UNIVERSITY OF TARTU
SCHOOL OF LAW
Department of Public Law

Adelayo Adenike Banjo

THE ACTUALISATION OF PERSONAL DATA PROTECTION IN NIGERIAN LAW: AN ANALYSIS OF PERSONAL DATA PROTECTION IN THE NIGERIAN AND EUROPEAN UNION LEGAL SYSTEMS

Master's thesis

Supervisor
dr. iur. Paloma Krõõt Tupay

Tallinn
2020

TABLE OF CONTENTS

INTRODUCTION

At the time of entry into force of the International Covenant on Civil and Political Rights,[1] the right to privacy, which the right to personal data protection is closely connected with, was adequate in the protection of individuals from arbitrary or unlawful interference with their privacy, family, home or correspondence.[2] However, technological advancements and the widespread use of computers, mobile phones and the internet for daily activities necessitated a development in the laws to address issues such as the protection of personal data that has been made public, which arose as a result of these advancements.

Technological advancements cannot be overstated as the world has become a global village such that goods, services and information can be exchanged from the northern hemisphere to the southern hemisphere in less than an hour and these have benefitted both individuals and countries' economies. Additionally, these technological advancements have also aided the digitisation of information by governments and its agencies, corporations and even private persons through the collection and processing of personal data. Notwithstanding the advantages, the borderless nature of the internet, challenges which its regulation has posed for states, the invasion of privacy and the wide spate of crimes associated with the use of the internet such as identity theft, spamming and threat of viruses are some of the drawbacks of the technological advancements which have necessitated data protection laws and regulations.

Technological advancements and the risks associated with it led to the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) by the Council of Europe in 1981.[3] It was the first international instrument to guarantee the protection of individuals against abuses that arise from the collection and processing of personal data. In addition, the European Union (EU) in Article 8 of the European Charter of Fundamental Rights (the Charter),[4] which became legally binding in the EU in December 2009, guarantees the protection of personal data and it was the first time that the protection of personal data was acknowledged as a fundamental right at an international level. In 2016, the General Data Protection Regulation (GDPR)[5] which became

[1] The International Covenant on Civil and Political Rights, New York 19/12/1966, e.i.f. 23/03/1976.
[2] Ibid. Article 17.
[3] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg 28/1/1981, e.i.f. 1/10/1985.
[4] Charter of Fundamental Rights of the European Union, Nice 7/12/2000, e.i.f. 1/12/2012.
[5] General Data Protection Regulation (EU) 2016/679, 24/04/2016, e.i.f. 25/05/2018.

applicable in May 2018 was adopted. This led to the repeal of the Data Protection Directive (the Directive)[6] which came into force in 1995 and regulated the processing of personal data in the EU. The purpose of the GDPR was to improve the EU's data protection laws, enabling the protection of the right to privacy with focus on the digital challenges of the present. The preservation and development of the core principals and rights of data subjects and the obligations of the government make the GDPR a more comprehensive regulation on data protection than the Directive. Countries outside the EU recognising the legal and safety issues arising from the collection and processing of personal data have put in place or are in the process of initiating legislation and mechanisms for enforcement to guide the collection, processing and use of personal data. African countries like South Africa[7] and Ghana[8] have enacted personal data protection legislation while countries such as Nigeria have issued binding regulations pending the enactment of a principal legislation.[9]

Being the most populous black nation in the world and Africa's largest economy, an effective data protection regime is pivotal to the safety of the Nigerian society against breaches resulting from the lack of protection of personal data. Notwithstanding the lack of a principal and comprehensive data protection legislation, Nigeria has through provisions in various general and sector specific legislation regulated certain aspects of data protection. The provisions in some of these legislations include section 37 of the Constitution of the Federal Republic of Nigeria 1999 (the 'Constitution') which guarantees the right to privacy,[10] section 14 of the Freedom of Information (FOI) Act 2011 which obligates a public institution to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where the information is publicly available,[11] section 9 of the Credit Reporting Act 2017 which guarantees the rights of data subjects (persons whose credit data are held by a credit bureau) to privacy, confidentiality and protection of their credit information and also prescribes conditions for the disclosure of a data subject's credit information[12] and section 26 of the National Health Act 2014[13] which provides for the confidentiality of patient information. Regulations and guidelines issued by regulatory bodies such as the Nigerian Communications Commission (NCC) have also impacted data

[6] Data Protection Directive 95/46/EC, 24/10/ 1995, e.i.f. 13/12/1995.
[7] South Africa enacted the Protection of Personal Information Act on 19/11/2013although the substantive provisions are yet to take effect.
[8] Data Protection Act of Ghana, e.i.f. 10/05/2012.
[9] The Nigeria Data Protection Regulation, 2019.
[10] Constitution of the Federal Republic of Nigeria, e.i.f. 29/05/1999.
[11] Freedom of Information Act, e.i.f. 28/05/2011.
[12] Credit Reporting Act, e.i.f. 30/05/2017.
[13] National Health Act, e.i.f. 31/10/2014.

protection. For instance, the Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission (NCC) requires all telecommunications licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and to ensure that such information is securely stored and not kept longer than necessary.[14] They however apply only in relation to certain aspects of privacy and to certain sectors such as the non-disclosure of patients' health records as provided in the National Health Act. These legislations have proven to be ineffective in the protection of personal data especially due to advancements in technology and the digitisation of personal information and this is as a result of their lack of provisions relating to the general principles for the collection, processing and storage of personal data. For instance, a research by the World Wide Web Foundation observed that Nigerians are denied access to their personal data which has been stored manually as hospitals oftentimes deny patients access to their health records[15] which violates the principles of processing personal data.

In a bid to regulate and safeguard the collection and processing of personal data in Nigeria, the National Information Technology Development Agency (NITDA) in January 2019 pursuant to its powers under Section 6 (a) and (c) of the NITDA Act 2007 issued the Nigeria Data Protection Regulation 2019 (the 'Regulation')[16] which several writers believe is modelled after the GDPR.[17] It is important to state that regulations are used in Nigeria to address loopholes which were unforeseen by legislation or which arise before the enactment of a legislation. In the latter case, the regulation would cease to apply upon the enactment of legislation. While many writers have lauded the effort of the NITDA in issuing the Regulation, concerns have been raised as to the validity of the Regulation and the power of the NITDA to issue it.[18]

The Regulation has provided a framework for the protection, collection and processing of personal data with remedies for breach of the provisions of the Regulation. The application of the Regulation is still minimal as the situation which largely existed before the issuance of same regarding the collection and processing of personal data, which includes the misuse of

[14] Section 36 of the Consumer Code, e.i.f. 01/08/2007.
[15] C.E. Izuogu, Personal Data Protection in Nigeria, Report of World Wide Web Foundation, March 2018, p 23.
[16] Nigerian Data Protection Regulation 2019.
[17] A.K. Hunton, Nigeria Issues New Data Protection Regulation, Privacy and Information Security Blog, 05/04/2019 available at https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/ accessed on 20/04/2020.
[18] G. Greenleaf, Nigeria Regulates Data Privacy: African and Global Significance, 158 Privacy Laws & Business International Report 23, (2019) University of New South Wales Law Research Series 66.

personal data, still exists. It is however hoped that in the course of time, and the enactment of a principal legislation on data protection, more people will become aware of data protection and will seek redress, using remedies provided in the Regulation and future legislation, against breaches which is widespread in Nigeria.[19] Based on the foregoing, there is not only a need to enact a principal legislation for the protection of personal data but also to raise awareness as to the importance of the protection of personal data in Nigeria. Also, there is presently a Data Protection Bill, 2015 (the 'DPB') which was passed by the National Assembly in Nigeria on the 9th of May, 2019 which is awaiting presidential assent. The DPB seeks to regulate the processing of information in relation to individuals and an examination of the principles reveal that it is roughly based on the fair information practice principles. It should be noted that several efforts have been made in Nigeria to enact a primary data protection legislation which have failed[20] but it is hoped that the DPB will be successful.

The accomplishments of the EU in the application and implementation of its personal data protection laws as seen in practice and in the case law of the Court of Justice of the European Union (CJEU) as well as the use of the GDPR as a template for the Regulation is the basis for comparison of the EU with the Nigerian personal data protection legal system. Hence, certain aspects of the Nigerian personal data protection legal system will be examined in this research thesis and compared with corresponding aspects of the EU personal data protection legal system because the EU has an established tradition of regulating how personal data is handled which has been developed through years of wilful practice. This comparison will be beneficial for the Nigerian data protection legal system which is still developing with the consequential effect of aiding law reforms and policy development for effective personal data protection in Nigeria.

The research problem is an evaluation of the notion of the right to the data protection in Nigeria in order to determine if there is a pre-existing right to personal data protection, how it is interpreted and what it encompasses using the EU as a yardstick because of its jurisprudential progression in the field of personal data protection which were a consequence of the loopholes that emanated from technological advancements. Furthermore, the author will examine the principles governing the processing of personal data through a comparison

[19] Punch Nigeria, Cyberattacks, Data Breaches top concerns of IT Experts published April 22, 2019, assessed at https://punchng.com/cyberattacks-data-breaches-top-concerns-of-it-experts/ on 15/12/2019.
[20] R. Akindele, Data Protection in Nigeria: Addressing the multifarious challenges of a deficient legal system- 26 Journal of International Technology and Information Management 2017(4), p 112.

of Article 5 of the GDPR and Section 2 of the Regulation in order to determine the challenges to effective data protection through the differences or similarities identified.

This research paper will serve as a guide in the determination of the concept of personal data in Nigeria, the existence of a right to data protection in Nigeria and the extent to which it is guaranteed if it does exist, and the steps which are necessary to ensure that personal data is effectively protected. The author's research could/can be useful to the Government of Nigeria which is still grappling with understanding the usefulness of efficient and effective data protection laws, and it could also serve as an informative tool on data protection for private individuals and entities in Nigeria.

The aim of this research paper is to compare the present data protection regulation in Nigeria with that of the EU in order to assess whether the respective legal frameworks provide adequate and effective data protection in relation to the processing of personal data. This will be achieved through the determination of the following research questions: (a) the meaning of personal data in Nigeria and the EU (b) the notion and scope of the right to data protection under the subsisting laws and regulations in Nigeria and the EU (c) the capacity of Nigeria's Data Protection Regulation, 2019 to effectively guarantee data protection through an examination and comparison of the principles of processing personal data contained in the Regulation of Nigeria and the GDPR of the EU (d) the lessons that could be deduced from the comparison of the Nigerian and EU data protection legal systems (e) the challenges which may serve as a hindrance to effective data protection in Nigeria.

The author will apply comparative and analytical methods in the course of this research. The principal focus of the author will be on data protection provisions and legislation in Nigeria and the EU. A comparative approach is taken by the author in order to better assess the right to data protection in Nigeria using the EU as a reflective tool from which lessons on the enactment and application of data protection legislation could be drawn. These will be analysed in conjunction with relevant primary sources such as the General Data Protection Regulation, the Nigerian Constitution, the Charter of Fundamental Rights of the European Union and the Nigeria Data Protection Regulation amongst others. Secondary sources which include books such as EU Data Protection Law written by Denis Kelleher and Karen Murray, Data Protection; A Practical Guide to UK written by Peter Carey, African Data Privacy Laws edited by A.B. Makulilo will be utilised in this research paper. Articles written by authors such as C.E. Izuogu, G. Greenleaf and I.A. Nwankwo on data protection will also be used in

the writing of this paper. Additionally, some decisions of the Court of Justice of the European Union and the superior courts of Nigeria which are relevant to the research paper will be touched upon.

The thesis consists of three chapters with the first chapter delving into the meaning of personal data in Nigeria and the EU. The notion and the scope of the right to data protection in both Nigeria and the EU will be analysed. The fundamental rights to which the right to data protection has been linked and the court practices that have impacted personal data protection in Nigeria and the EU will be examined.

The second chapter will analyse the principles for processing of personal data as enumerated in section 2 of the Nigeria Data Protection Regulation, 2019 vis-à-vis article 5 of the GDPR. The application of article 5 by the CJEU will also be considered to provide a better understanding of the principles of processing personal data and its application in daily life.

The third chapter will analyse the lessons from the comparison of the Nigerian and EU data protection regimes in order to determine the challenges which could arise from the difference or similarities in the Nigerian personal data protection practice in the future. Furthermore, the challenges that could serve as a hindrance to an effective data protection regime in Nigeria will be examined with a view to proffering solutions to tackle same.

Keywords: Data Protection, Nigeria, European Union, Nigeria Data Protection Regulation, General Data Protection Regulation.

1. EVALUATION OF THE DEFINITION AND SCOPE OF THE RIGHT TO DATA PROTECTION IN NIGERIA AND THE EU

Data protection refers to personal data and the rules which apply to the processing of these data. Data protection and effective data protection laws are important as a result of the constant technological advancements in software and hardware as well as the need to safeguard personal information stored on computers to prevent their abuse and misuse. It is a necessary component of a society's legal and political values.[21]

In the EU, the right to data protection is considered to be of utmost importance and this is inferred from legal instruments which include treaties and regulations that guarantee this right. These legal instruments provide the basis for the protection of personal data of EU nationals and the processing and transfer of same. It is pertinent to state that before the adoption of the Charter of Fundamental Rights of the European Union (the 'Charter')[22] and the General Data Protection Regulation ('GDPR')[23] by the European Union Parliament in 2016, the Data Protection Directive (the 'Directive')[24] which became legally binding in December 1995, was the first significant instrument to affect privacy and data protection with its purpose being to facilitate the movement of personal data around the EU. The Directive was repealed and replaced, with effect from 25 May 2018, by the GDPR[25] but the substance of both instruments is similar. Additionally, the Court of Justice of the European Union ("CJEU") has through its case laws, significantly contributed to the development of the right to the protection of personal data.

Although there is no fundamental right to data protection in Nigeria, data protection is a budding area of law which is currently encompassed under the right to privacy as provided in the Nigerian Constitution and some sector specific legislations and regulations. There is however a Data Protection Bill pending presidential assent and a Data Protection Regulation issued in 2019 by the National Information Development Technology Agency ('NITDA') which aims to regulate processing of personal data in Nigeria. It has been posited by several

[21] P. Blume, et al, Nordic Data Protection Law, DJOF Publishing Copenhagen, 2001, p. 1.
[22] Ibid. footnote 4.
[23] Ibid. footnote 5.
[24] Ibid. footnote 6.
[25] The GDPR replaced the European Union's 1995 Data Protection Directive (1995 Directive), 1995 O.J. (L281) 31, which has provisions similar to those in the GDPR.

writers[26] that though there is no express right to data protection under Nigerian laws, the right can be inferred from extant laws and regulations.

1.1 Meaning of Personal Data in the European Union

Although the right to the protection of personal data is guaranteed by the Charter, there is no stated definition of personal data therein. The definition of personal data in the EU is as contained in Article 4(1) of the GDPR which provides that "any information relating to an identified or identifiable natural person; 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."[27]

Personal data in the EU simply means any information that easily distinguishes a person from others. These include the name of a person, whether it is the given name or the name by which they can be identified such as a nickname, the national identification number or even that contained on the driver's licence of a person, the online identifier of a person which may be an IP address, an email address or social media username.[28] The definition further extends to specific components of a person such as the physical and physiological features in a photograph, drawing or a disability; the genetic composition like the DNA, blood type or blood group; the mental component as contained in a mental health record; the economic component like the assets and liabilities of a person; the cultural components like the origin; the social identity such as the political or religious beliefs.[29] It is on the basis of this definition that the CJEU held that the recorded image of persons is personal data within the meaning in Article 2(a) of Directive 95/46.[30] This is based on the specific component which is the physical component.

In the determination of whether or not some information is personal data, the test used is if the information can be used to identify a person as such, information that cannot be linked to

[26] E. Salami, The Nigerian Data Protection Regulation 2019: Overview, Effects And Limits, datenschutz-notizen published on 2/04/2019, available at https://www.datenschutz-notizen.de/the-nigerian-data-protection-regulation-2019-overview-effects-and-limits-3522349/ assessed on 15/04/2020.
[27] Art. 4(1) of the GDPR.
[28] P. Carey, Data Protection; A Practical Guide to UK and EU Law, 5th Ed., United States of America, Oxford University Press, 2018, p 9.
[29] Ibid. p 10.
[30] C–345/17- Buivids case, para 32.

a natural person is not considered to be personal data.[31] For instance, the publication in the national dailies in Estonia of the nationality of the first person who tested positive for COVID-19 would not be held to be personal data because there are other persons of that nationality in Estonia. The case would however be different if the person could be easily identified, such as if he was the only person of that nationality in Estonia.

However, situations have arisen where documents which contain the personal information of a natural person was held not amount to personal data. For instance, in YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,[32] the CJEU was asked to determine whether the legal analysis in the minutes of a person who applied for residence permit constituted personal data. It held that although the data, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, which relate to the applicant and contained in the minute, are information relating to an identified natural person and is thus personal data, the legal analysis in a minute which may contain personal data, does not in itself constitute personal data as defined in Article 2(a) of Directive 95/46.[33]

Notwithstanding the definition of personal data provided by the GDPR, the CJEU has by its jurisprudence, expanded the scope of personal data to include the written answers provided by a candidate in an exam and any comments made upon the answers by the examiner.[34] The Court stated that to rule otherwise would have the effect of entirely excluding that information from the obligation to comply with the data protection principles and safeguards, and the rights of access, rectification and object of the data subject which led the Court to conclude that the use of 'any information' in the definition of personal data, in Article 2(a) of Directive 95/46 (now Article 4(1) of the GDPR), indicates the intent of the EU legislature to widen the scope of personal data to include both objective and subjective information which involve the data subject.[35] The CJEU has held that the following constitute personal data: the name of a person which includes his phone coordinates or information about his working conditions or hobbies,[36] data found, indexed and stored by search engines,[37] the name(s) of

[31] IT Governance Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, 2nd Ed. United Kingdom, IT Governance Publishing, 2017, p 20.
[32] Joined cases, C-141/12 and C-372/12.
[33] Ibid. para 38 and 39.
[34] C-434/16, Peter Nowak v Data Protection Commissioner.
[35] Ibid. para 34
[36] Case C-101/01, Lindqvist v Sweden, para 23.

the air passenger(s), information necessary to the reservation, such as the dates of the intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passenger.[38] The expansion of the meaning of personal data by the CJEU is not limited to the above decisions.

Furthermore in Breyer v. Bundesrepublik Deutschland,[39] the CJEU stated that in order for information to constitute personal data, it is not required that all the information which can be used to identify a person, must be in the hands of one person.[40] Kelleher and Murray note that in determining what constitutes personal data, an objective test should be applied and the manner of processing personal data should be disregarded.[41] From the foregoing, it is observed that the definition of personal data in the EU is not limited to the identifiers stated in the GDPR but expandable as is seen from the decisions of the CJEU on information which constitute personal data and this is achieved through defining personal data based on the circumstances of the case.

1.2 Meaning of Personal Data in Nigeria

The applicable definition of personal data in Nigeria is that provided in the Data Protection Regulation (the 'Regulation') issued by the National Information Technology Development Agency ('NITDA') in 2019. It defines personal data as '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.' From the definition, personal data in Nigeria is any information or attribute that makes the identification of a person unmistakeable. This means that personal data in Nigeria will include an individual's name, address, photograph, email address, bank

[37] C-131/12, Costeja Gonzalez v Google Spain and Google, para 27.
[38] Opinion 1/15, The European Court of Justice on the EU-Canada Passenger Name Record Agreement of 26 July 2017, para 1.
[39] C-582/14, Breyer v Bundesrepublik Deutschland.
[40] Ibid. para 43.
[41] D. Kelleher and K. Murray, EU Data Protection Law, United Kingdom, Bloomsbury Publishing Plc. 2018, p 81.

details, social media username and posts, medical information, IP address, IMEI number, telephone number and any other information which can be linked to a living person.

The provision of identifiers by the Regulation helps to clarify what information constitutes personal data in relation to a natural person but it is believed that reliance on the specific identifiers provided by the Regulation for the definition of personal data could lead to unfairness. This is likely where the information claimed as personal data by an individual cannot be classified under any of the identifiers in the Regulation coupled with the lack of judicial jurisprudence in that particular field of law. It is thus posited by the author that the test to be used for determining what information constitutes personal data is an objective one based on the facts of a case. This definition has however not been tested in the Nigerian Courts but it is believed that in the determination of what constitutes personal data, it will be sufficient.

1.3 The notion and scope of the right to data protection in the EU

An integral part of this research paper is the notion of the right to data protection in the EU. Recital 1[42] to the GDPR reiterates that the protection which accrues to natural persons in relation to the processing of their data is a fundamental right as provided in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).[43]

Before the Charter became legally binding in 2009, the right to data protection was oftentimes linked to the right to respect for private and family life.[44] This is mainly because they both protect the personal space and confidentiality of individuals which consequently led to the right to data protection being oftentimes treated as a component of the right to privacy. This is deduced from the decision of the CJEU in Promusicae v Telefonica de Espana[45] when it stated that the case included the right that protects the protection of personal data and

[42] Recitals provide additional information to the Articles of the GDPR which aid the understanding of the GDPR by the general public. They provide valuable supplementary information. They are not legally binding and cannot be relied upon as a ground for derogating from the actual provisions of the act in question. See Nilsson Case C-162/97, Nilsson and Others, para 54.
[43] European Union Agency for Fundamental Rights, Handbook on European data protection law, 2018 ed., Luxembourg: Publications Office of the European Union, 2018, 17
[44] Article 7 of the Charter
[45] Case C-275/06, Promusicae v Telefonica de Espana; See also Case C-92/09, Volker und Markus Schecke, para 47.

consequently, private life.[46] The CJEU continually linked the right to data protection and the right to respect for private and family life together even after the Charter became binding. This was stated to be as a result of the CJEU's literal interpretation of the words, 'there is a particular protection of the fundamental right to privacy with respect to the processing of personal data',[47] as found in the Directive/95/46/EC in the adjudication of cases.[48]

The European Union Agency for Fundamental Rights believes that the right to personal data protection is wider in scope than the right to private and family life because the right to data protection involves any processing of all kinds of personal data notwithstanding the relationship and consequence on privacy and as a result they cannot be used interchangeably.[49] It also posits that the right to private and family life and data protection in the EU are different in both expression and scope as while the right to private and family life generally prohibits interference, except in cases of justifiable public interest, the right to data protection provides a mechanism of safeguards to protect the processing of personal data of individuals which is no longer private.[50] It has also been opined by various authors that the disagreement in the concept of privacy which has been interpreted to mean a right to be let alone, limited access to self, discretion, management of one's personal information and freedom to make decisions without unwarranted meddling[51] is detrimental to the right to data protection because irrespective of the concept of privacy, it cannot provide a comprehensive description of the individual's rights and organisation's obligations under data protection laws.[52]

Upon entry into force of the Charter in 2009, the right to data protection which had previously been incorporated under the right to private and family life became a clearly distinct right in the EU and it is thus undeniable that the right to data protection exists in the EU. The Charter recognises an individual's right to have their personal information protected and used, with their consent, in a reasonable and legal way.[53] Furthermore, the CJEU in the Schrems case[54] upheld the prominence of the right to data protection distinct from the right to

[46] Ibid. para 63.
[47] Article 1(1) of Directive 95/46/EC.
[48] M. Brkan and E. Psychogiopoulou, Courts, Privacy and Data Protection, Edward Elgar Publishing 2017, p 13.
[49] Ibid. footnote 43, p 20.
[50] Ibid. footnote 43, p 19.
[51] D. Solove, Conceptualising Privacy- 90 California Law Review 2002, p 1087-1155.
[52] B.V. Alsenoy, Data Protection Law in the EU: Roles, Responsibilities and Liability, United Kingdom: Intersentia Ltd 2019, p 159.
[53] Article 8 of the Charter.
[54] C-362/14, Schrems case.

respect for private life.[55] The case law of the CJEU on the right to data protection is continuously growing with decisions ranging from issues relating to the definition and processing of personal data to the rights of individuals and obligations of organisations.

The right to data protection in the EU is complemented with the GDPR which was adopted in 2016 and became legally binding on the member states of the EU in 2018. The aim of the GDPR is to provide a comprehensive and uniform regulatory framework for data protection in the EU[56] and it applies to the partial or full processing of personal data through automatic and manual means.[57] The activities of the controllers[58] and processors[59] in respect of the personal data of EU citizens, residents such as students from other countries and even tourists irrespective of whether or not the data is processed in the EU is what the GDPR seeks to regulate.[60]

The GDPR places great responsibility on the processors and it does not matter whether they are established in the EU as long as the personal data being processed is that of EU data subjects and the processing relates to the offer of goods and services, irrespective of whether a payment is required.[61] Thus the GDPR would be applicable to an American cloud-based services provider that has no establishment in the EU but offers its products to individuals in the EU, regardless of whether a payment is required or not, as long as the offer involves the processing of the data of the individuals.[62]

The right to data protection under EU law relates only to living persons but it allows member states to provide rules for the processing of the personal data of deceased persons. The right is however not absolute and can be limited by EU law or national law which must be proportional, justifiable and necessary to protect the rights of others.[63] The CJEU in Schecke

[55] Ibid. para 54.
[56] European Commission, Safeguarding Privacy in a Connected World- A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, COM (2012) 9 final, 25/01/2012, p 7.
[57] Article 2(1) GDPR.
[58] Article 4(7) GDPR defines a controller of personal data as whoever determines the means and purposes of processing individuals' personal data such as a company or a government institution.
[59] Article 4(8) defines a processor as a natural or legal person who processes personal data on a controller's behalf.
[60] Article 3(1) GDPR.
[61] Article 3 (2) GDPR.
[62] W. Gregory Voss, European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting- 72The Business Lawyer, Winter 2016–2017, p 223.
[63] Article 52 (1) of Charter.

and Harmut cases[64] upheld this position when it stated that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.

The CJEU has in multiple cases recognised the need to strike a balance between conflicting rights such as the right to freedom of expression and the right to data protection. This is as seen in the case of Lindqvist v Sweden,[65] in which the applicant was prosecuted by the respondent for breaching its data protection law by publishing personal information of some of her colleagues in the parish on her internet site.[66] The CJEU was asked to determine whether the provisions of Directive 95/46 bring about a restriction which conflicts with the general principles of freedom of expression of the applicant. It was held that the applicant's freedom of expression has to be fairly balanced against the protection of the private life of individuals. Likewise, in the case of Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,[67] the CJEU was asked to decide the justifiable balance between the freedom of expression and data protection in case of journalistic activity under Article 9 of the Directive 95/46 which gave member states the power to make necessary exemptions or derogations in respect of processing of personal data for journalistic, artistic or literary purposes in order to strike a balance between the right to privacy and the freedom of expression. The Court held that in order to achieve a balance between the right to privacy and the freedom of expression, the derogations and limitations permitted by Article 9 under the Directive must apply only "insofar as strictly necessary. The Court further stated that the exemptions provided in Article 9, apply to both media organisations and all persons engaged in journalism[68] irrespective of the means of transmission of personal data and whether or not the publication is undertaken for profit-making purposes since profit-making may be necessary for professional journalistic activity.[69] The Court concluded that processing activities should be considered as being 'solely for journalistic purposes' within Article 9 of the Directive 'if the sole object of those activities is the disclosure to the public of information, opinions or ideas'.[70]

[64] Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen, para 48.
[65] Case C-101/01, Lindqvist v Sweden.
[66] Ibid. para 2.
[67] Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy.
[68] Ibid para 58.
[69] Ibid. para 60.
[70] Ibid. para 62.

1.4 The notion and scope of the right to data protection in Nigeria

The above stated definition of personal data in the Nigerian legal system can lead one to believe that there is a fundamental right to data protection in Nigeria but this is erroneous because there is no provision for such in any law in Nigeria. This lack of an express provision for protection of personal data could mean that the concept is non-existent in Nigerian jurisprudence. In a country with a population of about 204 million people,[71] data is valuable and Piero Scaruffi recognised this by stating that data is becoming more valuable than oil, because unlike oil which does not generate more oil, data generates more data which ultimately leads to more revenue.[72] The field of data protection in Nigeria is growing at snail's pace but slow growth is definitely better than no growth. Notwithstanding this slow growth, processing of personal data by both state and private organisations is done in large numbers daily. For instance, the banks collect and process personal data to open bank accounts for individuals, the telecommunications companies collect and process personal data to register the SIM cards of individuals while the government, both at federal and state level, collect and process individual data for the issuance of driver's licences, international passports, voter's card and other documentation without due security measures taken.[73] This makes it easy for personal data to fall into the wrong hands or be abused. Although there is no stated right to data protection in Nigeria, there have been legal commentaries which opine that the right to data protection can be inferred from the right to privacy[74] and other national legislations and regionals conventions.[75]

1.3.1 Regional Conventions

Nigeria is a member of regional organisations such as the African Union (AU) and the Economic Community of West African States (ECOWAS) which have both adopted data protection instruments that can only be implemented in Nigeria when it has been enacted into

[71] Worldometer, Nigeria Population (Live) available at https://www.worldometers.info/world-population/nigeria-population/ assessed on 28/01/2020

[72] P. Scaruffi, Big Data: History, Trends and Future, published in 2016 available at http://www.scaruffi.com/singular/bigdata.html accessed on 28/02/2020.

[73] Paradigm Initiative and Privacy International, The Right to Privacy in the Federal Republic of Nigeria: Stakeholder Report, Universal Periodic Review, 31st Session- Nigeria, March 2018, p. 8-11.

[74] R. Clark, Introduction to Dataveillance and Information Privacy, Definition of Terms, available at www.rogerclarke.com/DV/Intro.html, accessed on 28/02/2020.

[75] Y. Okojie, Information is the New Oil in Nigeria, SPA Ajibade & Co, Privacy and Data Protection, published 20/07/2017, p 2.

law by the National Assembly.[76] For instance, the Supplementary Act on Personal Data Protection (the 'Supplementary Act')[77] of ECOWAS which was adopted in 2010 is a regional convention from which the right to data protection in Nigeria may be inferred. It was adopted to provide uniform data protection laws for West Africa and consequently enable the free movement of personal data within West Africa. The Supplementary Act further required all member states to enact legislations which would regulate the collecting and processing of personal data. The Supplementary Act is comprehensive and would have provided for effective protection of personal data in Nigeria but so far, it has had no influence on data protection in Nigeria because it has not been ratified by the National Assembly as required by section 12 of the Constitution.[78] It should be noted that even though the Supplementary Act is an integral part of the ECOWAS Revised Treaty which requires member states to fulfil the obligations thereunder, or be sanctioned for failure to do so,[79] most ECOWAS member states have failed to implement it in contravention of Article 5 of the ECOWAS Revised Treaty which provides that member states shall take all necessary measures to ensure the ratification and dissemination of legal texts that are needed to implement the Treaty.[80] However no sanctions have so far been imposed on any of the erring states, including Nigeria due to the lack of political will on the part of the member states of ECOWAS.

Another regional convention from which the right to data protection in Nigeria could be inferred is the African Union Convention on Cyber Security and Personal Data Protection (Convention)[81] which was adopted in 2014. The objective of the Convention is to provide the necessary rules for the establishment of a credible digital environment, to address the vacuum in the regulation and legal recognition of electronic communications and electronic signature and the lack of specific legal rules for the protection of consumers, intellectual property rights, personal data and information systems and privacy online.[82] The Convention further emphasises the need for member states to establish legal and institutional frameworks for data protection and cyber security. However, like the Supplementary Act, Nigeria has failed

[76] Section 12(1) of the Constitution.
[77] Supplementary Act A/SA.1/01/10.
[78] I.S. Nwankwo, African Data Privacy Laws, Law, Governance and Technology Series 33, A.B. Makulilo (ed.), Switzerland: Springer International Publishing AG 2016, p 71.
[79] Article 77 of the ECOWAS Revised Treaty, Cotonou 24.07.1993.
[80] Ibid. Article 5.
[81] African Union Convention on Cyber Security and Personal Data Protection, adopted on 27/06/2014 in Malabo, Equatorial Guinea.
[82] Ibid. Preamble.

to ratify the Convention[83] and as a result, it has not entered into force and is thus inapplicable.[84]

1.3.2 National Legislations

Irrespective of Nigeria's failure to ratify the regional conventions, the right to data protection is also inferred from various national legislations and some of the data protection provisions in these legislations are as discussed hereinafter. The right to data protection in Nigeria has been linked by different authors[85] to the right to privacy as contained in Section 37 of the Constitution. It provides that citizens, their homes, correspondence, telephone conversations and telegraphic communications are guaranteed privacy.[86] The application of the right to privacy as presently guaranteed to data protection issues will be challenging because of the more intrusive and invasive nature of modern technology which require processing of personal data sometimes by organisations not in the same geographical location as the individual whose data is being processed. Additionally privacy which has no widely accepted definition is not only a broad concept but it is also one of the least litigated and researched rights in Nigeria[87] and this could lead to difficulties in its application to data protection especially since there are no supplementary materials to serve as a guide for the courts. The right to privacy as provided by the Constitution is applicable only to citizens of Nigeria either through birth, registration or naturalisation[88] as a result foreign residents in Nigeria are not protected thereunder.

Furthermore, the permitted derogations from the right to privacy, in the author's opinion, would possibly render its application to data protection ineffective as section 45 of the Constitution provides that the right to privacy is limited by 'any law that is reasonably

---

[83] African Union, List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf accessed on 27/02/2020

[84] Ibid. footnote 76.

[85] See C.E. Izuogu, Data Protection and other Implications in the ongoing Sim Card Registration Process, published on 2nd May, 2010, available at https://ssrn.com/abstract=l597665 accessed on 27/02/2020; F. Ololuo, Data Privacy and Protection under the Nigerian Law published on l9/02/2020, available at https://www.mondaq.com/Nigeria/Privacy/895320/Data-Privacy-And-Protection-Under-The-Nigerian-Law#_ftn1 accessed on 27/02/2020.

[86] Ibid. footnote l0.

[87] A.O. Salau, Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission: Regulation without Predictability, 7th International Conference on Information Law and Ethics, 22nd-23rd February, 2016 available at http://icil.gr/download.php?fen=years/2016/downloads/documents/icil_2016_proceedings_book.pdf accessed on 20/04/2020.

[88] Section 25-27 of the Constitution.

justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedom of other persons.'[89] These derogations have however not been developed in Nigerian legal system as the courts oftentimes resolve cases of human rights violations resulting from derogations without recourse to finding the balance between the rights and derogations. For instance in Chukwuma & Others v. Commissioner of Police,[90] The police entered a private hotel and dispersed a meeting holding therein because the conveners had failed to obtain a police permit in order to assemble. The Court of Appeal upheld the action of the police on the ground that the organizers should have obtained the permit as required by the Public Order Act. The Court failed to balance the constitutional right to assemble with the maintenance of public order especially since the meeting was held in a private place. The lack of structure and prescribed standard for balancing of rights against lawful derogations has led to the misuse of these derogations to abuse human rights by Nigeria's security agencies with little recourse to the courts for remedy. For instance, the Nigerian Police Force has normalised the conducting of searches without the necessary warrants or reasonable suspicion as provided in section 29 of the Police Act.[91]

Additionally, the right to data protection can be inferred from the Consumer Code of Practice Regulations, 2007 (the 'Consumer Code') issued by the Nigerian Communications Commission (NCC) pursuant to its powers under Section 106 of the Nigerian Communications Act 2003 (NCA).[92] The Consumer Code is legally binding on licensed telecommunications operators (licensees) in Nigeria to regulate their services and related consumer practices. Section 4(2) of the Consumer Code provides for the Schedule to the Consumer Code which is a General Consumer Code of Practice (the 'General Code') contains provisions, in Parts VI and VII, which relate to data protection and the procedure for complaints in the event of failure to adhere to part VI of the General Code.[93] Section 35 of the General Code provides the general principles for the processing of information of individual consumers and its provisions are that consumer information must be fairly and lawfully collected and processed, the information must be relevant, processed in accordance

[89] Section 45 (1) of the Constitution.
[90] (2005) 8 NWLR (Pt 927) 278.
[91] Nigeria 2019 Human Rights Report, Country Reports on Human Rights Practices for 2019: United States Department of State, Bureau of Democracy, Human Rights and Labour, p 16.
[92] Consumer Code of Practice Regulations, 2007, S. I. 32 of 2007, e,i.f. 01/08/2007.
[93] Schedule to the Consumer Code of Practice Regulations, 2007, General Code of Practice, Part VI and VII.

with the consumer's other rights amongst other principles.[94] It further provides for the transfer of consumer information, subject to any terms and conditions consented to by the consumer, as approved by the NCC, or as permitted or required by other applicable laws or regulations.[95]

The General Code mandates licensees to meet generally accepted fair information principles which include the notification of individual consumers about the information they collect, its use and disclosure, the choices of consumers in relation to the collection, use and disclosure of the information; the accessibility by consumers to the information and their right to ensure its accuracy; the security measures which have been taken to ensure the protection of the information including the enforcement and redress mechanisms in the case of failure to observe these measures.[96] The General Code also mandates the licensees who collect information to adopt and implement a policy on the proper collection, use and protection of consumer information.[97] The provisions of the General Code are comprehensive in the protection of personal data of individuals however, the General Code being a sector specific code only applies to licensees in all telecommunications services offered to the public.[98] As a result, though effective in the telecommunications sector, it would be ineffective in other private sectors such as the financial sector and the public sectors where personal information is collected and processed daily.

In 2019, the National Information Technology Development Agency (NITDA) issued the Nigeria Data Protection Regulation pursuant to its powers under the NITDA Act[99] hence it is not an act of the legislature. The objectives of the Regulation include safeguarding the rights of living persons to data privacy, ensuring transactions involving the exchange of personal data are conducted safely and prevention of exploitation of personal data.[100] The Regulation applies to 'all transactions intended for the processing of personal data and to actual processing of personal data notwithstanding the means by which the data processing is being conducted or intended to be conducted and in respect of natural persons in Nigeria; to natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent'.[101]

[94] Ibid. Section 35 (1).
[95] Ibid. Section 35 (1)(h).
[96] Ibid. Section 35(2).
[97] Ibid. Section 36.
[98] Ibid. Section 3.
[99] Section 6(b and c) of the National Information Technology Development Agency Act, 2007.
[100] Section 1.0 of the Regulation.
[101] Section 1.2 (a) and (b) of the Regulation.

The Regulation mandates all public and private organizations that control data of natural persons in Nigeria to make their respective data protection policies available to the general public within three months after the date of issuance of the Regulation.[102] The Regulation is presently the most comprehensive data protection instrument in Nigeria but its application has raised several issues such as the powers of the NITDA to issue a regulation of general application on data protection in Nigeria which said power is reserved to the National Assembly.[103] Some commentators have also argued that the Regulation is in conflict with other sector specific regulations such as the Directive issued by the NCC which instructed telecommunications companies to monitor calls and other communication services passing through their networks in a bid to curb insecurity.[104] The application of the Regulation, just like the Constitution, is also limited to personal data of natural persons who are Nigerians or of Nigerian descent hence it is inapplicable to foreigners resident in Nigeria.[105]

The right to data protection can also be deduced from the Freedom of Information (FOI) Act, 2011. Section 14(1) of the FOI Act provides that a public institution has an obligation to deny an application for information that contains personal information such as (a) files and personal information maintained with respect to clients, patients, residents, or other individuals receiving social, medical, educational, vocational, financial, supervisory or custodial care or services directly or indirectly from public institutions; (b) personal files and personal information maintained with respect to employees, appointees or elected officials of any public institution or applicants for such positions; (c) files and personal information maintained with respect to any applicant, registrant or licensee by any government or public institution cooperating with or engaged in professional or occupational registration, licensure or discipline; (d) information required of any tax payer in connection with assessment or collection of any tax unless disclosure is otherwise requested by the statute; and (e) information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agency on the commission of any crime unless the individual involved consents to the disclosure, or where such information is

[102] Section 3.1 of the Regulation
[103] A. Alao, A Review of Data Protection Bill 2019 HB02: Three Ways It Affects Nigerians, Legalnaija Blawg, published 10/06/2019, available at https://www.legalnaija.com/2019/06/a-review-of-data-protection-bill-2019.html accessed on 28/02/2020.
[104] O. Oduwole, New NCC Directive Will Push Telcos to Violate Nigeria Data Protection Regulation, Tekedia, published 18/10/2019, available at https://www.tekedia.com/new-ncc-directive-will-push-telcos-to-violate-nigeria-data-protection-regulation/ accessed on 28/02/2020
[105] Ibid. footnote 101.

publicly available.[106] It further defines personal information 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'.[107] The purpose of the FOI Act is to allow unrestricted access to public records and information whilst protecting personal data or information. However, the FOI Act is only applicable to public institutions and agencies in Nigeria[108] consequently, it is ineffective to regulate the processing of personal data by private organisations in Nigeria.

The courts in Nigeria have indirectly through reliance on the right to privacy inferred a right to data protection as was seen when the Federal High Court in Godfrey Eneye v. MTN Nigeria Communication Limited[109] held that the unlawful release of the plaintiff's telephone number to unknown third parties which resulted in unsolicited text messages was a violation of his constitutional right to privacy. The defendant argued that the plaintiff's mobile phone number was not private as it was available to his family, friends, associates and clients who could have disclosed the number to other persons. It was further argued by the defendant that a violation of privacy involves actions such as invasion of a home, spying on a person, eavesdropping on the conversations and access to private documents which do not apply in the following case. The FHC disagreed with this position and awarded damages in the sum of 5 million naira (about 12,000 euros) against the defendant for violation of the plaintiff's fundamental right to privacy. The defendant filed an appeal against the judgment of the trial court but the Court of Appeal dismissed the appeal and held that the countless text messages sent to the plaintiff without his consent at all times is a violation of his fundamental right to privacy of his telephone conversations, correspondence and his person and telephone line and telephone message inbox.[110] Also in Barrister Anene v. Airtel Nigeria Ltd,[111] the plaintiff sued the defendant alleging that countless unsolicited calls and text messages to his private mobile number by the defendant (service provider), and third parties it disclosed his telephone number to, breached his right to privacy. The Court granted his claim and awarded the sum of 5 million naira against the Defendant.

It is undeniable that these cases would have been appropriately and thoroughly resolved under data protection laws than the right to privacy as the courts would have simply

[106] Section 14(2) FOI Act.
[107] Section 31 FOI Act.
[108] Section 1(1) FOI Act.
[109] FHC/ABJ/CS/431/2012 (unreported case).
[110] CA/A/689/2013.
[111] FCT/HC/CV/545/2015 (unreported case).

examined the definition of personal data, the processing of same, the conditions for the lawful processing of personal data and the exemptions thereto in arriving at its decisions.[112] Despite the lack of a stated right to data protection, the subsisting laws in Nigeria have somehow filled the vacuum that has been left by the non-availability of a data protection legislation. There is however a lack of uniformity in the laws and the mechanism for remedying a breach are so muddy that writers such as Adeniyi have postulated that an individual whose right to data protection has been breached by any organisation may institute an action in the tort of negligence against such organisation if it can be established that there was a duty of care, which has been breached and as a result, the person has suffered some damage.[113] This is easily problematic as the onus of proving negligence is on the individual and it might be difficult for the individual to discharge the onus since he must show that a duty of care was owed to him by the organisation, which duty was breached and the breach has resulted in damage. Thus where the individual fails to prove one of the elements of negligence the case is bound to fail.

1.5 Comparison between the meaning of personal data and the notion and scope of the right to data protection under the subsisting laws in Nigeria and the EU

The meaning of personal data in the EU and Nigeria are similar as they both clearly relate to information about an identified or identifiable living person. There are clear identifiers of personal data provided in both definitions which include the name of an individual, an identification number, an IP address amongst other identifiers. The meaning of personal data in the EU is not restricted to the identifiers in the GDPR as it has been broadened through the decisions of the CJEU while the meaning of personal data in Nigeria is currently limited to that provided in the Regulation.

The right to data protection as provided in Article 8 of the Charter is a distinct fundamental right in the EU[114] and not just a tool for economic cooperation between the member states as was initially construed at the time of adoption of the Directive in 1995.[115] The right to data protection is supplemented by the GDPR which is a regulatory framework for the

[112] I. Nwankwo, Nigeria's Data Privacy First Responders, ICT and Law in Nigeria, 4/04/2018, available at https://iheanyisam.wordpress.com/2018/04/04/nigerias-data-privacy-first-responders/ assessed on 27/02/2020
[113]A.S. Adeniyi, The Need for a Data Protection Law in Nigeria, Communications and IT Law published 18/07/2012, available at https://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/ assessed on 27/02/2020.
[114] L.A. Bygrave, Data Privacy Law: An International Perspective, United Kingdom: Oxford University Press, 2014, p 59.
[115] Ibid. p 57.

harmonisation of data protection laws to observe and promote respect for data protection rules in the EU. Under Nigerian law, there is no fundamental right to data protection under chapter 4 of the Constitution which provides for the fundamental rights of Nigerians. Notwithstanding, the right is inferable from various national legislations and regulations which have helped in various albeit minimal ways to safeguard personal data.

The GDPR which is legally binding on the member states of the EU has general application in the EU in relation to the processing of personal data. This ensures that the standard of the right to data protection available irrespective of the geographical location in the EU is parallel. The multiplicity of data protection sections in Nigerian law leads to a disparity in the standard of protection under each legislation. Thus the standard of protection afforded an individual under the Consumer Code is distinct from that under the FOI Act. This is due to the fact that the Consumer Code and the FOI Act regulate and relate to different organisations, the telecommunications organisations and government organisations respectively, and they also have different supervisory bodies.

All EU nationals and foreign residents are guaranteed the right to data protection which is also extended to tourists within the EU. The right to data protection under Nigeria's subsisting laws is only available to Nigerians living in Nigeria and non-residents of Nigerian descent. This exempts foreign residents and tourists which is clearly detrimental as the little safeguards which could be gotten from the subsisting laws, is not available to foreigners thus making their personal data susceptible to manipulation and exploitation. The right to data protection in the EU and Nigeria is applicable to only living persons, hence a dead person's personal data is not protected under the subsisting laws but the EU allows for member states to make laws which will apply to the processing of personal data of dead people. There is no such provision in Nigeria.

The right to data protection is not absolute hence it can be limited by an EU law or national law. The law must be proportional, justifiable and necessary to protect the rights of others. This allows for the balancing of other rights against the right to data protection in order to determine which right should be given priority. The test used is an objective test and the facts and circumstances of the situation help to determine the balance which should be afforded each right. The right to privacy in Nigeria from which data protection has been inferred can also be limited by a reasonably justifiable law such as one to protect the public safety, health, morality or order or for the protection of the rights of other persons These derogations have

not been developed as in the EU legal system as cases in which rights have needed to be balanced against lawful derogations have been decided without any reference or attempts to balance conflicting rights.

The GDPR does not apply to certain situations, like processing of personal data for personal or household activities, processing by competent law enforcement agencies and processing for the purpose of safeguarding national security, whereas, the Nigerian instruments, for instance the Regulation does not provide any exemptions of its application to processing of personal data hence it could be argued that the provisions of the Regulation should be adhered to when parents take pictures of their children and post it on social media. This will be onerous.

Transfer of personal data to a foreign country from both Nigeria and the EU is permitted. Both legal systems require that before personal data can be transferred to a third country, such country must have adequate data protection laws for the protection of the rights of data subjects in relation to the processing of their personal data. Although what constitutes adequate data protection laws is not stated, data protection laws of a third country are considered adequate by the EU if its data protection laws, regulatory mechanisms and international obligations are parallel to that of the EU.[116] There is no stated criterion of how adequacy of data protection laws is measured under Nigerian law.

[116] Ibid. Kelleher and Murray, footnote 41, p 109.

2. PRINCIPLES OF PROCESSING PERSONAL DATA IN NIGERIA AND THE EU

The principles of processing personal data are the standards which must be adhered to by the data controller in the processing of personal data. These principles are considered the common denominator for the processing of personal data and they also serve as the yardstick to be followed by both the public and private organisations.[117] Processing includes but is not limited to actions such as collecting, deleting, altering and retrieving in relation to personal data. The principles regulate and ensure that personal data is collected, processed, transmitted and transferred lawfully without violating the right to data protection of the individual. The principles of processing personal data are interconnected and as a result, all the principles are to be complied with in the processing of personal data.[118]

2.1 Examination of Article 5 of the General Data Protection Regulation in the EU

Processing of personal data as defined by the GDPR refers to 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[119] These principles relate to the fundamental rules which must be adhered to in the processing of personal data in the EU.[120] Restrictions to the processing principles are permitted by EU law only when they correspond to rights and obligations that are provided in Articles l2 to 22 and the said restrictions must respect the essence of the fundamental rights and freedoms. Exemptions from and restrictions to the processing principles must be provided for by law, pursue a legitimate aim and be necessary and proportionate measures in a democratic society.

The seven principles are (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality;[121] and (g) accountability.[122] These principles will be distinctly examined below.

[117] Ibid. Bygrave, footnote l14, p l45.
[118]Ibid. Carey, footnote 28, p 32.
[119] Article 4(2) GDPR.
[120] Ibid. Kelleher and Murray, footnote 4l, p l37.
[121] Article 5(1) of the GDPR.
[122] Article 5(2) of the GDPR.

2.1.1 The Principle of Lawfulness, Fairness and Transparency

According to Carey, the first principle consists of three obligations which are to process personal data lawfully, to process such data fairly and to process personal data transparently.[123] Lawfulness requires that the procedure for data processing must be in compliance with the law and the conditions for lawful processing of data have been set forth in Article 6 of the GDPR, thus any processing that fails to meet the conditions set forth in Article 6 would be regarded as unlawful.[124] In order to process personal data lawfully, one of the six conditions as listed in Article 6 of the GDPR must apply.[125] The first condition is consent which must be given by the individual for the processing of his data.[126] Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[127] Consent must be explicit and unequivocal as a result, it cannot be presumed from silence. Consent must be obtained for each processing activity when the data is to be used for multiple purposes.[128] The condition of consent requires that data subjects are allowed to withdraw their consent without any consequences whenever they deem fit with the data controller informing them of their right to withdraw before consent is given.[129] The individual must be informed of the use for which his personal data is being processed and the identity of the data controller. Data controllers must possess lawful grounds for processing personal data, and not use it in ways that will have unwarranted negative effects on the individuals concerned. Consent must also not be obtained with duress as might be seen in an employee-employer relationship.

Processing of personal data will be lawful where it is necessary for the performance of a contract or before entering into a contract.[130] This condition relates to a contract to which the individual is a party and if the individual decides against executing the contract then personal data cannot be lawfully processed under this condition. Compliance with legal obligation[131] as a condition stipulates that processing of personal data is lawful if it is to carry out a task imposed by law thus the provision of the bank account details of an individual to the police

[123] Ibid. Carey, footnote 28, p 33.
[124] Ibid.
[125] Ibid. Kelleher and Murray, footnote 41, p 153.
[126] Article 6(1)(a) GDPR.
[127] Article 4(11) GDPR.
[128] Recital 32 to the GDPR.
[129] Article 7(3) GDPR.
[130] Article 6(1)(b) GDPR.
[131] Article 6(1)(c) GDPR.

by a bank for investigation is a lawful purpose even if the consent of the individual is not obtained. The fourth condition for lawful processing is for the protection of the vital interest of the individual[132] and this condition is only applicable when there is no other lawful basis for processing data and it is in the best interest of the individual such as in an emergency medical situation. Processing personal data to protect vital interest may be done for public interest such as for humanitarian purposes, like for monitoring epidemics and their spread.[133] Processing of personal data necessary for the performance of a public interest task or in the exercise of official authority is considered lawful.[134] For this condition to be applicable there must be a law on which the processing is based that requires the controller to exercise his official authority or which requires the performance of a task to be carried out in the interest of the public. The Union or Member State law shall be the determinant of 'whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association'.[135] The last condition for lawful processing as stated in Article 6(1)(f) of the GDPR is processing necessary for the legitimate interest of the controller or third party.[136] The legitimate interests of the controller or the third party must be weighed against the interests or fundamental rights and freedoms of the individual in order to determine which is more important.[137]

The principle of fairness requires that personal data be processed with the individual's best interests at heart. Bygrave opines that the principle of fairness is broader than can be seen from its connotation.[138] Kelleher and Murray posit that the principle of fairness is unclear but may become clear using the concept of proportionality in explaining it.[139] According to Bygrave, the logical expectations of individuals must be taken into account by data controllers in the processing of their personal data and further processing must not unreasonably interfere with the privacy interests of the individual.[140] Personal data or its

[132] Article 6(1)(d) GDPR.
[133] Recital 46 to the GDPR.
[134] Article 6(1)(e) GDPR.
[135] Recital 45 to the GDPR.
[136] Article 6(1)(f) GDPR
[137] Recital 47 to the GDPR.
[138] Ibid. Bygrave, footnote 114, p 146.
[139] Ibid. Kelleher and Murray, footnote 41, p 138.
[140] Ibid. footnote 114.

processing must not be obtained by undue pressure or duress.[141] Processing of personal data in fairness also requires that individuals must be informed of any risks that may result from processing their personal data in order to prepare them for any adverse effects.[142]

The principle of transparency requires that any information that relates to the processing of personal data must be clear and unequivocal to ensure that the risks, rules, safeguards and rights involved in the processing of the data are understood by the individuals. Information should be given before processing of data begins and in the course of processing, if need be. For instance, if data was collected to be processed for one purpose, and the purpose for which it was collected changes, then the individual must be informed. Transparency also requires that the purpose for processing of personal data and the identity and address of the organisation or institutions processing the data should be known to the individual. Individuals must be able to access their data irrespective of where the processing occurs.[143]

2.1.2 The Principle of Purpose Limitation

Purpose limitation requires that data collected should be for 'specified, legitimate and explicit purposes' and such data should not be processed in a way that is not compatible with the purposes for which it has been collected.[144] This principle is related to the principle of lawfulness, fairness and transparency as it requires controllers to state in clear terms the purposes for which personal data is to be processed before it commences.[145] The principle of purpose limitation also requires that the purpose for processing personal data should be legitimate. A specific purpose exists, for example, when an online store requires the consumer's telephone number and address for the purpose of delivering the consumer's goods but if the online store starts to send newsletters to the consumer, then it will be in breach of this principle.

The purposes for processing personal data must only be used for the original purpose for which it was collected.[146] Controllers are allowed to use data for purposes that are incompatible with the original purpose for which it was collected in cases where it is for archiving purposes in the public interest; scientific or historical research purposes; or

[141] Ibid.
[142] Ibid. Handbook on Data Protection, footnote 43, p. l17.
[143] Recital 39 to the GDPR.
[144] Article 5(1)(b) GDPR.
[145] Ibid. footnote 43.
[146] Ibid. Carey, footnote 28, p 34.

statistical purposes.[147] In the determination of whether a new purpose is compatible or not, the controller should discern if there is a link between the original purpose for collecting data and the new purpose, the circumstances surrounding the original collection of the data, the type of personal data which can be either sensitive or non-sensitive, the possible effects on individuals in relation to the new processing and the safeguards which have been put in place such as encryption.[148]

2.1.3 The Principle of Data Minimisation

The principle of data minimisation stipulates that 'personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed'.[149] This principle requires data controllers to process data that would aid the purpose for which it is collected. The controller must ensure the personal data being processed is sufficient to achieve the stated purpose, is related to the stated purpose and is restricted to the amount of data necessary to achieve the stated purpose, not more than needed.[150]

In determining whether processing of personal data meets the data minimisation principle, the purpose for processing of data will be examined and it differs from one individual to another. Thus the data which would be required of a person with prosthetic legs who applies for a driver's licence would be different from that required of a person without prosthetic legs. The principle also requires that personal data which is insufficient for its stated purpose should not be processed. Controllers are prohibited from collecting excessive data in the hopes that it will be used sometime in the future. For instance, information about an individual's next of kin is relevant and minimal in case of an emergency but information about the family members of an individual will be excessive if the controller collects it in the event that the next of kin is unavailable during an emergency. There may however be circumstances which could warrant the collection of more data than is necessary such as where a student has an allergy, the school could collect information about the type of allergy and the medication or treatment required so as to prepare for an allergic reaction which may never occur.

[147] Article 89(1) GDPR.
[148] Recital 50 to the GDPR.
[149] Article 5(1)(c) GDPR.
[150] Ibid. Handbook on Data Protection Law, footnote 43, p 127.

2.1.4 Principle of Accuracy

The principle of accuracy requires that personal data should be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.[151] Kelleher and Murray believe that this principle is highly significant and must be read in line with the right of rectification[152] which allows an individual to seek correction of their data from the controller when an inaccuracy is discovered.[153] An obligation is placed on controllers to ensure that data collected is correctly recorded. The source of the data must be recorded and where it is discovered that personal data is incorrect for its stated purpose of processing, then rational measures necessary to correct or delete the incorrect data should be taken promptly.[154] Accuracy also requires that personal data collected is regularly checked to ensure that it is current. The application of this principle is necessary in all data operations.

The obligation to ensure accuracy of personal data must be viewed in the context of the purpose of processing the data. Thus where an employee receives a pay cut, the records should be updated by the employer for tax purposes. Provisions should be made for individuals to check the accuracy of their personal data and correct or delete same if necessary. For instance, an employee who has changed his place of residence should be able to delete the old address and replace it with a new one in his bio-data. Some situations forbid the update of personal data because the purpose of storing the data is to record specific events such as in cases of medical records of a wrongful operation, updating the record is strictly prohibited but supplementary remarks could be added to the record.[155] This is important because it might become necessary in future to give an explanation for treatments received by the patient such as for insurance purposes.

Additionally, situations may arise where the failure to frequently check the accuracy of the personal data and update it, if necessary, could be detrimental to the data subject such as where an individual's creditworthiness is important for getting a loan, if the individual formerly had bad credit and thereafter good credit but the data was not updated, this will cause the bank to refuse the request for a loan. Records of mistakes should be kept free of any

[151] Article 5(1)(d) GDPR.
[152] Ibid. Kelleher and Murray, footnote 41, p 143.
[153] Article 16 GDPR.
[154] Ibid. Carey, footnote 27, p 37.
[155] Ibid. Handbook on Data Protection, footnote 42, p 128.

misleading facts about the mistake for instance where an individual is wrongfully convicted of murder, but is later acquitted by the court of murder and convicted for manslaughter, the records must properly reflect this facts.

2.1.5 Principle of Storage Limitation

The principle of storage limitation requires that personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'.[156] Time limits should be created by the controller to enable the review of personal data stored in order to determine whether it is necessary to keep the data longer or not. If personal data becomes unnecessary for the purpose for which it was obtained, then the data should be deleted or anonymised. Thus, it will be a breach of this principle if a food delivery company, like Bolt, stores a customer's address for unreasonably long periods. The company will not be in breach of this principle if it stores the address for three months and then deletes same where it observes that the customer has not used the service in those three months. The GDPR does not provide the time limit for storing data, thus the time limit is set by the controller depending on the purpose for storing the data. Thus the food delivery company could retain the address of the customer for three months to save the customer the time of having to fill in the address every time food is ordered.

The storage limitation principle is applicable to personal data which is stored in such a way that enable the easy identification of individuals.[157] Data may however be stored for longer periods under this principle where it is stored for archiving purposes for public interest, scientific or historical purposes, or for statistical use. The stored data must not be used for any other purposes except that stated above. The controller must set up necessary safeguards to ensure the continued protection of the rights and freedoms of the individual.

The principle of storage limitation is closely connected with the principles of data minimisation and accuracy. This is because the retention of data for longer than necessary

[156] Article 5(1)(e) GDPR.
[157] Ibid. Handbook of Data Protection, footnote 43, p 130.

could lead to it being irrelevant, excessive and inaccurate which is a breach of the principles of data minimisation and accuracy.

2.1.6 Principle of Integrity and Confidentiality

The principle of integrity and confidentiality requires that personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.[158] This is also referred to as the security principle under the GDPR. The obligation of the controller under this principle is to ensure that data is secure by putting in place the necessary safety measures which protects personal data against loss, destruction, damage and unlawful processing. This principle helps to safeguard the individual from detrimental effects which could arise from the dangers of unauthorised or unlawful use of personal data.[159]

The security measures required by the GDPR can either be technical or organisational depending on the circumstances of the case with regular evaluations being conducted. The GDPR further states that 'the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons' must all be considered when implementing the security measures.[160] The improper security of systems by controllers can lead to harm to individuals' personal data such as identity theft, fraud or even physical harm through loss or abuse to personal data. Security of systems is necessary for compliance with other aspects of the GDPR.

Pseudonymisation and encryption of personal data are some of the technical and organisational measures which can be used by controllers.[161] Pseudonymising data entails substituting the features in personal data which make an individual identifiable, with a pseudonym and thereafter storing the substituted features separately.[162]

The technical and organisational measures adopted must ensure the 'confidentiality, integrity and availability' of the controller's systems and services and the personal data processed within them. The measures must enable timely restoration of access to personal data in case

[158] Article 5(1)(f) GDPR.
[159] Ibid. Handbook on Data Protection, footnote 43, p 131.
[160] Article 32(1) GDPR.
[161] Ibid.
[162] Ibid. footnote 160.

there is a physical or technical occurrence. Serious personal data breaches must be reported to the supervisory authorities and where it would probably result in a violation of rights, the individuals whose data has been breached should be notified.[163] Controllers must also put in place the necessary processes to assess the efficacy of their measures and carry out any necessary improvements.

2.1.7 Principle of Accountability

The principle of accountability under the GDPR states that 'the controller shall be responsible for, and be able to demonstrate compliance with the other principles'.[164] Controllers are expected to take responsibility for processing of personal data and if necessary, show the ways in which they have complied with the other principles of processing data in the GDPR.[165] This principle entails measures which include the recording and reporting of personal data breaches,[166] implementing personal data protection policies and security measures, documentation of processing events and regular updates of personal data and deletions,[167] where necessary. The obligation of controllers under this principle is a continuous one and as a result, controllers must constantly reassess and update accountability measures if necessary.[168]

2.2 Application of the EU's Principles of Processing Personal Data by the European Court of Justice

The decisions of the CJEU in relation to the principles of processing personal data are relevant because the interpretation of the law by the CJEU through its decisions have been helpful in the clarification and uniform interpretation of EU law. Its decisions have also aided a better understanding and application of EU law. It should be noted that there are currently few decided cases of the CJEU resulting from issues arising from the GDPR because the GDPR became legally binding in 2018 and is thus relatively new. However, the decisions of the CJEU of issues arising from the principles of processing personal data under the provisions of the Directive are still valid and applicable to the GDPR because

[163] Ibid. Alsenoy, footnote 52, p 41.
[164] Article 5(2) GDPR.
[165] Ibid. Kelleher and Murray, footnote 41, p 151.
[166] Article 33 and 34 GDPR.
[167] Article 35 and 36 GDPR.
[168] Ibid. Handbook on Data Protection, footnote 43, p 134.

though the Directive was repealed, the substantive provisions on the principles of processing of personal data are similar except for the principle of accountability which was first introduced in the GDPR. The decisions of the CJEU on the principles of processing personal data have helped in both the development and improvement of the data protection laws in the EU.

The CJEU in Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)[169] held that where a public administrative body of a Member State transmits personal data to another public administrative body that further processes those data, the data subjects must be informed about that transmission.[170] One of the issues for determination was whether the data subject should have been informed of the identity of the data controller and the purpose for transmission of tax data which related to the income of the data subject from the National Tax Administration Agency to the National Health Insurance Fund in Romania for processing. The principles of lawfulness, transparency and purpose limitation in the processing of data were upheld in this case. The failure of the administrative body to inform the data subject about the intention to transfer and the actual transfer of personal data to another body for use other than that for which consent was given is a breach of the principle of lawfulness and transparency which requires consent of the data subject to be obtained for further processing of the data and for the data subject to be informed of what the data is been processed for and the identity of the data controller. It is also a breach of the principle of purpose limitation which requires that personal data should only be collected for a purpose that is specified in advance, and that those data should not be used for purposes that are not compatible with the stated purpose.

The case of Peter Nowak v Data Protection Commissioner[171] related to the refusal of the Data Protection Commissioner to allow Mr Nowak view his corrected exam script because the information contained in it did not constitute personal data.[172] The issue arose when Mr Nowak wrote an accounting examination and failed even though it was an open book examination. He thereafter requested access to his exam script but his request was refused. Upon the refusal by the examination body, he sent a complaint to the Data Protection

[169] C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others.
[170] Ibid. para 28-46.
[171] Case C-434/16, Peter Nowak v Data Protection Commissioner.
[172] Ibid. para 2.

Commissioner who responded that 'exam scripts do not generally fall to be considered [for data protection purposes] … because this material would not generally constitute personal data'.[173]

The CJEU was asked to determine whether the exam script constituted personal data. In arriving at its decision, the Court examined whether the principles for processing of personal data would apply in that particular situation or not. The Court stated that as long as the principles of accuracy and storage limitation under Article 6(1)(d) and (e) of the Directive apply to written answers submitted by a candidate at a professional examination and the comments made by an examiner in relation to the answers, the Court must hold that permitting a candidate access to those answers and to those comments, protects the right to data protection of the candidate as guaranteed under the Directive.[174] From the decision of the CJEU in Nowak's case, it can be said that the principles of processing personal data can help an organisation clarify doubts as to whether information constitutes personal data or not. Thus if any of the principles or rights under the GDPR apply to the information, then it can be concluded that it is personal data.

The decision of the CJEU in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González[175] is highly significant in relation to processing of data as it helped to develop certain principles. In the case, Mario Costeja whose house was issued a confiscation order which was published in a newspaper that eventually digitised its publications requested for the erasure of his personal data from the publication.[176] This was because any search on Google relating to him brought up these newspaper publications. He argued that since the confiscation procedure against his house had been terminated, it was irrelevant in the present that he was still being referenced.[177] His claim was dismissed by Spanish Data Protection Authority on the ground that the article was lawfully published in the newspaper.[178] It however decided that Google Spain and Google Inc. being search engines are data processors and should thus erase the personal data of Mario Costeja.[179]

[173] Ibid. para 18-21.
[174] Ibid. para 56.
[175] Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
[176] Ibid. para 14.
[177] Ibid. para 15.
[178]Ibid. para 16.
[179] Ibid. para 17.

Google Spain and Google Inc. appealed the decision which was referred to the CJEU by the High Court of Spain. The issues for determination by the CJEU included whether Google is a controller of personal data and therefore subject to EU law, Google's obligations as a data processor and whether a citizen has the right to request for the erasure of his personal data from Google. The CJEU held that Google is a controller of personal data because it "collects such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results" and also because it determines the purposes and means of this processing.[180]

The Court further held that Mario Costeja had a legitimate right to deny the disclosure of his personal data, even if such disclosure is not harmful to him and this right is based on his right to privacy. Consequently, he could request the erasure of his data, if the information disclosed is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine". The Court reiterated that Mario Costeja had the appropriate right to request the erasure of the data and Google had the obligation to erase the data.[181] This decision introduced the right of individuals to be forgotten and the obligation on data controllers to respect the right. The principles of purpose limitation and data minimisation in processing personal data were applied by the CJEU in this case.

2.4 Examination of Section 2 of the Nigeria Data Protection Regulation, 2019

It is pertinent to restate that the Nigeria Data Protection Regulation is a secondary source of law and as a result, its influence on data protection in Nigeria will be restricted especially where its provisions are in conflict with acts of parliament.[182] Pending the enactment of a principal data protection legislation, the Regulation will serve as a mechanism to regulate the processing of personal data in Nigeria and as such, the principles of processing personal data as contained in section 2 of the Regulation will be examined. The preamble to the Regulation states that the use of online information systems by public and private organisations, the need to protect personal data against breaches and the recognition of data protection regulations in other jurisdictions is the basis for issuing the Regulation.

[180] Ibid. para 41.
[181] Ibid. para 99.
[182] Ibid. footnote 104.

Processing in relation to information or data is defined by the Regulation to mean obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: (a) organisation, adaptation or alteration of the information or data; (b) retrieval, consultation or use of the information or data (c) disclosure of the information or data by transmission or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.[183] By this definition, any action that is carried out on the personal data of an individual is processing. Thus the receipt of the information of a person seeking admission into a university will amount to processing if the university acts on the information. However, in processing the information, the university must respect certain rules laid down by the applicable legislation.

The rules of processing of personal data are as stated in Section 2.1 of the Regulation under the sub-heading 'governing principles of data processing'. Section 2.1(1) provides that personal data shall be (a) 'collected and processed in accordance with specific, legitimate and lawful purpose consented; (b) adequate, accurate and without prejudice to the dignity of human person; (c) stored only for the period within which it is reasonably needed; and (d) 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.'[184] Section 2.1(2) provides that 'anyone who is entrusted with the personal data of a data subject or in possession of same owes a duty of care to the said data subject'.[185] Section 2.1(3) provides that 'anyone who is entrusted with the personal data of a data subject or who is in possession of same shall be accountable for his acts and omissions in respect of data processing'.[186]

It is important to state that data protection in Nigerian legal system being a budding area of law is deficient of scholarly works on the principles of processing personal data in Nigeria and as a result, the author will analyse these principles through factual situations and general trends observed in Nigeria to have either been in breach or in compliance with the principles of processing personal data as contained in the Regulation.

[183] Section 1.3 Regulation.
[184] Section 2.1(1) (a-d) Regulation.
[185] Section 2.1(2) Regulation.
[186] Section 2.1(3) Regulation.

2.4.1 Principle of Lawfulness and Purpose Limitation

The principle of lawfulness and purpose limitation in the Regulation require that personal data must be obtained lawfully and processed for the specific purpose for which consent was given by the individual. Hence processing personal data for a purpose which was not specified at the time of obtaining consent or for a purpose for which consent was denied is a violation of this principle. Also obtaining and processing of personal data in a manner which is illegal under any law in Nigeria, contradicts the principle of lawfulness. Further processing is however allowed under the Regulation for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[187]

A daily violation of this principle is observed on widely used social media sites in Nigeria such as Facebook and Nairaland, which together with their stated purpose which is the connection of persons also send targeted advertisements to individuals. Personal information collected under this principle can only be used for purposes other than that for which it was collected after the consent of the individual has been obtained. Thus in the popular case of Godfrey Nya Eneye v MTN Nigeria Communication Ltd,[188] the receipt of unsolicited texts from third parties such as telemarketing companies to whom the plaintiff did not disclose his telephonenumber, is a violation of the principle of purpose limitation as the personal information of Godfrey Eneye was obtained by the defendant for the specific purposes of rendering telecommunication services such as the receiving and making of phone calls, sending of text messages and provision of internet services. It is also a breach of the principle of lawfulness because the Regulation forbids the transfer of personal data to any person.[189]

In order for processing of personal data to be lawful, the Regulation sets out five conditions in Section 2.2. The conditions for lawful processing include processing after consent has been given by the individual,[190] processing necessary for the performance of a contract in which the individual is a party,[191] processing necessary to comply with a legal obligation,[192] processing necessary for the protection of the individual's vital interests or of another living

[187] Section 2.1(1)(a)(ii) Regulation.
[188] Ibid. footnote 109.
[189] Section 2.1(1)(a)(i) Regulation.
[190] Section 2.2(a) Regulation.
[191] Section 2.2(b) Regulation.
[192] Section 2.2(c) Regulation.

person[193] and processing necessary for the performance of a duty in the public interest or in exercise of a public obligation.[194] The Regulation further lays down the rules for obtaining consent by providing that consent must not be obtained by fraud, coercion or undue influence. Individuals must be informed of their right to withdraw consent easily before the consent is given. Consent of the individual must be obtained before transfer of personal data to a third party. The consent must be unequivocal and the onus is on the controller to ensure that consent was properly obtained before processing of data commenced.[195]

It was reported in 2015 that Passenger Name Records were collected before commercial flights for screening of passengers by the agencies in charge of border security such as the Nigerian Police Force, Department of Security Services, Nigerian Customs Service, Nigerian Immigration Service and the Nigerian Military.[196] The transfer of the passengers name records to the border security for the purposes of screening can be argued to be lawful processing necessary for compliance with a legal obligation. It can also be argued to be a violation of the principle of purpose limitation if there is no reasonable suspicion of any security threat.

2.4.2 Principle of Data Minimisation, Accuracy and Fairness

The Regulation requires personal data to be adequate, relevant and limited to what is necessary with regards to the purposes for which it is processed and personal data must be accurate and up to date.[197] It also requires that consideration must be had for the dignity of the individual in processing of personal data.[198]

The aim of data minimisation is to ensure that controllers do not collect more data than is necessary to achieve a specified aim. Thus data will be excessive if the political view or sexual orientation of an individual is asked on a job application. In 2019, the app, Truecaller which aids the identification of unknown numbers, was accused by the NITDA of violating the principle of data minimisation by obtaining more information than it needed for its

[193] Section 2.2(d) Regulation.
[194] Section 2.2(e) Regulation.
[195] Section 2.3 Regulation.
[196] U.S. Department of State, Chapter 2. Country Reports: Africa Overview, 2015, available at https://2009-2017.state.gov/j/ct/rls/crt/2015/257514.htm accessed on 06/03/2020.
[197] Section 2.1(1)(b) Regulation.
[198] Ibid.

purpose.[199] Furthermore, organisations in Nigeria such as banks and telecommunications operators oftentimes collect more information than is necessary for specified purposes. For instance, in order to open a bank account, a person is asked their state of origin and local government area which is irrelevant data in those circumstances.

The principle of accuracy places a continuous obligation on controllers to ensure that personal data is correct and up to date. This is because inaccurate data could be detrimental to an individual such as where a life altering decision is made on incorrect data. For instance, the Credit Reporting Act 2017 (CRA) requires the Credit Bureaux to update their database regularly in relation to the nature of information stored whenever information is provided by a Credit Information Provider.[200]

There have been situations where newspapers have published controversial stories about certain persons using the photograph of other people. These incidences were corrected by putting out the correct picture of the concerned individual. Accuracy requires that information that is incorrect should immediately be rectified or erased. This requires individuals to have access to their personal data in order to make any necessary corrections. It is believed that the steps for rectifying of personal data under this principle should not be tedious as tedious procedures for rectification of data could discourage an individual from taking steps to correct inaccuracy in their data. In Nigeria, correction of errors on an international passport can be done by filling an online form to that effect on the NIS website which must thereafter be submitted in person to the NIS headquarters in Abuja.[201] The Joint Admissions and Matriculation Board (JAMB) which regulates admissions into the higher institutions on the other hand allows for correction of data to be done in the state of resident[202] which is less tedious than the procedure of the NIS.

This principle places an obligation on both the data controller and the individual to ensure that data is accurate. The controller however has more obligations because it has to ensure

[199] Y. Kazeem, Nigeria is investigating a Swedish call blocking app for privacy breaches but exposes holes in its own laws, published 24/09/2019, Quartz Africa, available at https://qz.com/africa/1714872/nigeria-investigates-truecaller-amid-lagging-data-protection-laws/ accessed on 06/03/2020.
[200] Section 6(1)(d) CRA.
[201] Nigeria Immigration Service, Passport Application: Correction of error(s), available at https://immigration.gov.ng/standard-passport/ accessed on 06/03/2020.
[202] Joint Admissions and Matriculation Board, Correction Of Data: Correction Of Names, available at https://www.jamb.org.ng/changeName.htm accessed on 06/03/2020.

that the date is accurate and up to date, and where inaccuracies are discovered, immediate steps must be taken to correct them.

The principle of fairness in the Regulation is expressed as human dignity and it requires controllers to process personal data respectfully in a manner and for purposes which an individual would reasonably expect such that he or she does not become a victim of unfair negative effects from the failure of the controller to process data fairly. Thus obtaining of personal data through misrepresentation or deception and using it in a manner that adversely affects the individual contradicts the principle of fairness. The provision of the names, telephone numbers and location of many Nigerians by the Independent National Electoral Commission (INEC), the body responsible for conducting the elections to the All Progressives' Congress (APC) during the general elections in 2019, which led to the receipt of telephone calls from unknown persons campaigning for the ruling party is clearly a breach of the principle of fairness. This is because the personal data which was obtained for registration of voters for elections was unlawfully transferred to the APC and thereafter used in a manner which was not reasonably expected by the citizens, that is for campaign purposes.[203]

2.4.3 Principle of Storage Limitation

Storage Limitation requires controllers not to store personal data for a period longer than is necessary for the purpose for which it was collected and when it is no longer needed it should be deleted. Controllers can only store personal data for as long it is needed, for the specific purpose for which it was obtained.[204]

This principle is important because storing of personal data for longer than is necessary can make it susceptible to exploitation. Internet service providers in Nigeria are mandated by the NCC Guidelines to store personal data related to internet service for at least twelve months[205] which is in violation of the principle of storage limitation as the personal data could be hacked. It has been established that data retention policies amount to an interference with the

[203] O. Adanikin, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, International Centre for Investigative Reporting published 01/02/2019 available at https://www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/ accessed on 06/03/2020

[204] Section 2.1(1)(c) Regulation.

[205] Nigerian Communications Commission, Guidelines for the Provision of Internet Service, https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/62-guidelines-for-the-provision-of-internet-service/file.

right to privacy[206] and also, mandatory data retention limits the ability of individuals to stay anonymous.[207]

Furthermore, the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 mandates service providers to keep all prescribed traffic data and subscriber information for at least two years.[208] The CRA requires the credit bureau to maintain credit information for at least six years from the date the information was obtained and the information can be further archived for ten years and after which they will be destroyed by the credit bureau.[209]

2.4.4 Principle of Integrity and Confidentiality

This principle as contained in Section 2.1(1)(d) of the Regulation provides that personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This principle requires information risk assessment to be carried out by data controllers using data discovery tools to identify personal data vulnerabilities in their systems, which should be strengthened to ensure the personal data in their care is highly secured and is not at risk of being easily obtainable by cyber fraudsters. This is the security principle of the Regulation and it is highly important because of the need to protect the personal data of individuals from breaches which may result from poor technical or organisational measures.

The rampant hacking of public and private websites in Nigeria is proof of the necessity of this principle. For instance the website of a Nigerian airline company was hacked in 2019 by a group called the Moroccan Revolution Team.[210] The website was inaccessible to the customers of the airline for at least five hours. The ability of the website to be hacked showed a defect in the security structure of the airline which put the personal data of its customers at

[206] Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para 22 (23 April 2014).
[207] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015), noting at paragraph 55: "Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."
[208] Section 38(1) Cybercrimes(Prohibition, Prevention, Etc) Act 2015.
[209] Section 5 CRA.
[210] S. Okike, Nigerian airline company, Aero Contractors website hacked by allegedly ISIS-tied group, Techpoint.africa, published on 14/08/2019, available at https://techpoint.africa/2019/08/14/nigerian-airline-company-aero-contractors-website-hacked-by-alleged-isis-tied-group/ accessed on 6/03/2020.

risk. Additionally, in 2018 a hacker who was arraigned by the Nigerian Police stated that he hacked the Nigerian banking system with ease such that he was able to obtain customers' information and withdraw money from various bank accounts.[211]

Public websites are not exempted from breaches as the National Assembly website, Small and Medium Enterprises Commission website and the Nigerian Court of Appeal website have been hacked[212] with personal data of over one thousand persons released during the hack of the National Assembly website.[213]

The register of voters which is maintained by INEC has constantly been mishandled and released to the public to the detriment of the individuals whose data is contained on those registers. This is because the personal data of these individuals are used by political parties to commit election fraud, thereby impacting on the fairness of the elections. This is due to a lack of adequate security measures on the part of the electoral body.

2.4.5 Duty of Care

This principle states that the controller owes a duty of care to the individual.[214] According to the Black's Law Dictionary, duty of care is a legal obligation which is owed by one person to another person which must be fulfilled.[215] The controller under this principle must ensure that the obligations arising out of the Regulation in relation to the processing of personal data are complied with. These obligations include processing of data in accordance with the laid down principles and respecting the rights of the individual such as access to personal data, information regarding the purposes for processing an individual's personal data and the third parties to whom the data may be disclosed.[216]

---

[211] E. Usman and L. Nwanekwu, Hacking into Nigerian banks very easy, says medical doctor turned cyber-criminal, Vanguard, published on 20/05/2018, available at https://www.vanguardngr.com/2018/05/993772/ accessed on 6/03/2020.
[212] J. Daniel, Top African data breaches, security stories show enterprises under stress, CIO, published on 7/01/2020, available at https://www.cio.com/article/3512957/top-african-data-breaches-security-stories-show-enterprises-under-stress.html accessed on 06/03/2020.
[213] Waqas, Nigerian National Assembly Hacked, Huge Database Leaked by @LolSec, HackRead, published on 23/10/2012, available at https://www.hackread.com/nigerian-national-assembly-hacked-huge-database-leaked-by-lolsec/ accessed on 06/02/2020.
[214] Section 2.1(2) Regulation.
[215] Black's Law Dictionary, 7th Ed. United States of America, West Publishing Co. 1999, p 521.
[216] Section 2.13.6 Regulation.

2.4.6 Principle of Accountability

This principle places the responsibility of ensuring that all the other principles set out in the Regulation are complied with on the controller. Hence the controller must be conversant with the principles that need to be complied with and thereafter ensure that system checks are regularly carried out so as not to fall into a breach.

2.5 Comparison of the Principles of Processing Personal Data in the EU and Nigeria

The principles of processing personal data provided by the GDPR and the Regulation are similar and this is probably because the GDPR served as a model for the Regulation. Thus all the principles including the accountability principle which was first introduced in the GDPR is incorporated into the Regulation. Also the reasons for storing data longer than necessary in both instruments are similar and these include when personal data is stored for archiving purposes for public interest, scientific or historical purposes, or for statistical use. The conditions for lawful processing of personal data provided in the Regulation are similar to that provided in the GDPR except lawful processing for the legitimate interest of the controller. The Regulation does not provide for the pseudonymisation and anonymisation of data which is stored for longer than necessary unlike as provided in the GDPR.

The form and structure of some principles in the Regulation are different but the substance is similar to that contained in the GDPR. Thus the inclusion of duty of care and human dignity in the Regulation is for the overall objective protecting personal data by ensuring that certain rules are followed in order to prevent any adverse effects to the individual which may result from the controller's failure to adhere to the laid rules. Hence irrespective of the phrasing, the substance and results of both instruments will be similar.

The judicial jurisprudence on the principles of processing data in the EU is surplus as the CJEU has in a plethora of cases decided issues which arose from the principles of processing personal data in the EU. This has led to the establishment of the right to be forgotten which emanated from the principle of storage limitation. The principles of processing in the Regulation have not been judicially tested in Nigeria and violations of these principles abound.

3. TOWARDS REALISING EFFECTIVE DATA PROTECTION IN NIGERIA

The absence of a principal data protection legislation has for long created a void in protecting personal data in Nigeria and has led to a multiplicity of incomplete and ultimately ineffective data protection provisions. This void though somewhat filled with the issuance of the Regulation which validity is still in question, has raised several issues such as national security issues stemming from the daily processing of personal data of Nigerians by both public and private institutions and even third parties. Personal data breaches are highly prevalent as is seen from the preceding chapter as a result, the provision and safeguarding of a right to data protection distinct from the right to privacy as well as the enactment of a data protection law should be a major source of focus and motivation for all Nigerians especially because technological advancements are not slowing down with almost all daily activities being done virtually.

3.1 Lessons arising from the comparative analysis of the Nigerian and EU data protection legal systems

The comparative analysis of the data protection systems of Nigeria and the EU has helped to reveal the amount of effort required in the Nigerian system to help it achieve optimal data protection. The commitment of the EU to data protection is evident in its human rights-based approach to data protection. This is seen from the inclusion of a fundamental right to data protection in the Charter[217] and the adoption of the GDPR which has been described as the most significant regulatory revolution in relation to data protection in contemporary times.[218] The intention of the drafters of the GDPR is to make sure that human rights are implanted in handling of personal data by all organisations. Nigeria needs to adopt a human-rights based approach to data protection as the absence of rudimentary data protection laws provide with clarity a complete disregard for protection of personal data in Nigeria. The clamour for comprehensive and strict data protection laws cannot be over-emphasised as many foreign governments keep finding new ways to interfere in the domestic affairs of other countries as seen in the interference of Russia in the American elections held in 2016 and the exposure by

[217] Article 8 of the Charter.
[218] C.J. Hoofnagle, B. Sloot & F. Borgesius, The European Union General Data Protection Regulation: what it is and what it means- 28:1 Information & Communications Technology Law 2019, 65-98, p 3, available at https://doi.org/10.1080/13600834.2019.1573501 accessed on 10/03/2020.

Edward Snowden of the mass surveillance of individuals by the American National Security Agency through the records of personal data of companies such as Google and Facebook.[219]

The legality of the GDPR as a mechanism for the protection of personal data is indisputable as it was enacted by the EU Parliament to ensure adequate and uniform control in the EU over the use and access of organisations to the personal data of EU nationals. The GDPR being a regulation and a primary source of law is directly applicable to EU member states. The legality of the Regulation issued by the NITDA has been questioned thus creating doubts as to whether the Regulation will be complied with or not. Salami opines that the NITDA lacks the powers to enforce the fines for breach of the Regulation because even though the enabling act allows it to develop regulations for electronic governance, its ability to charge and receive fines is arguably beyond the scope of the powers conferred on it by the NITDA Act hence an action could be brought to nullify the provisions for the charging and enforcement of fines. He also further contends that since section 6 of the NITDA Act only empowers the NITDA to make regulations in respect of companies dealing with information technology and the importation of technology, it can be argued that the NITDA lacks the requisite powers to enforce the Regulation against organisations that do not deal in information technology, like the financial sector which is subject to the regulation of the Central Bank of Nigeria.[220] The uncertainty of the legal effect of the Regulation has a tendency to water down its effects and compliance and it is hoped that a judicial decision on the legality of the NITDA to issue the Regulation would lay all the issues plaguing the Regulation to rest.

The GDPR has been said to be complex which makes understanding difficult for the average person[221] hence the need and heavy reliance on the CJEU for the interpretation of data protection laws. The CJEU has been highly instrumental to the development of data protection laws in the EU as its interpretation of data protection laws using a teleological approach has been beneficial in achieving the purposes of the EU in enacting data protection laws. For instance the decisions of the CJEU have helped to expand the definition of personal data in addition to the definition in the GDPR. It has also developed new rights such as the

[219] G. Greenwald, NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 7 June 2013, available at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data accessed on 10/03/2020.
[220] Ibid. Salami, footnote 26.
[221] I. Nicolaidou and C. Georgiades, The GDPR: New Horizons, EU Internet Law, T.-E. Synodinou et al. (eds.), Springer International Publishing AG, Switzerland 2017, p 17.

right to be forgotten as seen in Google Spain's case. The Court has also in some decisions invalidated EU law which it found to be restrictive of the people's rights by using the proportionality test as seen in the Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.[222] These allude to the importance of the courts in the development of the practical application of law in a legal system. The Nigerian courts were innovative in their decisions in the cases of Godfrey Eneye and Barrister Anene, when they applied the right to privacy to cover unsolicited marketing messages thus providing precedent for similar situations which might arise. This type of judicial initiative is highly encouraged especially because of the limited data protection awareness and competence which makes the prosecution of violators near impossible as can be grasped from the lack of case law in that area.

3.2 Challenges of realising effective data protection in Nigeria

The achievement of effective data protection in Nigeria can only happen if the challenges which serve as obstacles are properly identified and tackled. These challenges include:

3.2.1 Lack of a Comprehensive Data Protection Law

The lack of a comprehensive data protection law which has general application is the major challenge to realising data protection in Nigeria. It can be argued that the subsisting laws, regulations and guidelines issued by various regulatory bodies should suffice in protecting personal data in Nigeria. This is erroneous because these laws, regulations and guidelines are not uniform and as a result, the provisions are bound to conflict. Furthermore, each of these Acts, regulations and guidelines has different regulatory bodies for the purposes of enforcement and this will be expensive, confusing and exhausting for organisations, especially for multi-sectorial organisations. For instance, the National Identification Management Commission (NIMC), the body in charge of issuing national identity cards for Nigerians, is in charge of the NIMC Act, the NCC is in charge of Nigerian Communications Regulation and the Central Bank of Nigeria is the supervisory body for the Credit Reporting Act. These are just a few of the supervisory bodies and they all have different enforcement procedures.

[222] Joined Cases C-293/12 and C-594/12.

The right to privacy as provided in the Nigerian constitution which has been used by the courts in Nigeria to determine cases that should have been readily decided under data protection law cannot effectively safeguard personal data because while privacy protects a person's private life, data protection protects information which is not protected under privacy such as the pictures posted on a person's social media page. For example, under the right to privacy, an argument by a newspaper organisation that the pictures posted by a person on their Facebook page are no longer private and can be published will be upheld by a court of law but under the right to data protection, such an argument will be dismissed because though the pictures had become visible and accessible to the public, the newspaper organisation cannot publish same without the consent of the person. Personal data protection entails many technicalities which were not envisaged by the legislature during the drafting of the Constitution. The scope of the right to privacy in the Constitution is limited to the homes, correspondence, telephone conversations and telegraphic communications and does not include automated communications.

Many abuses and exploitation of personal data have arisen in the course of processing of personal data from the lack of data protection legislation. There are currently many cases of databases being hacked with the personal data of users being released to the public by the hackers due to the lack of effective security measures of processing systems and it is impossible to hold the organisations accountable because of the lack of regulation and enforcement mechanisms. Most organisations find the requirements of data protection to be tedious and oftentimes expensive and as a result prefer to do business in countries that have weak data protection systems as in Nigeria. A lack of data protection laws also mean that the personal data of Nigerians will be subject to the laws of other countries who have no legal obligation to protect the data in the manner they would the data of a country with effective data protection law.

Additionally, rights which accrue from a data protection law are being violated daily because of the lack of data protection legislation. For instance, the NCC during an event stated that the Office of the National Security Adviser (ONSA) had unrestricted access to the NCC's SIM registration database for the monitoring and apprehension of criminals.[223] The principles of processing personal data are constantly violated with no recourse for remedy. Moreover,

[223] NCC Confirms FG Monitoring of Phone Calls in Nigeria, March 7, 2018, Technology Mirror, available at https://technologymirror.com.ng/ncc-confirms-fg-monitoring-of-phone-calls-in-nigeria/ accessed 10/03/2020.

the security agencies have oftentimes acted outside the scope of their powers in relation to lawful and authorised surveillance and the high crime rate in Nigeria has shown that surveillance of citizens for the purpose of curbing crime and terrorism is ineffective. The lack of mechanisms for checks and balances will ultimately lead to abuse of powers by the various regulatory bodies.

3.2.2 Lack of Digital Awareness and Understanding

As at January 2020, there were 186,023,609 active telephone subscribers in Nigeria[224] and United Nations Educational, Scientific and Cultural Organisation (UNESCO) in its 2018 statistics claimed that about 41,763,792 Nigerians were illiterate.[225] The term data protection among many Nigerians is significantly new or non-existent and as a result, they do not know the impact of data protection on their daily lives. The lack of knowledge on the part of people has been used by governments to suppress human rights. People are unaware of the power which they wield especially in a democratic society like Nigeria. Many of the literate population that should stand in the gap for the illiterate population in relation to data protection are nonchalant about the consequences which might result from the lack of effective data protection. Hunger for knowledge is fast depreciating with people dwelling more on frivolities such as the latest trends in fashion or technology rather than obtaining knowledge for the purpose of closing the gap between what should be known and what is already known. It is a common occurrence to read stories which include the personal data of individuals being shared on social media sites and blogs. For instance, the author recalls a tweet which called for the publication of the photograph and name of the Italian citizen who allegedly travelled into Nigeria with COVID-19 with many replies echoing this sentiment. This is irrespective of the fact that publicising the name and photograph would be a breach of doctor-patient confidentiality which is a known phenomenon in Nigeria.

Additionally, the official language of Nigeria is English, thus all laws and regulations are written in English irrespective of the fact that there are also official languages[226] in various regions of Nigeria. Therefore a businessman in the North who only speaks Hausa is most

[224] Industry Statistics, March 16, 2020, Nigerian Communications Commission, available at https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables accessed on 10/03/2020.
[225] Education and Literacy, UNESCO Institute for Statistics, available at http://uis.unesco.org/en/country/ng accessed on 10/03/2020.
[226] Apart from English Language, the three major languages are Yoruba which is spoken in the West, Hausa in the North and Igbo in the East.

likely going to be unaware of any provisions which relate to data protection. The laws are not interpreted by the state and local governments into the indigenous languages of the regions and are thus inaccessible to individuals who do not speak English.

3.2.3 Lack of Political Will

The lack of desire to protect personal data on the part of the Federal Government is a major challenge to effective data protection in Nigeria and this is because effective data protection laws will be detrimental to some of the Federal Government's policies and actions such as the surveillance of citizens through various channels such as the registration of mobile SIM cards. For instance, in March 2019, the President of Nigeria failed to assent the Digital Rights and Freedom Bill which was a comprehensive data privacy and protection framework. Its purpose was to protect the privacy and data protections rights of Nigerians and provide legal guidelines regarding surveillance.[227]

The failure of the Government to recognise the importance of data protection is quite disturbing because the personal data of citizens have been accessed as a result of weak laws through hacking of the websites of government agencies. The Government continues to fail in its obligations to protect the citizens and even itself due to the lack of appropriate security measures. Elections are held every four years in Nigeria which means that no person in Government will be in office for life. Using this reasoning, one would think that putting in place appropriate data protection mechanisms which will be beneficial after political office will be a priority for the occupants of political seats in Nigeria. The cost implication of implementing data protection laws might be another reason for the lack of political will. This cost implication arises out of the need to employ specialists in data protection and train the staff in various agencies on data protection unfortunately, the Government's interests are more channelled towards money making policies.

3.2.4 Lack of a Judicial Activism

The Nigerian judiciary has endured a rather tumultuous history ranging from the harassment and persecution of judges during the military era to political interference, corruption and

[227] V. Ekwealor, Nigeria's president refused to sign its digital rights bill, what happens now?, published March 27, 2019, Techpoint.africa, available at https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/ accessed on 10/03/2020.

intimidation in the present democratic era. Unlike presently, some of the judgments of the Supreme Court during the military era were landmark judgments which period promoted judicial activism. One of the landmark decisions was that of the Supreme Court in Abacha v Fawehinmi,[228] where it was held that the domestic courts could apply the provisions of the African Charter on Human and Peoples Rights to allegations of violations of fundamental rights since it had been ratified and domesticated by the National Assembly. This confirmed that the role of the judiciary is not limited to interpreting laws but also to development and encouragement of direct action in the legal system. Presently, the judiciary is battling political interference from the executive because of its dependence on the executive for funding. The lack of independence of the judiciary along with corruption of some judges and nepotism in the appointment of judges which results in the appointment of non-qualified individuals and consequently, low quality judgments, have been detrimental to judicial activism in Nigeria.

The dependence on the executive arm of government for funding has led to a watering down of judgments especially in situations where the Government is a party in a suit. Many judges are afraid to give decisions against the Government for fear that they will be victimised and subsequently removed. For instance, in 2016, the homes of some judges were raided by the State Security Service in the middle of the night on allegations of corruption. The crackdown continued till January 2019, when the Chief Justice of Nigeria, Walter Onnoghen was suddenly suspended by the President of Nigeria, days before the general elections and was replaced by another justice without recourse to the National Judicial Council.[229] This was believed to be a calculated attempt by the executive to intimidate the judiciary into doing its bidding.[230]

It is vital in a democracy that judges are impartial and independent of all external pressures so that justice is dispensed fairly and lawfully. The judiciary is supposed to serve as a watchdog for the safeguarding of the rights and freedoms of citizens against the excesses of the executive. However until the judiciary is independent, the appointments of judges is based on merit and political interference is done away with, the judiciary will not achieve its full potential.

---

[228] (2001) 51 WRN 29.

[229] The NJC is empowered by chapters 20(a) and 21(a) of the Third Schedule of the Constitution to investigate judges accused of misconduct and recommend appropriate sanctions to the President. It also recommends judges for appointment and promotion and enforces the procedures laid down for judges, especially the Code of Conduct for Judicial Officers of the Federal Republic of Nigeria.

[230] Nigerian chief justice's suspension raises international concerns, January 26, 2019, BBC News, available at https://www.bbc.com/news/world-africa-47015698 accessed on 10/03/2020.

3.2.5 Lack of cooperation between the Public and Private Sectors

A lack of cooperation between the public and private sectors will continue to pose a challenge for data protection in Nigeria. The government may remain passive in relation to data protection unless there is a push from the private sector. Granted there are many organisations that might be dreading the cost of implementing data protection mechanisms who are satisfied with the lack of legislation hence they see no reason to push for data protection laws. Many organisations in the private sector are violators of the existing data protection provisions in the subsisting legislation and guidelines hence they will prefer ineffective data protection laws as they could be liable to pay huge fines if the data protection laws were effective.

Furthermore, there are presently many issues plaguing the Nigerian society such as poverty, violations of stated human rights which many non-governmental organisations consider more important than personal data protection.

3.3 Possible solutions to the challenges of realising effective data protection in Nigeria

The growing importance of a comprehensive data protection law is irrefutable and according to Izuogu, Nigeria must take deliberate steps to safeguard personal data by reorganising the legal system to become adaptable to the problems which have arisen from technological advancements. He further suggests that in order to curb the criminal activities which are committed via mobile phones, an effective system which will permit lawful interception should be put in place. This would prevent the use of anonymity in telecommunications for criminal activities which is the reason for which the NCC has instructed registration of SIM cards.[231] The National Assembly must take immediate steps to enact a data protection legislation which will cover all aspects of personal data protection such as the principles of processing personal data, the lawful conditions for processing personal data, the rights of individuals, the obligations of data controllers and the procedures for seeking redress for any violations. It must also contain provisions that outline the procedures for lawful and authorized interception of communications within the digital environment without sacrificing the constitutional rights of citizens thus making derogations from data protection very strict. It is important that there is room to amend the data protection law to accommodate any new threat which was not predicted at the time of enactment of the legislation.

[231] C.E. Izuogu, Data Protection and Other Implications in the Ongoing SIM Card Registration Process published on 2nd May, 2010 available at SSRN: https://ssrn.com/abstract=1597665 assessed on 06/03/2020.

It is highly important that the regional instruments on data protection are ratified by Nigeria. These instruments will help to fill the lacuna left by the lack of a data protection law which will give the National Assembly sufficient time to research, draft and enact a law which will cater to the Nigerian society in relation to data protection. The only advantage to not having a data protection legislation is that there are model laws and practices from which inspiration can be drawn thus Nigeria can adopt the best practices from the regional instruments and the data protection laws of other countries and regions and enact a law that reflects Nigerian realities. Thus the Supplementary Act of ECOWAS and the GDPR which are both comprehensive data protection instruments could serve as models for the Nigerian data protection law.

A law is as good as its enforcement and as such, comprehensive data protection legislation will be weakened if there is no independent data protection regulator. The law must provide for an independent law enforcement agency to monitor the implementation of the law and enforce its provisions where necessary. The legislation should be further strengthened by ensuring that the regulator is not answerable to the government as the independence of the regulator is important for effective safeguards of the personal data of Nigerian citizens. An independent regulator will ensure that government agencies and private organisations follow the stipulated law when collecting and handling the personal data of citizens. Furthermore, in the case of any breach of the law by the government for instance, the data regulator will not hesitate to take the necessary steps to remedy the breach without fear of being dismissed, where the head of the regulatory body is a government appointee, or cutting off of funds. The regulator must be extremely knowledgeable about data protection such that it is able to readily furnish sound guidance on all the provisions of the data protection legislation.

The public and private sectors have to take the necessary steps to train the members of their staff to ensure strict adherence to the data protection legislations. This will ensure that the members of staff have sufficient understanding of the organisation’s obligations in the collection and processing of personal data in the course of executing their duties. The data protection legislation should also mandate the publication of the processes which have been taken to comply with the legislation by all the public institutions and the private organisations. There should be a reasonable time limit attached to it. Furthermore, the legislation should provide corrective and punitive measures for failure to fulfil the law and these measures should be proportionate to the probability of damage caused by the breach

and gravity of the failure to fulfil stipulated obligations. Nigeria can also host an international conference on data protection which will likely draw the best minds in the field from all over the world to discuss the developments and changes in data protection. This will help in the education of private and public organisations. Participation in international conferences on data protection should also be encouraged through governmental subsidising or private sponsorship of persons interested in data protection to attend the conferences.

Awareness about data protection and issues which pertain thereto is highly important in achieving effective data protection. Mass education about data protection is important especially in a country like Nigeria which has many citizens who only speak their indigenous languages. It is thus necessary that the rights of citizens and the obligations of the government and private organisations in relation to data protection be simplified and translated into all indigenous languages. This might be tedious and expensive but the state has an obligation to safeguard the rights of its citizens. In order to achieve this, the Federal, State and Local Governments must play their parts to ensure that every citizen is educated on their data protection rights. This can be achieved through the various means of mass media and audio-visual educational materials. In the event that the government lacks the political will to raise the necessary awareness and educate the citizens, then the non-governmental organisations in conjunction with the regulator can educate the citizens on their data protection rights. It is believed that this will increase participation of citizens which will in turn boost compliance and enforcement. Additionally, as computer science and information and communication technology have been added to the curricula of study in Nigeria as compulsory courses, it is also important that data protection is added to the curricula because every Nigerian will at certain points in their lives have their data processed. As a result, it is necessary to ensure that knowledge about data rights are instilled from primary school.

The judiciary is the custodian of the rule of law and democracy in any society and it is thus necessary that it works effectively. The Courts have an important role to play in deciding questions which may arise from the interpreting and application of the data protection laws hence the need to ensure proper and constant training of judges in relation to data protection issues. Just like the controllers and the regulator who must be up to date on data protection, it is also important that the judges keep up with the current trends in personal data protection spheres. Also, the independence of the judiciary is necessary to ensure that justice is done without fear or favour in cases of breach especially when the government is the violating party. Hence the power to appoint and fire judges should be completely vested in the National

Judicial Council, with checks and balances put in place to ensure that the powers are not exploited or abused. Furthermore, no individual, especially a member of the executive should have the discretionary power to fire a judge. The judges should not be afraid to use retributive justice to deter repeat violators of the law. Judicial activism should be encouraged and judges should not be afraid to interpret the laws objectively. In the determination of data protection cases, fairness and justice should be the ultimate goal of judges which would consequently help to develop the data protection laws in Nigeria via the rulings and pronouncements which shall serve as precedents.

Apart from the protection of personal data of EU nationals, the GDPR has also created jobs as organisations in order to ensure compliance with the provisions of the GDPR have had to employ data protection specialists. The high unemployment rate in Nigeria will benefit from an effective data protection system as organisations will need to employ specialists or experts in the field of data protection to ensure conformity.

The above proposed solutions if incorporated will set Nigeria on a path to an effective data protective legal system. However, since the goal is for long term data protection in Nigeria, it is important that the data protection mechanism for enforcement is constantly funded and this can be achieved by the allocation of adequate funds to the regulator which will be provided for in the national budget. These solutions are obviously not exhaustive but the author believes that these are fundamental to effective personal data protection in Nigeria.

CONCLUSION

The purpose of this research paper was to compare the present data protection regulation in Nigeria with that of the EU in order to assess whether the respective legal frameworks provide adequate and effective data protection in relation to the processing of personal data. The need for this research arose out of the technological advancements currently experienced in Nigeria which has resulted in mass processing of personal data by various public and private organisations leading to the abuse and exploitation of the personal data of Nigerians without due regard to the principles of processing of personal data.

The research problem was to evaluate if there is an existing right to data protection in Nigeria under the extant laws in Nigeria in order to determine how it is construed and what it comprises of using the EU as a comparison. In achieving the stated purpose of this research paper, the first research question that was analysed was the definition of personal data in Nigeria and in the EU. The meaning of personal data in the EU is as provided in the GDPR while the applicable definition in Nigeria is that provided in the Regulation of the NITDA. Information which is or can be linked to a living person is defined as personal data and it includes the name, the email address, the medical records and document identification number of an individual amongst other information. The meaning of personal data in both legal systems is similar in words but the application is different as the meaning of personal data in the EU has been expanded by the CJEU to include identifiers which are not specifically listed in the GDPR.

The second research question examined the notion and scope of the right to data protection in both legal systems. Article 8 of the Charter, the GDPR and some decisions of the CJEU were examined to determine whether there is an established right to data protection in the EU. The express provision of the right to data protection in the Charter which member states have an obligation to protect coupled with the adoption of the GDPR for the purpose of supplementing the Charter and ensuring harmonisation of the protection guaranteed in the EU territory is a testament to the existence of an established right to data protection in the EU. This is reinforced by the decisions of the CJEU upholding the right to data protection in its case law and even distinguishing it from the right to privacy in some cases. Furthermore, the scope of the GDPR is the processing of personal data of all living persons in the EU or of EU citizens in another territory thereby allowing the application of the GDPR extraterritorially.

Unlike in the EU where there is a Charter protected right to data protection, the lack of an explicit right in relation to data protection in Nigeria required an in-depth examination of the legal system and the extant laws. As a result the Constitution, the FOI Act, the Regulation and the Consumer Code for telecommunications subscribers were examined and it was deduced that a right to data protection can be inferred from certain laws and regulations. This is because the personal information of individuals, the manner of using it and remedy for violations are provided for by these laws and regulations which is what data protection seeks to achieve. Also the right to right to privacy was utilised by the courts in deciding issues which involved the disclosing of personal information to third parties by telecommunications companies which issue should have ordinarily been adjudicated under data protection. However, these laws and regulations apply to different sectors and lack general applicability hence creating gaps in the legal system. These laws and regulations are also only applicable to citizens of Nigeria living foreign residents vulnerable to exploitation of their data.

The third research question focused on the principles of processing personal data in Nigeria as provided in the Regulation and the EU as provided in the GDPR in order to determine any shortcomings. It was discovered that the principles in both legal systems are similar except for a few inconsequential differences such as the exclusion of the condition of legitimate interests for processing. Court practice on the principles of processing data is prevalent in the EU while there is currently no decided case on issues arising from the principles of processing data in Nigeria even though violations are prevalent. It is concluded from the examination of the principles of processing personal data in both legal systems that that the provisions are indeed adequate and will effectively protect the processing of personal data.

The final research question assessed the challenges which are hindering effective data protection in Nigeria. This was done in order to proffer solutions which could aid the Nigerian legal system in achieving effective data protection. In arriving at the solutions, the final chapter of the research paper highlighted the lessons which were learnt from comparing the EU and Nigeria's data protection systems. The lessons include the need for a human rights based approach to data protection, the importance of an efficient judiciary in a legal system, the importance of a general data protection legislation to regulate and enforce all kinds of processing of personal data. Thereafter, the challenges of realising effective personal data in Nigeria were examined and these include lack of comprehensive legislation, inadequate digital awareness and understanding, lack of judicial activism, lack of political will and lack of cooperation between the public and private sectors. The chapter was

concluded with recommendations which the author believes will help propel Nigeria to the realisation of an effective data protection system with the most significant one being the enactment by the legislature of a data protection law. Some of the other recommendations include cooperation between the private and public sectors, mass education about data protection and support and encouragement of judicial activism.

Information and communication technology has become an undeniable important aspect of daily life. The growth of e-commerce, virtual learning, electronic banking and digitisation of information has made the protection of personal data is now a necessity. Hence the obligation on states around the world to put in place appropriate structures and mechanism for the personal data protection. This research paper highlights the importance of effective data protection laws in Nigeria's legal system by shining the spotlight on the violations which have resulted from a lack of same. These include unsolicited messages to customers, surveillance of citizens by law enforcement agencies, identity theft amongst others. The negative impact of ineffective data protection laws in today's world can have adverse life altering effects on individuals.

Irrespective of the lack of an established right to data protection in Nigeria, this research paper has confirmed that personal data is protected under Nigeria's current existing laws however the protection afforded under these laws are insufficient because of the new developments which have arisen from technological advancements. Most of these laws lack the basic rules required for processing of personal data. The Regulation of the NITDA embodies what a data protection legislation should be its legality is however questionable as a result of the arguments of ultra vires raised by legal practitioners who believe that only the federal legislative body has the power to make such a general data protection law. Notwithstanding the arguments of ultra vires and the pronouncement of a judicial decision affirming same, the Regulation has provided rudimentary personal data protection in Nigeria even though its effects are still minimal. It is however important that a data protection legislation whose legality is not in doubt be enacted to address all of the loopholes identified and foster a robust data protection regime which will ensure security of personal information and the consequential fostering of competitiveness of Nigerian businesses in international trade.[232]

[232] Nigeria Data Protection Regulation 2019: A Safety Net for Personal Information or Just Band-Aid? Templars, available at https://www.templars-law.com/wp-content/uploads/2019/03/Templars-Thought-

TABLE OF ABBREVIATIONS

APC- All Progressives' Congress

CJEU- Court of Justice of the European Union

CRA- Credit Reporting Act

DPB- Data Protection Bill

ECOWAS- Economic Community of West African States

EU- European Union

FHC- Federal High Court

FOI- Freedom of Information Act

GDPR- General Data Protection Regulation

INEC- Independent National Electoral Commission

JAMB- Joint Admissions and Matriculation Board

NCA- Nigerian Communications Act

NCC- Nigerian Communications Commission

NDLEA- National Drug Law Enforcement Agency

NIMC- National Identification Management Commission

NIS- Nigerian Immigration Service

NITDA- National Information Technology Development Agency

ONSA- Office of the National Security Adviser

TFEU- Treaty on the Functioning of the European Union

UNESCO- United Nations Educational, Scientific and Cultural Organisation

---

Leadership_NIGERIA-DATA-PROTECTION-REGULATION-2019_-A-SAFETY-NET-FOR-PERSONAL-INFORMATION-OR-JUST-BAND_AID.pdf accessed on 12th March, 2020.

REFERENCES

TREATIES

1. African Union Convention on Cyber Security and Personal Data Protection, Malabo 27/06/2014.
2. Charter of Fundamental Rights of the European Union, Nice 07/12/200, e.i.f. 1/12/2009.
3. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg 28/1/1981, e.i.f. 1/10/1985.
4. Data Protection Directive 95/46/EC, 24/10/ 1995, e.i.f. 13/12/1995.
5. General Data Protection Regulation (EU) 2016/679, 24/04/2016, e.i.f. 25/05/2018.
6. International Covenant on Civil and Political Rights, New York 19/12/1966, e.i.f. 23/03/1976.
7. Supplementary Act on Personal Data Protection within ECOWAS, Abuja 16/02/2010.

NATIONAL LEGISLATION

8. Child Rights Act, e.i.f. 31.07.2003.
9. Constitution of the Federal Republic of Nigeria, e.i.f. 29/05/1999.
10. Credit Reporting Act, e.i.f. 30/05/2017.
11. Consumer Code of Practice Regulations, e.i.f. 01/08/2007.
12. Cybercrimes (Prohibition, Prevention, Etc) Act, e.i.f. 05/05/2015.
13. Data Protection Act of Ghana, e.i.f. 10/05/2012.
14. Freedom of Information Act, e.i.f. 28/05/2011.
15. General Code of Practice, e.i.f. 01/08/2007.
16. National Health Act, e.i.f. 31/10/2014.
17. National Information Technology Development Agency Act, e.i.f 05/10/2007.
18. Protection of Personal Information Act of South Africa, e.i.f. 19/11/2013.

SUBSIDIARY LEGISLATION

19. Nigerian Communications Commission, Guidelines for the Provision of Internet Service, 2006
20. Nigeria Data Protection Regulation, 25/01/2019.

CASE LAW

COURT OF JUSTICE OF THE EUROPEAN UNION

21. *Bodil Lindqvist v Åklagarkammaren i Jönköping*; C-101/01, 06/09/2003.
22. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*; C-293/12 and C-594/12, 10/06/2014.
23. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*; C-131/12, 13/05/2014.
24. *Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn;* C-162/97, 19/11/1998.
25. *Maximillian Schrems v Data Protection Commissioner*; C-362/14, 06/10/2015.
26. *Music Producers of Spain (Promusicae) v Telefónica de España SAU*; C-275/06, 29/01/2008.
27. *Patrick Breyer v Bundesrepublik Deutschland*; C-582/14, 19/10/2016.
28. *Peter Nowak v Data Protection Commissioner*; C-434/16, 20/12/2017.
29. *Sergejs Buivids*; C–345/17, 14/02/2019.
30. *Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others*; C-201/14, 01/10/2015.
31. *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Watson*; C-203/15, 21/12/2016.
32. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*; C-73/07, 16/12/2008.
33. *Volker und Markus Schecke GbR*; C-92/09, 09/11/2010.
34. *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M and S*; C-141/12 and C-372/12, 17/07/2014.

NIGERIAN COURTS

35. *Abacha v Fawehinmi*; (2001) 51 WRN 29.
36. *Chukwuma & Others v. Commissioner of Police* (2005) 8 NWLR (Pt. 927) 278.
37. *Godfrey Eneye v MTN Nigeria Communication Limited*; FHC/ABJ/CS/431/2012 (Unreported case).
38. *MTN Nigeria Communications Limited v Godfrey Enene;* CA/A/689/2013.
39. *Barrister Ezugwu Emmanuel Anene v Airtel Nigeria Ltd.*; FCT/HC/CV/545/2015 (Unreported case).

BOOKS

40. Alsenoy B.V. Data Protection Law in the EU: Roles, Responsibilities and Liability, United Kingdom: Intersentia Ltd 2019.
41. Blume P. et al, Nordic Data Protection Law, DJOF Publishing Copenhagen, 2001.
42. Brkan M. and Psychogiopoulou E. (eds.), Courts, Privacy and Data Protection, United Kingdom: Edward Elgar Publishing, 2017.
43. Bygrave L.A. Data Privacy Law: An International Perspective, United Kingdom: Oxford University Press, 2014.
44. Carey P. Data Protection; A Practical Guide to UK and EU Law, 5th Ed., United States of America: Oxford University Press, 2018.
45. European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2018 ed., Luxembourg: Publications Office of the European Union, 2018.
46. IT Governance Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, 2nd Ed. United Kingdom, IT Governance Publishing, 2017.
47. Kelleher D. and Murray K. EU Data Protection Law, United Kingdom, Bloomsbury Publishing Plc. 2018.
48. Nicolaidou Irene and Georgiades Constantinos. The GDPR: New Horizons, EU Internet Law, Synodinou Tatiana-Eleni, Jougleux Philippe, Markou Christiana and Prastitou Thalia (eds.), Switzerland: Springer International Publishing AG, 2017.
49. Nwankwo I.S. African Data Privacy Laws, Law, Governance and Technology Series 33, A.B. Makulilo (ed.), Switzerland: Springer International Publishing AG 2016.

ONLINE ARTICLES

50. Adanikin, Olugbenga. *2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, International Centre for Investigative Reporting* published 01/02/2019 available at https://www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/.
51. Adeniyi, Ademola Samuel. *The Need for a Data Protection Law in Nigeria*, Communications and IT Law published 18/07/2012, available at https://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/.

52. Alao, Adavize. *A Review of Data Protection Bill 2019 HB02: Three Ways It Affects Nigerians*, Legalnaija Blawg, published 10/06/2019, available at https://www.legalnaija.com/2019/06/a-review-of-data-protection-bill-2019.html.
53. Clark, Roger. *Introduction to Dataveillance and Information Privacy*, Definition of Terms, available at www.rogerclarke.com/DV/Intro.html.
54. Daniel, Jeremy. *Top African data breaches, security stories show enterprises under stress*, CIO, published on 7/01/2020, available at https://www.cio.com/article/3512957/top-african-data-breaches-security-stories-show-enterprises-under-stress.html.
55. Ekwealor, Victor. *Nigeria's president refused to sign its digital rights bill, what happens now?* published March 27, 2019, Techpoint.africa, available at https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/.
56. Greenwald, Glenn. *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 7/06/2013, available at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
57. Hoofnagle Chris Jay, Sloot Bart van der and Borgesius Frederick. *The European Union General Data Protection Regulation: what it is and what it means*, (2019), Information & Communications Technology Law, 28:1, 65-98, available at https://doi.org/10.1080/13600834.2019.1573501.
58. Hunton, Andrews. Nigeria Issues New Data Protection Regulation, Privacy and Information Security Blog, 05/04/2019 available at https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/.
59. Izuogu, Chukwuyere Ebere Izuogu. *Data Protection and other Implications in the ongoing Sim Card Registration Process*, published on 2nd May, 2010, available at https://ssrn.com/abstract=1597665.
60. Kazeem, Yomi. *Nigeria is investigating a Swedish call blocking app for privacy breaches but exposes holes in its own laws*, published 24/09/2019, Quartz Africa, available at https://qz.com/africa/1714872/nigeria-investigates-truecaller-amid-lagging-data-protection-laws/.
61. Nwankwo, Iheanyi. *Nigeria's Data Privacy First Responders, ICT and Law in Nigeria*, 4/04/2018, available at https://iheanyisam.wordpress.com/2018/04/04/nigerias-data-privacy-first-responders/.

62. Oduwole, Olayinka. *New NCC Directive Will Push Telcos to Violate Nigeria Data Protection Regulation*, Tekedia, published 18/10/2019, available at https://www.tekedia.com/new-ncc-directive-will-push-telcos-to-violate-nigeria-data-protection-regulation/.
63. Okike, Samuel. *Nigerian airline company, Aero Contractors website hacked by allegedly ISIS-tied group*, Techpoint.africa, published on 14/08/2019, available at https://techpoint.africa/2019/08/14/nigerian-airline-company-aero-contractors-website-hacked-by-alleged-isis-tied-group/.
64. Okojie, Yetunde. *Information is the New Oil in Nigeria*, Mondaq, Privacy and Data Protection, published 20/07/2017 available at https://www.mondaq.com/nigeria/data-protection/617422/information-is-the-new-oil-in-nigeria.
65. Ololuo, Francis. *Data Privacy and Protection under the Nigerian Law* published on 19/02/2020, available at https://www.mondaq.com/Nigeria/Privacy/895320/Data-Privacy-And-Protection-Under-The-Nigerian-Law#_ftn1.
66. Salami, Emmanuel. *The Nigerian Data Protection Regulation 2019: Overview, Effects and Limits*, datenschutz-notizen published on 2/04/2019, available at https://www.datenschutz-notizen.de/the-nigerian-data-protection-regulation-2019-overview-effects-and-limits-3522349/.
67. Scaruffi, Piero. *Big Data: History, Trends and Future*, published in 2016 available at http://www.scaruffi.com/singular/bigdata.html.
68. Usman, Evelyn and Nwanekwu, Lucky. *Hacking into Nigerian banks very easy, says medical doctor turned cyber- criminal*, Vanguard, published on 20/05/2018, available at https://www.vanguardngr.com/2018/05/993772/.
69. Waqas. *Nigerian National Assembly Hacked, Huge Database Leaked by @LolSec, HackRead*, published on 23/10/2012, available at https://www.hackread.com/nigerian-national-assembly-hacked-huge-database-leaked-by-lolsec/.

NEWSPAPER ARTICLES

70. NCC Confirms FG Monitoring of Phone Calls in Nigeria, March 7, 2018, Technology Mirror, available at https://technologymirror.com.ng/ncc-confirms-fg-monitoring-of-phone-calls-in-nigeria/.
71. Nigerian chief justice's suspension raises international concerns, January 26, 2019, BBC News, available at https://www.bbc.com/news/world-africa-47015698.

72. Cyberattacks, Data Breaches top concerns of IT Experts, Punch Nigeria, published April 22, 2019, available at https://punchng.com/cyberattacks-data-breaches-top-concerns-of-it-experts/.

JOURNAL ARTICLES

73. Akindele, Roland. Data Protection in Nigeria: Addressing the multifarious challenges of a deficient legal system- 26 Journal of International Technology and Information Management 2017(4).
74. Greenleaf, Graham. Nigeria Regulates Data Privacy: African and Global Significance, 158 Privacy Laws & Business International Report 23, (2019) University of New South Wales Law Research Series 66.
75. Gregory, Voss. European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting, The Business Lawyer; Vol. 72, Winter 2016–2017.
76. Salau, Aaron. Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission: Regulation without Predictability- Bottis M., Alexandropoulou E. (eds.), 7th International Conference on Information Law and Ethics, Broadening the Horizons of Information Law and Ethics. A Time for Inclusion, 22nd/23rd February, 2016, Greece: The University of Macedonia Press, 2017.
77. Solove, Daniel. Conceptualising Privacy, California Law Review 2002, Vol. 90, p 1087-1155.

OTHER SOURCES

78. African Union, List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.
79. Black's Law Dictionary, 7th Ed. United States of America, West Publishing Co. 1999.
80. Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, 23/04/2014.
81. Education and Literacy, UNESCO Institute for Statistics, available at http://uis.unesco.org/en/country/ng.

82. European Commission, Safeguarding Privacy in a Connected World- A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, COM (2012) 9 final, 25/01/2012.
83. Industry Statistics, March 16, 2020, Nigerian Communications Commission, available at https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables.
84. Izuogu C.E. Personal Data Protection in Nigeria, Report of World Wide Web Foundation, March 2018.
85. Joint Admissions and Matriculation Board, Correction of Data: Correction of Names, available at https://www.jamb.org.ng/changeName.htm.
86. Nigeria Data Protection Regulation 2019: A Safety Net for Personal Information or Just Band-Aid? Templars, available at https://www.templars-law.com/wp-content/uploads/2019/03/Templars-Thought-Leadership_NIGERIA-DATA-PROTECTION-REGULATION-2019_-A-SAFETY-NET-FOR-PERSONAL-INFORMATION-OR-JUST-BAND_AID.pdf.
87. Nigeria Immigration Service, Passport Application: Correction of error(s), available at https://immigration.gov.ng/standard-passport/.
88. Opinion 1/15, The European Court of Justice on the EU-Canada Passenger Name Record Agreement of 26 July 2017.
89. Paradigm Initiative and Privacy International, The Right to Privacy in the Federal Republic of Nigeria: Stakeholder Report, Universal Periodic Review, 31st Session-Nigeria, March 2018.
90. Recitals to the GDPR.
91. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015), noting at paragraph 55: Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."
92. U.S. Department of State, Chapter 2. Country Reports: Africa Overview, 2015, available at https://2009-2017.state.gov/j/ct/rls/crt/2015/257514.htm.

93. Worldometer, Nigeria Population (Live) available at https://www.worldometers.info/world-population/nigeria-population/.

Non-exclusive licence to reproduce thesis and make thesis public

I, Adelayo Adenike Banjo,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, The Actualisation of Personal Data Protection n Nigerian Law: An Analysis of Personal Data Protection in the Nigerian and European Union Legal Systems,

   supervised by supervised by Palooma Kroot Tupay, dr. iur.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Adelayo Adenike Banjo

29/04/2020