention requirements on financial institutions.

THE CONSUMER CODE OF PRACTICE REGULATIONS 2007

The Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission requires telecommunication operators to take reasonable steps to protect against "improper or accidental disclosure" and must ensure that such information is securely stored. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations". The Consumer Protection Framework issued by the Central Bank of Nigeria in 2016 contains provisions that restrain financial institutions from disclosing the personal information of their customers. It has however been evident that though these preceding pieces of legislation exist, there had been no comprehensive data protection and data privacy legislation in Nigeria.

One such industry-specific regulation is the Consumer Code of Practice Regulations 2007 (the "NCC Regulations") issued by the Nigerian Communications Commission ("NCC") - the regulator of the telecommunications industry in Nigeria). The NCC Regulations provide that all licensees must take reasonable steps to protect customer information against "improper or accidental disclosure" and must ensure that such information is securely stored. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations". Unlike the Constitution, the application of the NCC Regulations is not restricted to Nigerian citizens; they apply to all customer information relating to customers of any nationality that use a licensee's network.

THE NATIONAL IDENTITY MANAGEMENT COMMISSION ACT (NIMC ACT) 2007: Establishes the national identity database and the National Identity Management

Commission (NIMC) charged with maintaining the national database, the registration of individuals and issuance of general multipurpose identity cards.

THE NIGERIAN COMMISSIONS ACT (NCA) *2003*: Provides, amongst other things, for: the reform of the Nigerian Communications Commission (NCC) as an independent regulatory body for the communications sub-sector; the establishment of the National Frequency Management Council; and the establishment of the Universal Service Fund.

The Wireless Telegraphy Act 1998 (WTA): Regulates wireless telegraphy in Nigeria.

INTERNATIONAL LEVEL

AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION *2014.* The African Union Convention on Cyber Security and Personal Data Protection (the Convention) is an international legal instrument entered into by the members of the African Union (AU), including Nigeria. Respecting data protection, the Convention has the goal to address the need for a harmonised legislation in the area of cyber security in member states of the African Union, and to establish in each state party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. However, the Convention — like any international treaty entered into by the government of Nigeria — does not acquire the force of law in Nigeria, until enacted into law by the National Assembly, pursuant to Section 12 of the Constitution.

Nigeria's regional obligations Nigeria is the 26th African country to regulate data privacy (of 54 African Union member states), and the 134th in the world. It is not yet a signatory to the African Union's data protection Convention.

SUPPLEMENTARY ACT ON PERSONAL DATA PROTECTION WITHIN ECOWAS (THE ECOWAS DATA PROTECTION ACT On 16 February 2010, the signatories of the ECOWAS7 Treaty, including Nigeria, adopted the ECOWAS Data Protection Act on the protection of personal data within ECOWAS member states. The ECOWAS Data Protection Act obligates member states to establish a legal framework of protection of data privacy relating to the collection, processing, transmission, storage, and use of personal data, subject to the general interest of the state8. However, the ECOWAS Data Protection Act is yet to acquire the force of law, pursuant to Section 12 of the Constitution.

CHALLENGES OF THE DATA PRIVACY AND PROTECTION IN NIGERIA

Personal information protection is an integral part of fundamental rights architecture. Currently, Data protection is a complex issue and has become a topical issue in recent times. Despite the benefits of the NDPR, this regulation does not consider privacy protection online, access to the internet, video surveillance, search engines and social networking. All these are

current challenges to the effective enforcement of the Act. The lack of a comprehensive database and Data Protection Authorities/Commissioners, as is the case for best pratices, may pose a major challenge for the enforcement of the Act. The process involved in obtaining information about an individual may cause delays in some important legitimate activities. For instance, it may hinder effective criminal investigation by authorised agencies. Individuals may take advantage of data protection laws to perform illegitimate actions, since to a large extent, they can influence who get access to their personal data and information. The Bill may constrain legitimate users of information (e.g. embassies, financial institutions, police, educational institutions, employees, etc) from obtaining adequate information about an individual and taking appropriate decisions based on such information.

The Regulation may propel companies doing business in Nigeria, especially those involved in marketing activities to review their business procedures relating to capturing and employing of personal data. The NDPR may cause a collision between the right to know and the right to privacy. Besides, it may negate the objectives of transparency, whistle blowing, freedom of information, and some code of conduct rules. There is also a Dearth of judicial decisions on data privacy violations which is intrinsic in the development of further judicial activism.[34] The regulation solely "applies to all transactions intended for the processing of *personal data* and to actual processing of *personal data*... and to natural *persons* residing in Nigeria or residing outside Nigeria but of Nigerian descent."[35] The NDPR applying solely to *personal data* and *natural persons* means the regulation excludes other forms of data and corporate organisations respectively.

RECOMMENDATIONS

Enact a Data Protection Act: Enact into law a Data Protection Act that contains data protection principles consistent with those contained in the African Union Convention on Cyber Security and Personal Data Protection and/or the EU's General Data Protection Regulation (GDPR).[36]

Amend the NIMC Act: Amend the NIMC Act to incorporate robust data protection principles and expand the powers of NIMC to function as a data protection authority to ensure that public and private institutions in Nigeria comply with the data protection principles when processing personal data.[37]

Enact a Child Online Privacy Protection Act: Enact an Act that includes basic standards of practice by online platforms in the online collection and use of information from children.

Engage the National Human Rights Commission (NHRC) to enforce data protection cases: The NHRC should enforce cases of personal data protection breaches by exercising its Section 5 (a) and (b) functions, which respectively authorise it to deal with human rights matters and their

[34] Olumide Babalola, *Data Protection And Privacy Challenges In Nigeria (Legal Issues)*, (2020) accessible at **https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-**

[35] Section 1.2 NDPR, 2019

[36] Abubakar Sanni Aliyu , The Nigeria Data Protection Bill: Appraisal, Issues, And Challenges, Supra Note 2

[37] Ibid

breaches, under the NHRC Act. The basis for this recommendation is that data protection is a substantive legal issue grounded in the right to privacy, as guaranteed by the Constitution.

Engage the Consumer Protection Council (CPC) to provide redress: Exercise its Section 2 (i) function under the CPC Act to provide redress to obnoxious practices or the unscrupulous exploitation of consumers. This study argues that the "obnoxious practices" or "unscrupulous exploitation" of consumers contemplated by Section 2 (i) also includes matters of data protection.

Ensure that the NIMC and sector-specific regulators with consumer protection authority (including the CPC and NCC) take action: Mandate data protection by design and transparency obligations by specifying that Ministries, Departments or Agencies, and regulated organisations (including online platforms) acting as data controllers implement data protection by design in systems, processes and technologies that process personal information.[38]

CONCLUSION

This NDPR ensures that the protection of personal data in Nigeria is in consonance with developing global best practices and fills the gap in the regulation of privacy rights and data protection in Nigeria. However, there is urgent need for a substantive data protection act in the absence of a comprehensive legislation from the National Assembly. In the era of technological proficiency and raging increase in cyber misdemeanours, it is in the interest of the citizenry that urgent steps in the form of water-tight legislation are taken to ensure rights of citizens are thoroughly protected.

For further information on this article and area of law, please contact Emeka Ekweozor Esq. at Dr.Paul C. Ananaba SAN & Co., Lagos by Mobile (+234 7063794206; 08110658699) Mobile and Email: emekaekweozor2@gmail.com; emekaekweozor@yahoo.com

[38] Ibid