Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries

Mohammed Agbali, Abubakar A. Dahiru, G. Daniel Olufemi, Inuwa A. Kashifu, Olatunji Vincent

Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries

Mohammed Agbali, Abubakar A. Dahiru [0000-0001-9858-5796], Daniel Olufemi G., Inuwa A. Kashifu and Olatunji Vincent

A. National Information Technology Development Agency, 28, P/H Crescent, Area 11, Garki, Abuja, Nigeria
magbali@nitda.gov.ng; d.a.abubakar@rgu.ac.uk; odaniel@nitda.gov.ng;kinuwa@nitda.gov.ng; volatunji@nitda.gov.ng

Abstract. Advances in new technologies present challenges to general expectations relating to collection, usage and cross-border control and transfer of personal data in recent times. Data has become the critical component of the fourth industrial revolution in global economies involving governments, businesses, and individuals. This paper considers the recent introduction of Data Protection Regulation in Nigeria (NDPR), which can be adjudged to have novel compliance structures globally. Using a qualitative approach, and further enabled by the institutional theory as a framework the paper examines the implications of the NDPR requirements for Data Controllers and Processors in key sectors of the economy. Findings from the study shows that there are five key components of the NDPR that can compel, motivate or support organizations to make significant structural changes such as standardization of processes, practices and IT assets to show conformity and/or gain legitimacy. The study equally identified the factors that facilitate or inhibit the adoption and implementation of the conditions of the NDPR categorised in line with the three pillars of the institutional theory framework. These findings projects policy direction in enhancing the institutionalisation of NDPR measures across key sectors. It will also inform businesses on necessary cause of action and changes to ensure privacy and protection of personal data collected from data subjects.

Keywords: *Data Protection, Data Privacy, Regulation, Data Controllers, Data Processors, Institutional Theory, Framework, ICT, NDPR.*

1 Introduction

Globalisation and phenomenal growth of Internet and Web access are complicating the challenges of personal data privacy and protection around the world. Vulnerabilities due to data collection in both public and private sectors are at a potentially remarkable stage. For instance, governments collect and process personal information from population census, birth certificate, voters register, and drivers' license records. On the other

hand, private corporations such as telecommunications operators, fund managers, and commercial banks increasingly build capacities for compiling databases of customer information aided by unlimited capability of new technologies with ease of tracking and retrieval.

With globalization and rapid technological advancements, there is obviously increased capability for organizations or businesses to collect, analyse, store, transfer and interlink data for various purposes including direct marketing and personalized services [1]. In this regard, with identification technologies in the form of radio-frequency identification (RFID) and social media platforms such as Facebook, Instagram and other networks, data privacy and protection are currently being challenged [2].

In Europe and North America, developments in personal data processing technologies evolved with data privacy legislation and several other initiatives to improve the level of privacy protection. The first data privacy act by German Federal State of Hessen dated back to 1970 and was followed by the adoption of Swedish Data Protection act in 1973 [3]. Similarly, the United States government formulated the popular Fair Information Practices (FIPs) since 1973 [4]. The development of modern data protection laws started with the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data,1981 (aka Convention 108). The Convention enumerated the core principles of data processing which are still the basis of modern data protection laws today. The next major intervention is the European Union Data Protection Directive, 1995. Similarly, while issues around protection of citizen's telephone conversation, correspondence, telegraphic communications, etc. are covered under section 37 of the 1999 constitution of the Federal Republic of Nigeria [5], the National Information Technology Development Agency (NITDA), pursuant to Section 6(c) of the NITDA Act 2007, issued a Data Protection Guideline in 2013. However, upon the issuance of the EU General Data Protection Regulation (EUGDPR) in 2016, and other international developments on privacy protection, NITDA issued the Nigeria Data Protection Regulation (NDPR) [6] on 25th January 2019.

In Nigeria, Data Privacy and Protection regulation has been evolving since the introduction of the NDPR which is a subsidiary legislation. The NDPR aims to safeguard the rights of citizens and people living in Nigeria to data privacy and protection in order to foster the integrity of commerce and industry in the volatile data economy. It also aims at enhancing the secure exchange of data; improve business operating environment and create sustainable jobs [6]. The NDPR applies to public and private entities processing data of Nigerians.

In this paper, we examine the implications of data privacy and protection regulations in the context of a developing country – Nigeria, with particular attention to data intensive businesses. These businesses include financial service providers such as banks/fund managers, telecommunications companies, health-care service providers and a host of other operators that need to take into account the Nigeria Data Protection Regulation (NDPR) requirements as it relates to their businesses. To address this issue, a research question was raised '*what are the implications of the new NDPR for data controllers in Nigeria'?*

We provide answers to this question through a comprehensive systematic literature review and analysis of feedback obtained from audit reports filed by entities as well as

expert's interviews. We found five key components of the NDPR that can compel, motivate or support organizations to make significant structural changes such as standardization of processes, practices and IT assets to show conformity and/or gain legitimacy. We equally identified the factors that facilitate or inhibit the adoption and implementation of the conditions of the NDPR categorised in line with the three pillars of the institutional theory framework adopted for this study. The findings are discussed and enumerated to inform policy makers on the implications of their approaches towards ensuring compliance. It will also educate businesses on necessary cause of action and changes to ensure privacy and protection of personal data they solicit from data subjects.

The remaining part of the paper is organized into distinctive sections as follows: Section 2 presents related works in the field of privacy and data protection. Section 3 summarizes the concept of institutional theory. Section 4 discusses the methodology adopted for this study. Section 5 presents the result and discussion of the findings. Finally, Section 6 concludes the paper.

2 Related Work

The growing dependence by businesses on information technology (IT) to manage their data has led to increase in information security and privacy risks implications. The term 'privacy' is a multifaceted concept currently gaining traction in the field of computing. According to Nissenbaum [7], privacy is a contextual integrity and one of the most enduring social issues associated with information and communication technologies (ICT). The author opined that privacy is breached if personal data is used or made available outside its intended context. Data protection on the other hand refers to the processes of safeguarding the confidentiality of data including ensuring its privacy and protecting it from compromise. According to Friedewald et al., the concept of data protection is both broader and more specific than the right to privacy [2]. Art. 8 of the EU Charter of Fundamental rights is the first legislative attempt to distinguish data protection from privacy. According to Lynskey [8], the right to data protection provides individuals with more rights than right to privacy. The enhanced control introduced by data protection serves two purposes- a) it proactively promotes individual personality rights which are threatened by personal data processing and b) reduces the power and information asymmetries between individuals and those who process their data. In this regard, data protection is not intended only to make the protection of privacy real but also seeks to protect other rights relating to conscience, non-discrimination and a host of other concerns or interests.

Article 12 of the United Nations Universal Declaration on Human Rights provides- *no one shall be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* The declaration is a statement of intent of every member of the United Nations, including Nigeria. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Free-

doms guarantees the right to respect for private and family life, home, and correspondence. The African Charter on Human and People's Rights on the other hand does not provide for the right to privacy. This lacuna has been justified on the basis that Africa has more pressing rights issues such as child labour, slavery, terrorism etc. However, it has been argued to the contrary that invasion of privacy by telecommunication companies on behalf of government is repressing fundamental rights to expression, beliefs and life.[1] The courts have ruled that illegal monitoring of employees' usage of computer such as private mails, browsing sites and social media activities is a breach of right to privacy[2]. Unlawful storage of data is also held to be a breach of privacy.[3]

The growing concerns about automated personal data systems therefore resulted in the introduction of data privacy measures, regulations, and conventions in the western countries such as United States of America (USA) through the US Department of Health, Education, and Welfare as well as in Europe through the Organization for Economic Co-operation and Development (OECD) and EU [1]. For instance, in a move to standardize the protection of personal data privacy, the European Union (EU) enacted the Data Protection Directive in 1995 [9]. The directive which among other things prohibits corporations and governments from using personal data for any purpose other than original purpose without permission, took effect in 1998 [10].

Organizations are facing ever increasing regulatory interventions (e.g., GDPR, CCPA, NDPR, PIPEDA, HIPAA, etc.) that may lead to significant structural changes such as standardization of processes, practices, and IT assets to show conformity and/or gain legitimacy. According to UNCTAD, 107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy [11]. Noteworthy is the growing level of adoption in comparing Europe, Asia and Africa.

3 Institutional Theory

The manner in which organisations respond to changes is often dependent on the socio-political, economic and technological influences exerted by the environment in which they operate as posited by Weerakkody et al., [12]. Thus, the impacts of such external forces on organizational behaviour have been studied by many researchers using the institutional theory. The core concept of institutional theory is that organizational structures and processes tend to acquire meaning and achieve stability in their own right, rather than on the basis of their effectiveness and efficiency in achieving desired ends, such as the mission and goals of the organization [13]. Few studies have focused on using the theory to understand the impact of IT-enabled change in organizations [12]. According to DiMaggio & Powell, institutions exert three types of isomorphic pressures or effects, viz. coercive, normative, and mimetic [14]. Jennings and Greenwood [15] suggest that the notion of institutional pressures is akin to the concept of institutional

[1] Privacy International at the 62nd Session of the African Commission on Human and People's Rights (ACHPR)

[2] Barbulescu v. Romania (No. 61496/08)

[3] Roman Zakharov v. Russia (No. 47143/06)

pillars proposed by Scott, which comprises of *"regulative, normative and cultural cognitive elements that, together with associated activities and resources, provide stability and meaning to social life"* (pp. 48) [16]. The basic similarity in all institutional theoretical claims however, is that something identified at a higher level is used to explain processes and outcomes at a lower level of analysis [17].

In this research, the strength of the institutional theory is employed to determine the various implications of data privacy and protection regulations on data intensive businesses in the context of a developing country – Nigeria. Specifically, Scott's [16] three key pillars that can make up or support institutions viz. *regulative, normative and cognitive* are employed.

Table 1. Institutional Theory Framework

	Regulative	*Normative*	*Cultural-Cognitive*
Basis of compliance	Expedience	Social obligation	Taken-for-grantedness Shared understanding
Basis of order	Regulative rules	Binding expectations	Constitutive schema
Mechanisms	Coercive	Normative	Mimetic
Logic	Instrumentality	Appropriateness	Orthodoxy
Indicators	Rules Laws Sanctions	Certification Accreditation	Common beliefs Shared logics of action Isomorphism
Affect	Fear Guilt/ Innocence	Shame/Honor	Certainty/Confusion
Basis of legitimacy	Legally sanctioned	Morally governed	Comprehensible Recognizable Culturally supported

Source: *Institutions and Organizations pp. 51 [16]*

Institutionalization, through the lenses of the regulative pillar can be viewed as a stable system of rules that can be informal or formal backed by monitoring and sanctioning powers and accompanied by feelings of fear or guilt and/or innocence or incorruptibility. In normative systems, not only are goals and/or objectives defined, appropriate methods of pursuing them are also defined. Norms and values can vary depending on what the position is or who the actors are. Thus, the appropriate goals or activities assigned to particular actors or positions leads to the creation of roles or normative expectations of how specific actors are required to behave. Cognition can be described as the psychological result of perception and learning and reasoning. Scott [16], DiMaggio & Powell [14], and other organizational scholars have stressed the centrality of cognitive elements of institutions as being the "*shared conceptions that constitute the nature of social reality and the frames through which meaning is made*" [16] pp.57.

In summary, the three pillars – *regulative, normative and cognitive*, all have their distinctive features and ways in which they operate as shown on Table 1. However, Scott pointed out that in most empirically observed institutional forms, a combination of the pillars are observed at work which can lead to the formation of a stable social system [16].

This research contributes to the few studies that have applied institutional analysis as a theoretical lens for studying the implications of IS/ICT regulations on organizations. For instance, institutional theory has been used by Appari et al to explain the variability in regulatory compliance prevalent in the US healthcare sector [18]. In their explanation of firms' response to information security and privacy issues, Greenway and Chan argue that information security research could leverage socio-organizational theory, like the institutional theory, to frame inquiries [19]. Similarly, D'Arcy and Hovav advocate application of institutional theory to study the relationship between organizational characteristics and security best practices [20]. In a developing country context, Dahiru et al have also used the theory to determine the associative interaction between exciters and inhibitors to technology adoption [21].

4 Methodology

The research methodology adopted by this study is a qualitative one. A systematic literature survey backed by a pilot study was conducted in Nigeria between November 2019 and January 2020. During this phase, the focus of the study is to obtain the implications of data protection and privacy laws/regulations on data intensive businesses across key sectors in Nigeria. Considering the broadness of the topic as well as potential legal and economic implications, a systematic literature review was initially conducted to provide insights into the topic and to collect adequate qualitative data [22]. Further, using the selected theoretical underpinnings of the institutional theory, a data collection instrument was developed to allow for expansion of the research and to provide an evaluation mechanism. The pilot study was carried out in line with the design emphasised by Naoum [23]. As Naoum posited, lessons drawn from feedback in a pilot study helps the researcher to refine and check the instrument before the main data collection exercise.

4.1 Research Context

Considering key criteria, Nigeria is Africa's largest economy [24]. In addition, Nigeria launched one of the most vibrant campaigns towards enforcement of data privacy and protection on African content in recent time. Data collection and analysis were carried out in Nigeria cutting across key sectors including telecommunication, banking and finance, and regulatory agencies. These sectors were selected based on their direct involvement in the personal data processing and management to enhance the quality of data used in this study. As technology researchers involved in various stakeholders' awareness programmes, the research team was able to access qualitative data through top quality interviews in both public and private sectors.

4.2 Data Collection

The study relied on gradual but systematic literature reviews including audit reports and face-to-face interviews using a semi-structured interview guide. The systematic literature survey was conducted to elicit information required to meet the objective of this study. During the face-to-face interviews, selection of participants was made based on participant's degree of involvement in the ongoing data protection and privacy revolution in Nigeria. The selection process also employed snowballing approach that facilitated researcher's contact with data privacy and protection experts across key sectors in Nigeria. In this pilot study, seven data intensive organizations were considered in both public and private sector and a total of eleven participants were interviewed. The participants included two executive directors, and three general managers, four senior managers and two CTOs. Participants profile are summarized in table 2. All the interviews were conducted in English language with note taking and audio recording and lasted for 45 to 55 minutes.

Table 2. Profile of Interview Participants

Sector	**Profile**			
	ED	**GM**	**SM**	**CTO**
Telecommunications	0	2	1	0
Banking/Finance	1	1	2	2
Regulatory Agencies	1	0	1	0
Total	**2**	**3**	**4**	**2**

4.3 Data Analysis

Data relating to Privacy and Protection advances were analyzed using institutional theory discussed in the previous section. Data Privacy and Protection issues in this study were evaluated within each domain (as shown in table 2) on the basis of qualitative data elicited through interviews and credible documents relating to NDPR. In view of the relatively small number of participants involved in this pilot study, results from the interviews were analyzed using qualitative manual method.

5 Results and Discussion

In this section, we describe the most important findings based on the feedback from experts' interviews, pertinent literature and audit reports. Considering the early stage of Data Protection regulation in Nigeria, the analysis focused on laying out the key issues relating to implications of Personal Data Protection for data controllers in key sectors. We achieved this through useful inputs obtained from experts in terms of Personal Data Protection implications in the context of Nigeria.

The recent adoption of NDPR brings about new obligations compelling all data controllers handling Nigerian personal data to review their existing data privacy and pro-

tection policies to ensure compliance with NDPR. To guide these tasks, this paper identified key implications of NDPR for data controllers. The 5 key components of NDPR identified in the analysis are summarised in Table 3.

Table 3. NDPR Implications for Data Controllers

NDPR Implications	Requirements
Data Controllers to Designate a Data Protection Officer	Data Controllers are required to appoint competent person or outsource data protection to verifiably competent firm to ensure adherence to NDPR.
Considering conditions for data processing in international context	Data Controllers are obliged to ensure that Data Subject consent explicitly to the proposed transfer, after being informed of possible risks of such transfer to a third country. Data Controllers must ensure that Data Subject is manifestly made to understand through clear warning of the specific implications of data protection likely to be violated as a result of such transfer to third country.
Ensuring Data Subject's right to data portability	Data Controllers are required to ensure that data subject reserve the right to have personal data transmitted directly from one controller to another.
Provision of measures for dealing with data breaches	Data Controllers are obliged to secure personal data against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, manipulation of any kind, and damage by natural elements.
Reckoning with penalty for dealing with default	Under NDPR, regulatory authority (NITDA) has powers to impose administrative fine on defaulting Data Controllers. Issues of non-compliance could cost Data Controllers a fine of up to 10 million Naira or 2% of Annual Gross Revenue of the preceding year.

Awareness of NDPR implications is key and can be viewed as the starting point for the NDPR requirements for implementation amongst data controllers. In this area, findings of this study only confirmed the awareness at the top-management level. For instance, when prompted to confirm the level of awareness of NDPR and the potential implications on their organization, participants of this study confirmed that only their top management is aware of the regulation and implications of not adhering to data protection laws, procedures and policies. Although the interviewees tend to confirm awareness at the management level, only one participant from the banking sector confirmed compliance and steps taken to engage Data Protection Compliance Organization (DPCO). This is an indication of the need for additional awareness creation and sensitization. Imple-

mentation of NDPR in Nigeria indicates the need to designate DPCOs in various organizations, which may have considerable impacts on controllers' technical competence and may need the hiring of more expertise.

Organizations involved in data processing in international context are also required to put in place security measures including rules for the onward transfer of personal data to foreign country or international organization. This principle is related to a host of other principles enunciated in the NDPR for data processing regarding data minimization, specific purpose, lawful and legitimacy, accuracy as well as storage and security of personal data (Art. 2.1a to 2.1d). Adherence to these principles can be considered reasonable. However, interviewees from the banking sector expressed concern regarding data they share with their partners in card sub-sector that maintain data centres worldwide, where in most cases, location of such centres remain unknown to them. This is in alignment with previous studies by Dahiru et al [21] that indicated how data is transferred to international 3rd parties without recourse to its sensitivity.

Implementation of NDPR also introduces a new right to data portability. This right imposes new capability on Data Controllers to ensure there is capability to provide data subject their personal data in compatible format when the need arises. One of the underpinning principles of the NDPR is that Data Controller must comply with basic minimum standards of information security management. In this regard, Data Controllers and Data processors are to ensure Confidentiality, Integrity and Availability. Interviewees have all indicated that their organizations have created a new role for Data Protection Officer within the organization and have appointed or are in the process of appointing an officer to fulfill that role.

Regarding data breaches, implementation of NDPR imposes new obligation for Data Controllers to notify the regulatory authority and data subjects of any data breaches without delay. In this regard, Data Controllers need to put in place notification mechanisms which may require serious changes to the existing systems especially in the area of new technologies. When asked to indicate whether or not their organizations have a register for data breaches and security incidence, interviewees across the sectors investigated indicated "*NO*" suggesting that they do not currently have an internal data protection policy in place to support implementation of this NDPR commitment.

Finally, implementation of the NDPR requires that Data Controllers and Data Processors reckon with sanctions in their processing principle for failure to do so may cost them a fine of up to 10 million Naira (Approx. USD27, 000, or €24, 000) by the regulatory authority. Response from interviewees indicate that while organizations are concerned about fines in monetary terms, they are more worried with brand image damage, and marketing and publicity. Thus, to ensure compliance and avoid these sanctions, Data Controllers have started to review their privacy and protection measures to keep to this requirement.

Further, the analysis of the audit report and feedbacks from experts' interviews led to identification of several factors arising from the adoption and implementation of NDPR in Nigeria. While some of the factors are positive and favourable in facilitating the implementation of NDPR conditions, some are negative, and hence inhibiting the implementation of NDPR measures. These identified factors are categorised in line with the three pillars of institutional theory framework as shown in Table 4.

Table 4. Institutional Factors in the Adoption of NDPR

Institutional Pillar	Facilitators	Inhibitors
Regulative	Well-articulated policies and guidelines NDPR Compliance monitoring Risk Assessment mechanism Capacity building for senior managers on NDPR	Lack of organizational plans and initiatives regarding NDPR Absence of legal framework and policy Insufficient technical staff & training
Normative	Awareness and sensitization of key stakeholders Monitoring & Evaluation of NDPR Implementation Funding with regards to NDPR enforcement	Lack of industry-wide direction on how to achieve NDPR objectives Absence of review mechanism for NDPR Absence of budgetary provision for NDPR
Cultural-Cognitive	Involvement of key Stakeholders in the implementation of NDPR Communicating the benefits of Personal Data Protection to stakeholders	Resistance to change and risks of leaving personal data unprotected Not realizing the importance of NDPR.

As Scott [16] pointed out, in most empirically observed institutional forms, a combination of the pillars are observed at work. Concerning the regulative pillar, formulation of well-defined policies appears to be the strongest factor facilitating the level of compliance with NDPR measures amongst stakeholders. Thus, formulation of such policies received inputs from key actors through series of stakeholders' engagements. Inhibiting factors under the same pillar include insufficient human capacity especially in technical areas and adequate training organized by top management.

Regarding the normative pillar, it is important to note that some of the data controllers are willing to conform to industry best practices and recognize the opportunities therein, however, data subjects are not yet conversant with the newly acquired rights as a result of the introduction of the NDPR. The findings from this study therefore suggest the need for continuous awareness for data subjects and adequate training for data controllers at organizational level. A major inhibiting factor highlighted under this pillar relates to absence or lack of funding for NDPR activities.

Regarding the Cultural-Cognitive pillar, involvement of key stakeholders in NDPR implementation and communicating the benefits of Data Protection to stakeholders were highlighted as facilitating factors. Under the same pillar, resistance to changes and risks of leaving personal data unprotected are highlighted as inhibiting factors. It is

therefore imperative to learn how to deal with the cultural changes inherent in data privacy and protection initiatives such as NDPR.

6 Conclusion and Future Work

This study attempts to identify Data Protection Regulation requirements and implications for Data Controllers and Processors in the context of a developing country - Nigeria. The research study analysed these implications using the institutional theory framework. Although the NDPR was launched in January 2019, most Data Controllers and Processors are yet to realise the complexity of its implications.

The identified implications of the new changes introduced by NDPR adoption and implementation were collated with 5 key aspects prioritised by Data Controllers for compliance in order to avoid sanctions from regulatory authority for non-compliance. Specifically, the research projects that controllers need to pay attention to awareness creation and designate DPOs for proactive implementation of NDPR requirements. NDPR also specifies procedures for data processing in international context. Thus, Data Controllers must consider this requirement when transferring personal data to third countries or international organisations. Similarly, the NDPR introduces obligations that require Data Controllers to ensure data portability. Data Controllers also need to ensure uniform standards or interoperability of their procedures for seamless transmission of data. Regarding data breaches, Data Controllers equally the appointment of a DPO that will support the compliance through the development of an internal data protection policy and a robust data breach reporting mechanism. Finally, as the NDPR also imposes sanctions for non-compliance, Data Controllers need to review their strategies and reckon with sanctions and adequate budgetary provision to support compliance when planning.

As part of the major contributions of this paper, some guidelines believed to facilitate the institutionalisation of NDPR measures across organisations were pushed forward. Evidence from this study as presented in the previous section suggests that use of institutional theory can help in interpretation of different level of NDPR adoption and implementation by Data Controllers. It can also help to project policy direction enhancing the institutionalisation of NDPR measures across key sectors. It is imperative therefore to extend the scope of this study in the future to cover more organisations in order to determine the extent to which the NDPR implementation facilitates and support the digital economy transformation in Nigeria.

References

1. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.
2. Friedewald, M., Wright, D., Gutwirth, S., & Mordini, E. (2010). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation–The european journal of social science research, 23*(1), 61-67.

3. Roos, A. (2006). Core principles of data protection law. *Comp. & Int'l LJS Afr.*, *39*, 102.
4. Gellman, R. (2014). Willis Ware's Lasting Contribution to Privacy: Fair Information Practices. *IEEE security & privacy*, *12*(4), 51-54.Ge
5. Law of the Federal Republic of Nigeria, (2004). Chapter 4, Section 37 *fundamental right of citizens to private and family life*.
6. Nigeria Data Protection Regulation (2019). Art 1.1. Retrieved from: https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf
7. Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.
8. Lynskey, O. (2014). Deconstructing data protection: the 'added-value'of a right to data protection in the EU legal order. *International & Comparative Law Quarterly*, *63*(3), 569-597.
9. Steinke, G. (2002). Data privacy approaches from US and EU perspectives. *Telematics and Informatics*, *19*(2), 193-200.
10. Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, *24*(6), 508-520.
11. United Nations Conference on Trade and Development UNCTAD. (2020). Data Protection and Privacy Legislation Worldwide Retrieved from: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx Accessed On: 18 February 2020
12. Weerakkody, V., Dwivedi, Y. K., & Irani, Z. (2009). The diffusion and use of institutional theory: A cross-disciplinary longitudinal literature survey. *Journal of Information Technology*, *24*(4), 354-368.
13. Miles, J. A. (2012). Management and organization theory: A jossey-bass reader. () John Wiley & Sons.
14. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, , 147-160.
15. Jennings, P. D., & Greenwood, R. (2003). 6bConstructing the iron cage: Institutional theory and enactment'. *Debating Organization: Point-Counterpoint in Organization Studies*, *195*
16. Scott, R. W. (2008). Institutions and organizations: Ideas and interests.
17. Clemens, E. S., & Cook, J. M. (1999). Politics and institutionalism: Explaining durability and change. *Annual Review of Sociology*, , 441-466.
18. Appari, A., Johnson, M. E., & Anthony, D. L. (2009). HIPAA compliance: an institutional theory perspective. *AMCIS 2009 proceedings*, 252.
19. Greenway, K.E., and Chan, Y.E. (2005) "Theoretical Explanations for Firms‟ Information Privacy Behaviors," Journal of AIS, 6, 6, 171–198
20. D‟Arcy, J. and Hovav, A. (2009) "An Integrative Framework for the Study of Information Security Management Research," in Jatinder Gupta and Sushil Sharma (Eds.), Handbook of Research on Information Security and Assurance, Idea Group Publishing, 55–67.
21. Dahiru, A. A., Bass, J. M., & Allison, I. K. (2014, November). Cloud computing adoption in sub-Saharan Africa: An analysis using institutions and capabilities. In *International Conference on Information Society (i-Society 2014)* (pp. 98-103). IEEE.
22. Glaser, B. G., & Holton, J. (2004). *Remodeling grounded theory*. Paper presented at the Forum Qualitative Sozialforschung/Forum: Qualitative Social Research Author, F.: Article title. Journal 2(5), 99–110 (2016).
23. Naoum, S. G. (2013). *Dissertation Research and Writing for Construction Students* (3rd ed. ed. Vol. Routledge 3rd ed. 2013)
24. National Bureau of Statistics. (2019). *Nigeria Economy Largest in Africa*. [Online]. Available: http://nigerianstat.gov.ng/