An Analysis of Data Protection and Compliance in Nigeria

Diyoke Michael Chika[1], Edeh Stanley Tochukwu[2]

[1]*Department of Sociology Nnamdi Azikiwe University Awka, Nigeria*

[2]*Department of Computer Science, Caritas University Enugu, Nigeria*

***Abstract*:-Contemporarily data protection and privacy has garnered increasing attention in recent years, majorly because data has become a ubiquitous asset in the global community, mirroring the transformation of our societies to data sharing age. Again, the regular and large-scale breaches of sensitive data around the globe have become a growing concern. In spite of these breaches and attacks, several countries of the world and organizations have not yet completely prioritized personal data protection particularly in the third world countries such as Nigeria. Thus it was on this note that this paper was set up to explore the data protection and compliance in Nigeria. The methodology was based on review of published articles, books and journals in order to draw a conclusion on the contemporary issues in data protection and compliance in Nigeria. The paper argued that the upsurge of data sharing and breaches in Nigeria is still hampered by inappropriate/inadequate data protection and privacy legislation, lack of enforcement drive, limited number of practicing professionals among others. In addition, it was observed that data protection and privacy are practically strange to the Nigerian society as data subjects are generally unaware of their privacy rights over personal data that belongs to them. The resultant effect is high level of data breaches and data privacy abuse in the country. In the light of the above, this paper concludes that it is clear that data has become a ubiquitous asset in the global community – Nigeria inclusive. Thus the paper recommends (amongst others) that there is need to strengthen the current legislation and enforcement procedures on data protection.**

***Key Words:* Data Privacy and Protection, Data Subjects, Compliance and Nigeria**

I. INTRODUCTION

Contemporarily, data protection and privacy has garnered an increasing attention in recent years, majorly because data has become a ubiquitous asset in the global community. Internet has brought the whole world together through exchange of information. As a matter of fact, a majority of the world's organizations has resorted to digital operations of their activities, thus requiring a dramatic flow of personal data.

In addition, and more importantly, the regular and large-scale breaches of sensitive data around the globe have become a growing concern. Several companies, including Uber and Facebook have been victims of cyber-attacks. For instance, in September 2018, there were reports that a cyber-attack exposed Uber's data, affecting 57 million customers and drivers. Facebook also had its share of cyber-attack in September 2018 as 90 million Facebook user accounts were exposed by a security breach in the UK (Techworld Staff, 2018). Only recently, the National Information Technology Development Agency (NITDA) was reliably informed and duly ascertained that the Lagos State Internal Revenue Service (LIRS) published a web portal - https://lagos.qpay.ng/TaxPayer, where personal information of tax payers of Lagos State was gleaned by the general public in breach of the Nigeria Data Protection Regulation Act (NDPR), 2019.

In spite of the above breaches and attacks, several countries of the world and organizations have not yet completely prioritized data privacy particularly in the third-world countries such as Nigeria. Also, our lives move increasingly digitalized to the online environment. The future of data protection is becoming more complex than ever. Cultural trends, social pressure, and new technologies pull us-or perhaps push us-towards sharing more personal data with others. Our friends in the social network are interested in such data, but so are corporations and governments. Again, the vast majority of the data that the world has produced are either personal data or data that can be traced back to specific individuals (Labadie and Legner, 2019).

Traditionally, organizations utilize different strategies of de-identification (anonymisation, pseudonymisation, encryption, key-coding, data sharing) to distance data from their real identities and allow analysis to proceed while at the same time containing privacy concerns. Over the past few years, however, computer scientists have over and over indicated that even anonymised data can often be re-identified and attributed to specific individuals (Ohm, 2010).

The last decades have seen the introduction and fortifying of data protection laws in few nations (Fausto, 2018). In Europe, for instance, the General Data Protection Regulation (GDPR) will replace the Data Protection Directive (Directive 95/46/EC) from May, 2018. Such regulations demand overwhelming penalties upon organizations that neglect to satisfactorily guarantee security and over transparency into their data processing activities. In addition, the EU-US Privacy Shield implements protection guidelines upon companies in the USA that process the data of European citizens. Organizations that plan to actualize privacy controls through either business process modifications or the execution of privacy-enhancing technologies (PETs) require techniques to assess and improve the current state of their procedures (Gibler, Crussell, Erickson, and Chen, 2012).

In the same vein the National Information Technology Development Agency (NITDA) was set up by the National Information Technology Development Agency Act 2007 (NITDA Act) as the legal organization with the obligation for planning, developing and promoting the use of information technology in Nigeria. In addition, Section 6 (c) of the NITDA Act., the NITDA Act empowers the Agency to do the following: "Develop rules for electronic administration and monitor the use of electronic data interchange and other forms of electronic communication exchanges as an option to paper-based strategies in government, business, education, the private and public sectors, labour, and other fields, where the utilization of electronic communication may improve the exchange of data and information". It was further to the foregoing powers that on 28th January 2019, NITDA published its Data Protection Regulation ("the Regulation") which aims at protecting personal data of all Nigerians and non- Nigerian residents in Nigeria. This Regulation is undoubtedly a game changer in the protection of data in Nigeria as it is contemporary and is a replica, in some respects, of the European Union (EU) General Data Protection Regulation (GDPR). The Regulation will rather be considered to be a Derogation, since it modifies some clauses in the GDPR to suit the Nigerian economic environment. The Regulation wastes no time in describing data which is defined to include a name, a photo, an email address, bank details, medical information, computer internet protocol (IP) address and any other information specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Therefore, this paper is an attempt to x-ray data protection and compliance in Nigeria. In doing so, it will identify the issues and challenges militating against data protection and compliance in Nigeria and in comparison, with other data protection and compliance bodies across the globe. In other to achieve these aims, the paper has been structured into four parts. While the first section introduces the work, the second part provides conceptual clarifications of variables that are associated with study. The third part looks at the issues and challenges, in comparison with other countries. Finally, the fourth part concludes the work and provides appropriate recommendations.

II. CONCEPTUAL CLARIFICATIONS

Data, Data Protection and Privacy

Data has been defined in many ways by different authors. These definitions reflect how the keywords are perceived in the scholarly domain. However, Zins, (2005) conceptualized data as everything or every unit that could increase the human knowledge or could allow to enlarge our field of scientific, theoretical or practical knowledge, and that can be recorded, on whichever support, or orally handed. The scholar added that data is commonly used to refer to records or recordings encoded for use in computer, but is more widely used to refer to statistical observations and other recordings or collections of evidence.

Earlier, Clarke (1992) maintains that data is any symbol, sign or measure which is in a form that can be directly captured by a person or a machine. While his definition lies within the domain of Information Science, to oxford learner's dictionary, data entails information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer. However Clarke, (1992) submitted that the dictionary meaning of data is rather abstract such that it cannot be applicable in the field of Information Science.

The Nigeria Data Protection Regulation 2019 (NDPR) defines the word as:

"Characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device. In conclusion we can refer to data as records of anything that can easily be translated to knowledge or information usually stored in computer.

There are different kinds of data, but for the purpose of this paper, we shall restrict our scope to Personal Data. It will be highly unavoidable to talk about Data Privacy without linking data to data owners. In the Data Protection space, the General Data Protection Regulation (GDPR) is recognized as the gold standard, which sees personal data as data that only includes:

> "Information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information".

Generally speaking, personal data is any information relating to a Natural Person including Name, online identifier (cookie or email address etc.), location data, ID number etc. While GDPR seems to serve as the gold standard for Data Protection to many countries, some countries have gleaned their own tailor-made data protection regulations. This type of regulation is regarded, in data protection parlance, as derogation. On the basis of derogations, the Nigerian Information Technology Development Agency (NITDA) has come up with Nigeria Data Protection Regulation. According to the regulation, "Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, an address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others".

So far, it seems vague as to what exactly constitutes personal data. The fact remains the same in all instances: "personal data is any data relating to a natural person or a Data Subject, and that must be considered in context". More realistically, personal data may constitute: biometric data, genetic information, medical history, criminal records, credit/debit card information, phone numbers, name, date of birth, sexual orientation, ethnic background, religious information, address/location, employee records, curriculum vitae, International Passport, National ID card, Driver's License, Fingerprint, IP Address, etc. To support this assertion, GDPR states that "personal data may also include special categories of personal data or criminal conviction and offences data". At this juncture, it is indicative enough that personal data is strictly restricted to data about a natural person. In the Data Protection domain, this natural person is called the "Data Subject".

Data Subject

On the other hand Data Subject is the person, whom the personal data is about or rather the person who owns the personal data under consideration. Prior to Data Protection Regulation, controllers and processors were reluctant about how personal data was being processed. It was normal for a controller to claim complete ownership of the personal data and process same without the knowledge of the Data Subject. GDPR recognizes this type of processing as an "invisible processing", viz: "collecting personal data from a source other than the individual without providing them with a privacy notice". With regards to the foregoing, data protection regulation imposes certain rights on the data subjects with regards to their personal data. These rights are meant to toughen the privacy of Data Subject's personal data. Some of these rights are: right to access, right to rectification, right to be forgotten, right to restrict processing, right to data portability, right to object.

Data Protection and Privacy

While data protection and privacy are sometimes used interchangeably, there are still some distinct differences. For instance, while they are both branches within data security, Data protection is commonly defined as the law designed to protect your personal data especially in this information society, in order to empower us to control our data and to protect us from abuses. It is essential that data protection laws restrain and shape the activities of companies and governments (Costa, 2012). These institutions have shown repeatedly that, unless rules restricting their actions are in place, they will endeavour to collect it all, mine it all, keep it all, share it with others, while telling us nothing at all. From this standpoint, data protection can, therefore, be seen as an attempt to tame the risks of data sharing in this sophisticated technology era.

Conversely, Data privacy or information privacy is concerned with the proper handling of data consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around: whether or how data is shared with third parties and how data is legally collected or stored. Put differently, data privacy can be seen as the right of an individual to be free from uninvited surveillance. To safely exist in one's space and freely express one's opinions behind closed doors is critical to living in a democratic society. Though most people agree on the importance of data privacy, and everyone has agreed that data protection is at the heart of ensuring privacy (Jeff, 2020).

With the rise of the data economy, the data privacy has become the most significant issues in our industries across the globe. Companies find enormous value in collecting, sharing and using data. Companies such as Google, Facebook, and Amazon have all built empires atop the data economy. Transparency in how businesses request consent, abide by their privacy policies, and manage the data that they've collected is vital to building trust and accountability with customers and partners who expect privacy. Many companies have learned the importance of privacy the hard way, through highly publicized privacy failures.

III. CHALLENGES MILITATING AGAINST DATA PROTECTION AND COMPLIANCE: THE NIGERIAN EXPERIENCE

Inappropriate/Inadequacy of Data Protection and Privacy legislation

Just like every other developing nation, inappropriate legislation to data protection has hampered data protection and compliance in Nigeria. Nigeria laws on data protection and privacy are not specific to the target. Not until January 25, 2019, Nigeria didn't have any devoted general enactment on data privacy and protection apart from the 1999 Constitution (as amended) which has not been particularly useful for the purpose of data privacy especially given the fast pace of technological advancements and the associated complexities and also considering our courts somewhat restrictive approach to the interpretation of the relevant section on privacy.

For instance Section 37 of the 1999 Constitution provides that:

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

In spite of the fact that the provision above does not explicitly make reference to "data", it is arguable that information on homes, correspondences and telephone conversations are captured in the definition of personal data; hence, the above provision can be utilized to defend such breach.

In addition, these inadequacies are manifested in the lack of an analogy between data breaches and their conventional counterparts. For instance, trespassing and hacking into a computer network. The penalty on trespass does not hold against hacking and accessing private data. This clearly illustrates a challenging situation whereby no relevant laws on hacking are available. Therefore, there are a lot of inadequacies in the Nigeria legislation on data protection which is also expected to be the case in other developing countries (Muli and Mutua, 2013).

Again, even with the legislations and the emergence of NDPR the capacity to adequately protect personal data and privacy especially in respect to data collection, control and processing fall short of international standard. For instance, the NDPR has been criticized for being sketchy compared to its European equivalent; the General Data Protection Regulations (https://techpoint.africa/2018/05/31/gdpr-compliance-nigeria/) (GDPR).

> "There is a lack of synergy among stakeholders," said Fatai Tella, chief data officer, Sterling Bank Plc. "We need to sit down and ask what we are solving? What are the data breaches that should necessitate a policy?" (businessday.ng 2019)

Although comparison, however, uncovers that the NDPR borrows a lot from the GDPR in its fundamental principles, it takes the issue of data privacy as a fundamental right of the data owner (or data subject) which should be protected through regulatory oversight even though the data has been submitted to a company for the provision of services. Therefore the lack of uniformity in data control is also a major challenge as it uncovered individuals and businesses to various entry points. . Be that as it may, the existence of many buckets of data is not exclusive to Nigeria. The difference is that, whereas the countries in the western world have attained a certain level of maturity in the handling of buckets of data, Nigeria is still on the way (Nigeria data protection regulation, NITDA Act., 2019).

Reporting Data Breaches

Despite the emergence of NDPR in Nigeria, most data breaches still go undocumented or unreported to the data subjects. Several reasons have been attributed to this, ranging from delay in informing the data subject of breaches in some situations, to data processor or data controller, to report data breaches, to the authority, and the authority required to notify the data controller whether they should notify the data subject of the breach.

This is contrary to The GDPR, under article 33, which obligates Controllers/Processors to report data breaches within 72 hours to the supervisory authority and to concerned parties if the breach poses an implementation challenge. Data protection and privacy laws in Africa will therefore have to establish adequate notification mechanisms in the event of data breaches.

In support of this, Olumide, (2020) added that data protection and privacy are practically strange to the Nigerian society. Data subjects are, generally, unaware of their property rights in data and Data collectors/administrators are numb to their corresponding duty to protect and/or respect the privacy of data entrusted in their hands. Eventually, there appears or appeared to be a stunning complicit quietness or absence of controllers in this field. Up until the development of negligible few civil societies, which as of late, made data privacy and protection their center concerns, Nigerians have never genuinely encircled about whatever happened to their information so long their other money related/physical rights remained undisturbed. Therefore, in a country where people's personal data is being shared without consent, experts note compliance might be difficult for many organizations, especially government agencies.

Consent to Data Collection

Another important issue is the consent for one's personal data which is an important aspect of data privacy of Nigeria data protection regulation and global data protection regulation in particular. Consent implies that valid consent must be obtained prior to the collection of data, especially through clear stipulation of the purpose of data collection and indication of the need for additional consent where personal data might be shared with third parties. Further, that data controller takes and keeps record of consent of individuals, and there must be provision for withdrawal of consent by the data subject at any time (European Data Protection Board, 2016).

Regrettably, in Nigeria, both government agencies and private firms have consistently failed to comply with these regulations by their actions, thus costing many untold embarrassment and hardships to individuals and even corporate bodies. In Nigeria, even without your knowledge, data and information about you is being generated and captured by companies and agencies that you are likely to have never knowingly interacted with.

Lack of Enforcement

Beyond the inadequacy that characterized the data privacy legislation in the country many social commentators and scientists alike have expressed concerns over the ability of government to conform to the provisions of the data protection regulation as many agencies and parastatals were known to flout the law.

So, despite coming up with the NDPR act by NITDA, it ought not to end there. The NDPR act, though issued on the 25th day of January 2019, was meant to take effect from 25th April 2019, at least with the Data Collectors distributing their protection policies as compulsorily required by section 2.5 of NDPR. However, according to (Olumide, NS),April 25 came and left, neither have the various Data Collectors published their privacy policies to our knowledge nor did NITD Apenalize them as provided under section 2.10

of the NDPR, thereby giving a rebuttable impression that the regulators are treating them with kid gloves.

There are other provisions requiring prompt and constant compliance, for example, section 4.1(2) requires every Data Controller to designate Data Protection Officers but this is sadly non-existent and remains unenforced by the regulator. One example that easily comes to mind is the recent breach of the NDPR act by the Nigeria Immigration Service following a publication of the international passport data page of a Nigerian resident in the UK. The data was published on the Service’s social media pages without the Data subject’s consent but we are not aware of any sanction meted to the Immigration Service under NDPR (Olumide, 2020)

This isn't the only Nigerian Government website with such vulnerability. Somewhere in the CAC website just by entering the name & CAC registration number of a business you can find everything about a business, including names and addresses of the directors, their contacts, etc. This is appalling; on the backdrop of the fact that most firms include their CAC number in their insignia. Many other websites can easily be manipulated to get very personal information on people.

Dearth of Practicing Professionals in the Country

Other pertinent challenges facing probably data privacy and compliance in Nigeria has to do with the emerging roles and problems with global data protection regulation (GDPR) which is expected to reshape the hierarchical structure of both private and public sector, as well as keeping track of the law and technological updates that are always in constant motion regarding data privacy and protection. This, of course, necessitated the need for expertise and professionals such as data protection officers (DPOs). Unlike many western nations, this role is not new to Nigerians and many third world nations but the country also lacks practicing professionals (Dode, 2018).

GDPR and its recitals define the DPO role as very important for both public and private sector, both large and small scale of data being processed. Even though the scale is not defined, but if there are personal data, DPO role is a must role for the company or authority. During his/her job, a DPO, being certified or not, should have enough knowledge to guide the company towards problems that the company or public entity might have on the road towards GDPR. A DPO has several duties to ensure the company complies with GDPR regulation. Regrettably, most of the companies rely on automated decisions; their decisions sometimes can be objects of complaints.

In addition, many Nigerian companies despite everything eye the NDPR buzz with a level of doubt, subtly wishing it goes away in view of the compliance costs in time and resources. Fortunately, the presence of data protection regulation is becoming internationally perceived as a sign for trust in a nation's online business space. As organizations become associated all inclusive and information trade turns into an inexorably essential piece of business exchanges, data protection is becoming a risk issue discussed at the negotiation stage between companies in different jurisdictions. Countries that intend to show seriousness to grow trust in their online business infrastructure must take data protection seriously.

IV. CONCLUSION AND RECOMMENDATIONS

Conclusively from the discussion, it is clear that data has become a ubiquitous asset in the global community, mirroring the transformation of our modern societies, in which massive data collection and analysis have become a key competitive advantage. However, the transformation also emerges with its own challenges particularly in emerging societies like Nigeria, despite the current mechanisms of alleviating them. This is majorly due to the complexities that surround data protections and privacy, Inappropriate/Inadequacy of Data Protection and Privacy legislation, dearth of practicing professionals and amongst others.

Accordingly, therefore, this paper recommends that since technology will continue to advance, there is a need for the government and relevant stakeholders alike to review existing laws on data protection to suit new technologies. Similarly, enforcement procedures need to be reviewed. Law enforcement agents need to be trained on dealing with more sophisticated data crimes. Education and training needs to be intensified to fill the gap of dearth of practicing professionals

Finally, there is a need to strengthen the current legislation and enforcement procedures on data protection. All these will eliminate the challenges and make the culture of data protection and privacy standardized in Nigeria.

REFERENCES

[1]. Arvind N & Vitaly S, (2008) Robust De-anonymization of Large Sparse Datasets, 2008 Proc. of IEEE Symp. on Security & Privacy 111; Latanya Sweeney, Simple Demographics Often Identify People Uniquely 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).

[2]. Costa, L. (2012) “Privacy and the precautionary principle” *Computer Law & Security Review*, *28*(1), 14–24. doi:10.1016/j.clsr.2011.11.004

[3]. Dode A, (2018) “The challenges of implementing General Data Protection Law (GDPR)” *https://www.academia.edu/37461999/The_challenges_of_implementing_General_Data_Protection_Law_GDPR_*

[4]. European Data Protection Board (2016) Guidelines on Consent under Regulation 2016/679 (WP259, rev.01) retrieved 2020 at: www.europeandataprotection.com/pdf

[5]. Fausto S (2018) Static Analysis for GDPR Compliance: https://www.researchgate.net/publication/336987954

[6]. Gibler, C, Crussell, J. Erickson, J and Chen H,(2012) Android Leaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale. *In Proceedings of TRUST '12. Springer- Verlag,*

[7]. Techworld Staff, (2018) ‘The most infamous data breaches’ Available from <https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/>Accessed 28 March 2020.

[8]. https://lagos.qpay.ng/TaxPayer

[9]. Jeff P, (2020) Data Privacy Guide: Definitions, Explanations and Legislation | Varonis: https://www.varonis.com/blog/data-privacy/

[10]. Muli D T, Mutua N M, (2013) Addressing the Challenges of Data Protection in Developing Countries European Journal of Computer Science and Information TechnologyVol.1, No. 1, Pp.1- 9.

[11]. Labadie, C Legner C, (2019) Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR: https://www.researchgate.net/publication/330133849

[12]. Nigeria Data Protection Regulation, NITDA Act, 2019

[13]. Olumide B (2020) Data Protection and Privacy Challenges in Nigeria (Legal Issues) *https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-*

[14]. Ohm, P (2010) Broken, Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701

[15]. Punch newspaper (2019) Concerns as Nigerian firms move to adopt data protection Regulation: https://punchng.com/concerns-as-nigerian-firms-move-to-adopt-data-protection-regulation/

[16]. Weber, R.H (2013) "Trans-border data transfers: concepts, regulatory approaches and new legislative initiatives"

[17]. Zins, C (2005) what is the meaning of data, information and knowledge *http://www3.interscience.wiley.com/cgi-bin/abstract/114083668/ABSTRACT*