International Journal of Library and Information Technology (IJLIT), Vol.2 No.1, March 2022. Pg.16 - 30

A COMPARATIVE STUDY OF DATA PROTECTION LAWS & POLICIES: A CASE STUDY OF NIGERIA

GAGA, THOMAS ALI
Department of Computer Science
Bingham University, Karu, Nasarawa State.

&

ORAGWU, OBUZOR KENNETH
Department of Computer Science
Bingham University, Karu, Nasarawa State.

ASTRACT
The paper evaluates the laws which regulate and govern data protection in Nigeria and contrasts them with that of a selected African Nation (South Africa). It then makes recommendations for improvement of data protection practices in Nigeria as policy gaps are identified and analysed (referencing global best practices for guidance), thereby positively impacting the data protection regime of the Nation. The term Data Protection is used when referring to the process of safeguarding vital information from corruption or compromise, and from theft or loss. As the amount of data being created has continued to grow, the need for the protection of same has continued to increase. Consequently, a significant part of any data protection strategy has to be based on ensuring that data can be restored quickly after corruption or loss. Protecting data from compromise and ensuring data privacy are other key components of data protection; however, where there are no laws to enforce these in the event of breach, the essence of those rights is lost. In order to uphold the sanctity of these rights, many nations of the world have put in place regulations and other mechanisms to guarantee them. The Data protection regulation for Nigeria is here analysed and recommendations are given to strengthen the regulatory policy document.

1.0 INTRODUCTION

In today's digital economy, data is of strategic importance and it is considered as the most valuable asset of the digital economy. With social, economic and governmental activities increasingly being carried out online, the flow of personal data is expanding exponentially, raising issues on data privacy and usage. Current technologies such as Cloud Services, Big Data and the Internet of Things, as well as other technological innovations and increased connectivity through 4G and 5G networks have delivered enormous benefits, but they also make it more urgent and imperative to address the various concerns over data privacy. The challenge for data protection regimes is in managing the risks and addressing the concerns that go with data flow without restricting or eliminating the potential benefits of the movement of data. The role of governments in developing policies for protecting electronic data is of paramount importance. It must be done to ensure trust and confidence electronic transactions. This requires collaboration among the various stakeholders (data subjects, data controllers and data administrators among others). Cross border e-commerce presents both developed and developing economies with amazing opportunities, but the countries that want to securely participate in the digital economy must consider the need for legal and regulatory frameworks to protect the personal data that they collect. According to a publication by The Economist in May 2017 (www.economist.com/weeklyedition/2017-05-06), Data is considered to be the 'oil' of the digital era. It stated that the world's most valuable companies such as Amazon, Uber, Google, Tesla etc. have become those whose subscribers are routinely required to provide their data to facilitate access. Thus the internet and smart phones have contributed significantly in making data more valuable, available and abundant. Virtually every human activity generates a digital trace nowadays. The more devices are connected to the internet the more data that can

be generated. The data industry has demonstrated such exponential growth that certain multinationals now position themselves as data purveyors and merchants.

Today's social media and internet users are typically required to provide personal data and sensitive information to facilitate access and use of these platforms. Almost all transactions conducted online require the release of some form of personal data. Although, social media users are often advised of data privacy terms (see Figure 1), they do not necessarily preclude the use or sharing of such personal data in specified circumstances. This introduces the risk of having personal sensitive information being potentially shared with unauthorized party or sold to high level security agents or blue-chip companies through direct marketing to enable surveillance and data gathering.

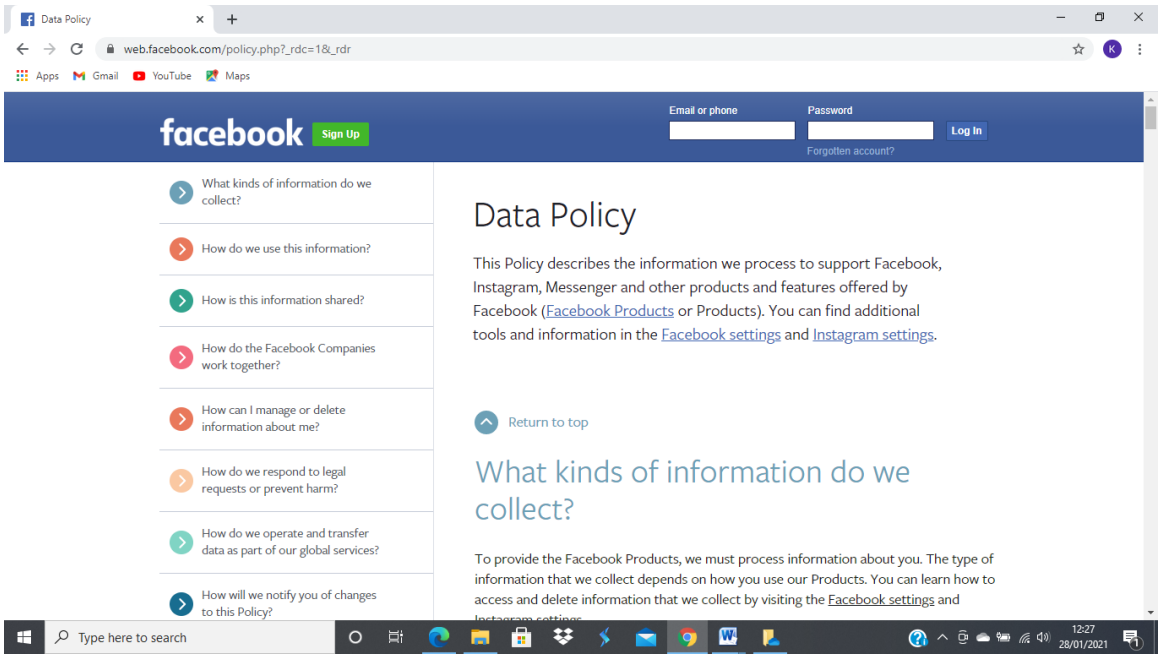

Figure 1

In 2008, there was widespread information regarding how top brands like Facebook experienced data breaches that exposed several millions of personal records to abuse by criminals. There appears to be a lucrative market for data, and hackers tend to sell data they steal to scammers.

These worrying developments have generated widespread concerns on how to improve security policies over the personal data that are captured, albeit in the knowledge that data protection laws never fully offer complete protection against malicious attacks and users are best advised to understand the basics of data privacy and how to protect themselves. For example, Google and Facebook have experienced breaches of the private data of users over the years and, on each occasion, these supposedly trusted companies failed to report/disclose the breaches (when they occurred) to enable customers take steps to protect themselves. The failure by these companies to disclose data privacy violations when they should have, underscores the importance of users and other stakeholders taking personal data security as a personal responsibility, but the question is, to what extent can this be achieved? And what legislations can help facilitate their achievement? Are those legislations in place and are they being enforced, following proper public awareness?

Data Protection has always been an important subject but in recent times the concept has become especially relevant, particularly in today's economy that in almost every transaction has evolved into one that is digitally driven. According to Crocetti & Peterson (2021), the term is used when referring to the process of safeguarding vital information from corruption or compromise, and from theft or loss. More so, as the amount of data being created has continued to grow, the need for the protection of same has continued to increase. Protecting data from compromise and ensuring data privacy are key components

of data protection (Hefner, 2020); however, where there are no laws to enforce these in the event of breach, the essence of those rights are lost. In order to uphold the sanctity of these rights, many nations of the world have put in place regulations, policies and other mechanisms to guarantee the safety of these data. In this regard, Nigeria has developed the Nigeria Data Protection Regulation (NDPR), which is the regulatory framework through one of the Federal Government Agency - National Information and Technology Development Agency (NITDA).

This paper will therefore review the NDPR and carry out a comparative study between the NDPR and the South Africa Data protection laws and regulations.

2.0 LITERATURE REVIEW

2.1 RATIONALE FOR DATA PROTECTION LAWS IN NIGERIA

An average Nigerian is used to the tedious task of registering for digital services. The request that Nigerians link their National Identification Number (NIN) to their Phone SIMs is a good and recent example of this. Nigerians have had to present themselves to Banks and Institutions concerned with these processes to get themselves an Identification number that will facilitate utilising of other e-services. The amount of information and data that are collected is rich – for example, the banks and mobile service providers know customers' names, date of birth, address, how much they earn and even what they spend their money on, etc. We routinely save bank card details on company websites, and a lot of people reuse the same password across multiple sites. Consumers are interested in getting services, but most times consider giving out data as a hurdle to overcome - that's fair enough. However, some data collectors don't always treat this data with the right amount of care. The conversation around data protection is yet to be fully discussed.

Cyber incidents can be a permanent loss of resources such as data, money or servers. It can be malicious, like hackers targeting one of the largest credit agencies in the world to steal millions of personal information, or an honest mistake, like sending sensitive medical information to the wrong person.

However, combating data incidents requires knowledge of what data has been stolen, and by whom. It is with this information that businesses and customers can react to protect themselves. Therefore, there is a need to forcing companies to report data breaches. is a critical missing piece in the 2019 National Information Technology Development Agency's (NITDA), Nigeria Data Protection Regulation (NDPR). The regulation undermines our national cyber security strategy. It means that without the public information on breaches both customers and other companies cannot react.

If a hacker steals data from a bank, they can use that data to attack the customer directly. But when companies are made to report the lost data, customers can protect themselves by simply changing passwords and warning relevant people of any potential fraud or impersonation. Although organisations feel reporting incidents can damage their reputations, reporting incidents act as a deterrent for poor cyber practices. Without reporting data breaches, Nigerian companies cannot learn from the mistakes of their peers. This has led to a divide in cyber preparedness between sectors of the economy. While the maritime, TELCO and consumer goods sectors struggle with phishing attacks, the financial services industry has made better progress. If breaches are reported, then NITDA can analyse them, discover themes and publically share findings.

In United Kingdom the General Data Protection Regulation states that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The General Data Protection Regulation (EU) 2016/679 ('GDPR') and the 2018 reform of the GDPR are regulations under EU law concerning data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also deals with the export of personal data outside of the EU and EEA. In Nigeria, while there are several legislations containing ancillary provisions which seek to protect data privacy, the most comprehensive statutory instrument for this

purpose is a subsidiary legislation made pursuant to the National Information Technology Development Agency Act, 2007 ('NITDA Act').

2.2 FRAMEWORKS GOVERNING DATA PROTECTION IN NIGERIA PRIOR TO NIGERIA DATA PROTECTION REGULATION (NDPR).

2.2.1 The Constitution

Section 37 of Nigeria's 1999 constitution forms the foundation of data privacy rights and protection in Nigeria. Section 37 guarantees and protects the right of Nigerians to privacy with respect to their homes, correspondence, telephone conversations and telegraphic communications. It deems Privacy in this respect a fundamental right which is enforceable in a court of law when breached. Prior to the NDPR, most cases of data privacy breaches were enforced under this section.

2.2.2 The NCC Consumer Code of Practice Regulation 2007

Part six of the Nigerian Communications Commission (NCC) regulation, generally deals with the protection of consumers' data in the telecoms sector. Regulation 35 of this code requires all licensees to take reasonable steps to protect the information of their customers against improper or accidental disclosures. It prescribes that licensees shall not transfer this information to a third party except as permitted by the consumer or commission or by other applicable laws or regulation. Data collected by the licensee must be such that is reasonably required for business purposes and not to be kept for longer than necessary. This law extends not only to electronic or written data but also to verbal data recorded by the licensee. It also provides for notification of the consumer of the use and disclosure of data obtained from them.

2.2.3 NCC Registration of Telephone Subscribers Regulation 2011

Regulation 9 and 10 of the NCC Registration of Telephone Subscribers Regulation 2011, deals with the data privacy and protection of subscribers. It provides for confidentiality of personal information of subscribers stored in the central database or a licensee's database. It also provides that this information shall not be released to a third party nor transferred outside Nigeria without the prior written consent of the subscriber and commission, respectively. This regulation also regards the information stored in the Central Database as the property of the federal government of Nigeria.

2.2.4 The Freedom of Information Act 2011

Section 14 of the Freedom of Information Act protects personal data. It restricts the disclosure of information which contains personal information by public institutions except where the involved data subject consents to its disclosure or where the information is publicly available. The Act also provides that a public institution may deny the application for disclosure of information that is deemed privileged by law (e.g. Attorney-client privilege, doctor-client privilege).

2.2.5 The Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes (Prohibition, Prevention etc.) Act, Nigeria's foremost law on cybercrimes criminalizes data privacy breaches. Generally, this Act prohibits, prevents and punishes cybercrimes in Nigeria. It prescribes that anyone or service provider in possession of any person's personal data shall take appropriate measures to safeguard such data.

2.2.6 The Child Rights Act 2003

The Child Rights Act protects the privacy rights of children. The Act protects and guarantees the right of every child to privacy, family life, home, correspondence, telephone conversation and telegraphic communications subject to the supervision or control of the parents or guardians.

2.2.7 The Consumer Protection Framework 2016

The Central Bank of Nigeria's Consumer Protection Framework prohibits financial institutions from disclosing the personal information of their customers. It also ensures that these financial institutions take appropriate measures to safeguard customers' data and necessitates the prior written consent of their customers before sharing these data with anyone.

2.2.8 The National Identity Management Commission (NIMC) Act 2007

Section 26 of this Act requires the approval of the Commission before a corporate body or anybody can have access to data stored in their database. The Act also empowers the NIMC to collect, collate and process data of Nigerian citizens and residents.

2.2.9 The National Health Act (NHA) 2014

The NHA which regulates health users and healthcare personnel restricts the disclosure of the personal information of users of health services in their records. It also ensures that healthcare providers take the necessary steps to safeguard such data.

2.2.10 The Federal Competition and Consumer Protection Act 2019

This Act stipulates that the Federal Competition and Consumer Commission shall ensure that business secrets of all parties concerned in investigations conducted by it are adequately protected during all stages of the investigation or inquiry.

2.2.11 The Nigeria Data Protection Regulation (NDPR) 2019

The NDPR is the major law specifically aimed at addressing data privacy and protection in Nigeria. The regulation was issued by the National Information Technology Development Agency (NITDA) in 2019 to comprehensively regulate and control the use of data in Nigeria. Though a subsidiary regulation and a copycat of the EU's GDPR, the NDPR regulation touches on principles of data processing, the requirement of Data Compliance Officers, requirement of data subject's consent for collecting and processing data, requirements for international transfers of data and rights of data subjects, inter alia. It also prescribes penalties for non-compliance with the regulation. Aside from the NDPR, there are other laws prior to that that touched on Data Privacy and Protection in Nigeria.

3.0 METHODOLOGY

The research work used in this study is called Qualitative research; it involves the process of collecting, analysing, and interpreting non-numerical data. Qualitative research can be used to understand how an individual subjectively perceives and gives meaning to their social reality (Denzin and Lincoln, 1994).
There are different types of qualitative research methods including diary accounts, in-depth interviews, documents, focus groups, case study research, and ethnography. The results of qualitative methods provide deep understandings of how people perceive their social realities, and in consequence, how they act within the social world. Qualitative research is endlessly creative and interpretive. Qualitative interpretations are constructed, and various techniques can be used to make sense of the data, such as content analysis, grounded theory (Glaser & Strauss, 1967), thematic analysis (Braun & Clarke, 2006) or discourse analysis.

The Qualitative approach, providing contextual backgrounds for the differing types of regulations in the selected countries was adopted for the research. The data used in the study were gathered secondarily, and a qualitative analysis was carried out to making sense of the various legislations. The study also examined and highlighted the gaps and areas that should be considered for improvement.

4.0 ANALYSIS

4.1 Data protection and regulations of two countries were used for analysis in this research work; the countries are Nigeria and South Africa. The table below highlighted the analyse the similarities and differences between the NDPR and the POPIA.

4.2 TABULAR COMPARISM OF SIMILARITIES AND DIFFERENCES IN THE DATA PROTECTION REGULATIONS AND PRACTICES OF NIGERIA (NDPR) AND SOUTH AFRICA (POPIA)

S/N	PRACTICE/ REGULATION	NDPR	POPIA
1	**Pseudonymisation**	The NDPR does not define or require pseudonymised data.	POPIA requires that "reasonable technical and organisational measures" be taken to prevent the loss of or unauthorised access to personal information.
2.	**Data processing records**	The NDPR does not impose the obligation to maintain a record of processing activities on either the controller or the processor.	Data controllers and data processors have an obligation to maintain a record of processing activities under their responsibility.
3.	**Timeline for Compliance**	3 months (April 1, 2019 deadline)	1 year (July 1, 2021 deadline)
4.	**Data protection impact assessment (DPIA)**	The NDPR does not require the data controller to consult the supervisory authority prior to any processing that would result in a high risk, but the NDPR requires controllers to conduct a detailed audit which must include an assessment of the impact of technologies on privacy and security policies.	A Personal Information Impact Assessment ("PIIA") is a process to help businesses in South Africa identify and minimise the data protection risks from processing personal information. This process is mandatory in terms of POPIA.
5.	**Data Protection Officer (DPO) appointment**	The NDPR provides for an obligation to appoint a DPO. In addition, the regulation stipulates that the contact details of the DPO must be communicated to the data subjects.	POPIA also provides an obligation to appoint an Information Officer. In addition, POPIA stipulates that the contact details ofthe Information Officer must be communicated to the data subjects.
6.	**Tasks of a Data Protection Officer (DPO)**	The NDPR does not address the tasks nor the role of a DPO within an organisation.	POPIA defines the tasks and role of an Information Officer within an organization.
7.	**Guidelines for appointing a Data Protection Officer**	The NDPR requires every controller to appoint a DPO, but doesn't specify any requirement for processors to appoint a DPO.	Under POPIA, there are guidelines for the registration and appointment of Information Officers, and inputs were sought for and received from the public as to what the procedure and requirements should be.

8.	**Data security and data breaches**	Under the NDPR there is no requirement for data controllers to notify the supervisory authority of a breach.	Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established. The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the data subject in a prescribed manner.
9.	**Right to erasure**	Under the NDPR, the data subject shall have the right to request the controller to delete personal data without delay.	Although POPIA does not explicitly grant a 'right to be forgotten', section 24 allows data subjects to request responsible parties to correct or delete personal information or records.

10.	**Right to be informed**	The NDPR states that data subjects must be provided with information about the collection or processing of their personal data.	Transparency is a key requirement under POPIA. Individuals or "data subjects" own their personal information and have the right to be informed about the collection and use of their personal information.
11.	**Right to object**	Data subjects have the right to object to the processing of their personal data for marketing and other purposes. Prior to the processing of personal data, the data subject must be informed of their right to object to the processing of their data as well as of the right to the restriction of processing concerning the data subject.	Under POPIA, everyone has the right to object to having their personal information processed. They have the right to withdraw their consent, or object if they can show legitimate grounds for their objection.
12.	**Right to access**	The NDPR recognises that data subjects have the right to access their personal data that is processed by a data controller.	Data subjects have the right to request, free of charge, confirmation of whether or not a responsible party holds personal information about them. Data subjects also have the right to request the record, or a description of the personal information being held by the responsible party, as well as information concerning the identity of all third parties who have had access to the personal information. This may be subject to a prescribed fee and the responsible party may require the payment of a deposit.
13.	**Right not to be subject to automated decision-making**	Section 3.1(3)(l) of the NDPR states that the controller shall inform the data subject about the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged	Under POPIA, a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the

		consequences of such processing for the data subject.	automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.
14.	**Right to data portability**	The NDPR provides individuals with the right to data portability. The NDPR defines data portability as the ability for data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format. In addition, when exercising the right to data portability, the data subject has the right to have personal data transmitted directly from one controller to another, where technically feasible, provided that this right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.	There is no right to data portability under POPIA.
15.	**Monetary penalties**	The NDPR outlines that depending on the violation, a penalty may be up to either: 2% of annual gross revenue of the preceding year or payment of the sum of NGN 10 million (approx. €25,000), whichever is greater where the data controller is dealing with more than 10,000 data subjects; or payment of a fine of 1% of the annual gross revenue of the preceding year or payment of the sum of NGN 2 million (approx. €5,000) whichever is greater where the data controller is dealing with fewer than 10,000 data subjects.	For the more serious offences the maximum penalties are a R10 million fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. For the less serious offences, for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.
16.	**Supervisory authorities**	Under the NDPR, the relevant supervisory authorities are	Responsible parties under POPIA must

		NITDA or any other statutory body or establishment having mandate to deal solely or partly with matters relating to personal data. In particular, the Administrative Redress Panel inaugurated by NITDA under the NDPR is granted the investigatory powers outlined above. In addition, under the NDPR, the HAGF is given mandate to supervise any transfer of personal data which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organisation.	obtain authorisation from the Information Regulator in order to: process: information on criminal behaviour or on unlawful/objectionable conduct on behalf of third parties information for the purpose of credit reporting transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information. The above provisions may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.
17.	**Civil remedies for individuals, including other remedies**	Under the NDPR, the data subject has the right to lodge a complaint with NITDA.	Under POPIA, the data subject has the right to lodge a complaint with the Information Regulator.
18.	**Accountability**	Accountability relates to accepting responsibility by taking ownership -to ensure that the organisation processes personal information in the manner intended by the regulator. The NDPR recognises accountability as a governing principle of data processing. In particular, Section 2.1(3) states 'anyone who is entrusted with personal data of a data subject or whois in possession of personal data of a data subject shall be accountable for his acts and omissions in respect of data processing.' This provision does not refer specifically to data	In terms of POPIA, this responsibility has been put squarely on the shoulders of the person whom the Act refers to as the "Responsible Party". The Act defines "Responsible Party" as follows: "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".

		controllers. However, as it refers to a person entrusted with personal data, this provision may cover data controllers.	
19.	**Data Transfers**	The NDPR allows personal data to be transferred to a foreign country, territory or one or more specified sectors within that foreign country, or an international organisation where NITDA has decided that the foreign country or international organisation ensures an adequate level of protection. The NDPR provides a list of criteria that NITDA or the Honourable Attorney General of the Federation ('HAGF') will consider in determining the adequacy of a third country or international organisation	POPIA allows personal data to be transferred to a third country or international organisation that has a similar level of protection to it.
20.	**Children and Data Protection**	The NDPR does not grant special protection to children's personal data, nor does it specify whether the consent of a parent or guardian is needed when processing children's data. Though the NDPR mandates that data controllers must take appropriate measures to provide information relating to processing that can be easily understood by a child, the NDPR, does not provide requirements for data controllers to make reasonable efforts to verify that consent is given by a parent or guardian when processing children's data.	In POPIA, personal information may only be processed if a competent person where the data subject is a child consents to the processing. So the processing personal information of children, except where necessary or required by law, is prohibited.
21.	**Territorial Scope**	The NDPR applies to all processing of personal data in respect of persons in Nigeria, or Nigerian citizens living abroad.	POPIA applies within South Africa only.
22.	**Controllers and Processors**	The NDPR provides that anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption	In POPIA, Data controllers must implement technical and organisational security measures. POPIA requires organisations to take "appropriate, reasonable technical and organisational measures" to prevent

		technologies, developing an organisational policy for handing personal data, protecting emailing systems,and providing continuous capacity building for staff.	"loss of, damage to or unauthorised destruction" and "unlawful access to or processing" when processing personal information.

4.3 SIMILARITIES OF THE NDPR AND POPIA.

Some common concepts in both NDPR and POPIA are as follows:

- That personal information belongs to the individual whose information is collected and/or provided.
- That organisations are entrusted with that information on a consensual basis.
- That the information must be used purely for the purpose it has been given.
- That the information must be protected and not put at risk of theft and abuse.

However there are unique and contrasting aspects of the Data Protection Regulations of these two countries, which shall be discussed in detail in the course of the study.

5.1 DISCUSSION

The Nigeria Data Protection Regulation (NDPR) stipulates requirements for data collection, processing and defines how the data should be held and the ability to be used by third-parties. The inclusion of penalties for various cyber related crimes is also a key milestone in deterring cyber criminals and ensuring compliance with the law. However, as laudable as this law appears, obstacles have been identified which if not addressed could make the regulation ineffective and of no value.

Putting policies and hefty penalties in place does not guarantee compliance or overall safety of the general public. Comprehensive security has to consider People, Process, Technology and Policy. Laws only take care of the policy bit. A lot still needs to be done for People (particularly awareness, understanding the contents of the laws and their rights), Process (putting the right infrastructure for reporting and prosecuting these crimes) and Technology (equipping the law enforcement with the right tools to identify and proactively detect non-compliance).

A major envisaged obstacle to the implementation of NDPR includes the low awareness of the regulation in the country. To address this, regulatory bodies will have to embark on nationwide awareness campaigns aimed at helping citizens understand the contents of these laws, process of identifying these crimes and how to report these to the police. Law enforcement training will also help equip police and prosecutors with the skills to identify cybercrime, obtain evidence and prosecute".

The absence of infrastructure for identification and implementation of the law is also an issue. To implement data protection requirements, organisations need to have capabilities (either in house or outsourced) for data protection assessment, reporting etc. These are skills that were previously not existent. There is still need to acquire tools to identify non-compliance, monitoring infrastructure, audits etc. To address this, regulators together with data processors and third parties need to invest in proper technologies and or processes for monitoring both compliance and non-compliance to these laws.

Furthermore, the biggest challenge consists in the lack of skills sets and knowledge in the area of Data Science, Analytics and Big Data to be able to ensure that an individual internet user's personal data is truly secure. The complex nature of the Internet and other enabling social media platforms is evolving at vast speeds and this then places an additional burden on not only NITDA to acquire personnel that have these requisite skills but also the judiciary and other enforcement agents that NITDA will need to work alongside in order to effectively enforce the NDPR in its true spirit.

The whole essence of NDPR and cyber security viz-a-viz protection is to ensure users of the World Wide Web and their data are treated in a manner that provides confidence to the consumer that their personal data information is not unduly exposed to third party data abuse or outright fraud. In the spirit of this the

NDPR provides guidelines, procedures and processes that should be adopted to ensure that the principles of a fair and neutral Internet are available to all citizens of Nigeria.

6.0 RECOMMENDATIONS

Based on the comparative analysis that was conducted, the following recommendations are here given for the NDPR update:

1. It is advised that NITDA recommends the adoption of pseudonyms in subsequent updates of the NDPR, since pseudonymisation or the use of artificial identifiers will protect data subjects and data controllers from public view while not excluding them from responsibility or lawsuits.
2. NITDA should impose an obligation to maintain a record of processing activities on either the controller or the processor (data administrator).
3. The deadline of three months which has since elapsed without much awareness of or conformity to the regulation by Nigerians organisations should be reviewed.
4. NDPR should clearly define the requirements for the appointment of a Data protection officer, as well as the tasks and roles of appointed Data Protection Officers (DPOs) within an organisation.
5. NDPR should require all data controllers to notify the supervisory authority (NITDA) of a data breach.
6. NDPR should give special protection to children's personal data by specifying that the consent of a parent or guardian should be required when processing children's data.

REFERENCES

1. The Economist: The World's Most Valuable Resource Is No Longer Oil, But Data, (2017).
2. De Hert, P., Papakonstantinou, V.: The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. Computer Law & Security Review. 28, 130–142 (2012).
3. The Race to GDPR: A Study of Companies in the United States & Europe. Ponemon Institute (2018).
4. Bélanger, F., Crossler, R.E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly. 35, 1017–1042 (2011).
5. Nicolaidou, I.L., Georgiades, C.: The GDPR: New Horizons. In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 3–18. Springer International Publishing, Cham (2017).
6. Mitrou, L.: The General Data Protection Regulation: A Law for the Digital Age? In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 19–57. Springer International Publishing, Cham (2017).
7. De Hert, P., Papakonstantinou, V.: The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? Computer Law & Security Review. 32, 179–194 (2016).
8. Kurtz, C., Semmann, M., Böhmann, T.: Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. In: AMCIS 2018 Proceedings (2018).
9. Petkov, P., Helfert, M.: Identifying Emerging Challenges for ICT industry in Ireland: Multiple Case Study Analysis of Data Privacy Breaches. In: AMCIS 2017 Proceedings (2017).
10. Karyda, M., Mitrou, L.: Data Breach Notification: Issues and Challenges for Security Management. In: MCIS 2016 Proceedings (2016).
11. Engels, B.: Data Portability and Online Platforms The Effects on Competition. In: BLED 2016 Proceedings. pp. 19–22 (2016).
12. Alboaie, L.: Towards a Smart Society through Personal Assistants Employing Executable Choreographies. In: ISD 2017 Proceedings (2017).
13. Fox, G., Tonge, C., Lynn, T., Mooney, J.: Communicating Compliance: Developing a GDPR Privacy Label. In: AMCIS 2018 Proceedings (2018).

14. Russell, K.D., O'Raghallaigh, P., O'Reilly, P., Hayes, J.: Digital Privacy GDPR: A Proposed Digital Transformation Framework. In: AMCIS 2018 Proceedings (2018).
15. El Kharbili, M.: Business Process Regulatory Compliance Management Solution Frameworks: A Comparative Evaluation. In: APCCM 2012 Proceedings. pp. 23–32 (2012).
16. Cleven, A., Winter, R.: Regulatory Compliance in Information Systems Research - Literature Analysis and Research Agenda. In: Enterprise, Business Process and Information Systems Modeling. pp. 174–186. Springer-Verlag, Berlin, Heidelberg (2009).
17. Abdullah, N.S., Indulska, M., Shazia, S.: A Study of Compliance Management in Information Systems Research. In: ECIS 2009 Proceedings. pp. 1–10 (2009).
18. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly. 28, 75–105 (2004).
19. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24, 45–77 (2007).
20. Bensoussan, A., Avignon, C., Bensoussan-Brulé, V., Forster, F., Torres, C.: RèglementEuropéen sur la Protection des Données: Textes, Commentaires et Orientations Pratiques. Bruylant, Brussels (2018).
21. Debet, A., Massot, J., Métallinos, N.: Informatique et libertés: la protection des données à caractère personnel en droit français et européen. Lextenso, Issy-les-Moulineaux (2015).
22. Voigt, P., Von Dem Bussche, A.: The EU general data protection regulation (GDPR): A Practical Guide. Springer International Publishing, Cham (2017).
23. Guadamuz, A.: Developing a Right to be Forgotten. In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 59–76. Springer International Publishing, Cham (2017).
24. European Data Protection Board: Guidelines On Consent Under Regulation 2016/679 (WP259, rev.01). EDPB (2018).
25. European Data Protection Board: Guidelines on Data Protection Officers (WP243 rev.01). EDPB (2017).
26. European Data Protection Board: Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01). EDPB (2018).
27. Iannopollo, E., Balaouras, S., Harrison, P.: The Five Milestones to GDPR Success. Forrester Research (2017).
28. Merlivat, S., Iannopollo, E., Parrish, M., Khatibloo, F., Oesterreich, M., Liu, S., Turley, C.: Digital Advertising under GDPR Hinges on Data Management. Forrester Research (2017).
29. Peyret, H., Cullen, A., McKinnon, C., Blissent, J., Iannopollo, E., Kramer, A., Lynch, D.: Enhance your Data Governance to Meet New Privacy Mandates. Forrester Research (2017).
30. Iannopollo, E., Balaouras, S., Pikulik, E., Dostie, P.: The State of GDPR Readiness. Forrester Research (2018).
31. Deutsche Telekom: Binding Interpretations: General Data Protection Regulation (GDPR). Deutsche Telekom (2016).
32. Nickerson, R.C., Varshney, U., Muntermann, J.: A Method for Taxonomy Development and Its Application in Information Systems. European Journal of Information Systems. 22, 336–359 (2013).
33. Sadiq, S., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., and Rosemann, M. (eds.) BPM 2007 Proceedings. pp. 149–164. Springer-Verlag, Berlin, Heidelberg (2007).
34. Zhang, M., Sarker, S., Sarker, S.: Drivers and Export Performance Impacts of IT Capability in 'Born-Global' Firms: a Cross-national Study. Information Systems Journal. 23, 419–443 (2013).
35. Grant, R.M.: The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation. California Management Review. 33, 114 (1991).
36. Baiyere, A., Salmela, H.: Towards a Unified View of Information System (IS) Capability. In: PACIS 2014 Proceedings (2014).
37. Bharadwaj, A.: A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. MIS Quarterly. 24, 169–196 (2000).
38.MTN Nigeria Communication Ltd v. Barr. Godfrey Nya Eneye, Appeal No: CA/A/689/2013 (Unreported).

39. Barr`. Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd, Suit No: FCT/HC/CV/545/2015 (Unreported).
40. Constitution of the Federal Republic of Nigeria 1999 (as amended).
41. Barr. Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd, Suit No: FCT/HC/CV/545/2015 (Unreported).
42. Joseph Cannataci, The Individual and Privacy Volume 1, (United Kingdom: Ashgate Publishing, 2015).