THE CHANGING PERSPECTIVE OF DATA PROTECTION REGULATIONS IN NIGERIA: AN EXAMINATION OF THE ISSUES AND CHALLENGES

Written by ***James Agbadu Fishim*, Anugbum Onuoha** & Peter Ter Ortese******

**Former Senior Lecturer Faculty of Law University of Abuja and judge of National Industrial Court of Nigeria, Nigeria*

***Senior Lecturer Faculty of Law River State University Port Harcourt, Nigeria*

****PhD Student of University of Uyo Akwa Ibom State Nigeria and Divisional Registrar National Industrial Court of Nigeria Uyo Akwa Ibom State, Nigeria*

ABSTRACT

Like several countries around the world, the Nigerian government, after years of stale debates and regulatory inactivity, took the issue of data protection and privacy very seriously in 2019 through the issuance of the Nigerian Data Protection Regulation (NDPR) 2019 by the National Information Technology Development Agency (NITDA). The NDPR laid down the legal structure for the collection, processing, storage, use, transfer, protection and disclosure of personal data. It is said that the NDPR was influenced by the EU GDPR and that nearly all the provisions of the two regulatory instruments are identical. The NDPR is a significant advancement for the Nigerian economy and Nigerians' privacy rights, considering its territorial implementation. It may also be Nigeria's strictest and most far-reaching data protection law, placing strict requirements on entities and stringent penalties if there is a default in compliance. The digital economy in Nigeria is expected to continue to grow and it will attract numerous global players who must comply with the regulations. This paper seeks to examine and evaluate the NDPR and its implications on businesses who collect and process data of Nigerian residents. Transitioning from a state of affairs where there were no strict privacy law or data protection obligations on companies and institutions, compliance and enforcement of the NDPR may be an unyielding issue. The paper would review some of these challenges and

proffer pragmatic solutions that can make the compliance and enforcement of the regulations more effective.

***Keywords*:** Data Protection, Data Privacy, Data Subjects, Compliance and Nigeria

INTRODUCTION

Like several countries around the world, the Nigerian government, after years of stale debates and regulatory inactivity, took the issue of data protection and privacy very seriously in 2019. This is because it is difficult to overemphasize the fundamental importance of data in today's world. The right to data privacy and protection is a guaranteed right, as many academics and advocates have noted, and should universally enjoy protection. A few other nations, apart from the EU[i], have implemented legislation to keep up with business trends in technology and its effects[ii]. In line with current realities and global norms, with the issuance of the Nigerian Data Protection Regulation (NDPR) 2019[iii] by the National Information Technology Development Agency(NITDA)[iv], Nigeria joined the league of countries implementing data protection laws. The NDPR lays down the legal structure for the collection, processing, storage, use, transfer, protection and disclosure of Nigerian residents' data. It is said that the NDPR was influenced by the EU GDPR and that nearly all the provisions of the two regulatory instruments are identical.

The NDPR is a significant advancement for the Nigerian economy and Nigerians' privacy rights, considering its territorial implementation. As new technological advancements are implemented into the various business sectors, the digital economy in Nigeria is expected to continue to grow and it will attract numerous global players who must comply with the regulations.

Although there are some provisions on data protection or privacy in various legislations such as the Cyber Crimes Act, it is the NDPR that explicitly provides for the minimum data security required in Nigeria for the collection, storage, processing, management, operation and technical control of personal data. It may also be Nigeria's strictest and most far-reaching data protection law, placing strict requirements on entities and stringent penalties if there is a default in compliance.

In light of the above, this paper seeks to examine and evaluate the Nigerian Data Protection Regulation (NDPR) 2019 and its implications on businesses who collect and process data of Nigerian residents. Transitioning from a state of affairs where there were no strict privacy law or data protection obligations on companies and institutions, compliance and enforcement of the NDPR may be an unyielding issue. Thus, the paper would review some of these challenges and proffer pragmatic solutions that can make the compliance and enforcement of the regulations more effective.

WHAT IS DATA PROTECTION

Personal data is any information, whether private, professional, or public, relating to a person. It is becoming increasingly difficult for people to retain ownership over their personal information in the online world, where large quantities of personal data are exchanged and transmitted instantly across the globe. This is where the protection of data comes in. Data protection refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it.[v] In short, a person should be able to decide whether or not, they want to share some information, who has access to it, for how long, for what reason, and be able to modify some of this information, and more.

Data protection is recognized as an important field of law, policy development and regulation. It combines elements of human rights and consumer protection and, in many international agreements and individual jurisdictions, data protection is considered a fundamental right[vi].

Data protection has always been motivated by a two-fold purpose, according to numerous commentators, which is: the protection of human rights and freedoms of individuals and, in particular, the fundamental right to data protection, on the one hand, and the achievement of the internal market, on the other, the free flow of personal data in this case[vii]. However, the Data Protection Regulation intends to protect private citizens against unjustified collection, storage, use and dissemination of their information.[viii]Data protection can be seen as a growing body of rules and standards to be taken into account by lawmakers in drafting legislation and by personal data controllers and processors. This growth is continuous, as new rules and

standards are called for every time new problems emerge due to new technological advances, such as the emergence of newer technologies and biometrics.[ix]

In certain countries, data privacy laws date back to the 1970s, reflecting concerns about the advent of computer and communication technology with its capacity to process vast quantities of data remotely. While considerably different regulatory approaches have been pursued by various national, regional and international initiatives, there is a remarkable degree of harmonization and coherence around the core principles which underpin them.[x]Popular concepts include the need to provide a compelling purpose, achieved either by agreement or other justification in consideration of conflicting public and private interest. Another central concept is the responsibilities relating to the accuracy of the personal data being processed, which require the data to be reliable, accurate and up-to-date. For both the processing subject and the processor, compliance with this principle should be mutually beneficial.

Since the 1960s and the expansion of information technology capabilities, business and government have been storing this personal data in databases.[xi]Databases can be searched, updated, cross-referenced and shared with other organisations worldwide with their data. When data collection and analysis became popular, individuals began raising questions about their data once they provided it. Who had the right to have the data accessed? Was it properly preserved? Was it being compiled without their knowledge and disseminated? Can it be used to discriminate against other human rights or abuse them? Via various national and international consultations, data protection principles have been developed from all these concerns, and in the face of increasing public concern. The German region of *Hesse* passed the first law in 1970[xii], while the US Fair Credit Reporting Act 1970 also contained elements of data protection[xiii].Around the same time, the UK set up a committee to investigate risks from private firms, which reached similar conclusions. Soon afterwards, national laws on data protection were enacted by various parliaments, starting with Sweden, Germany, and France. More than 142 countries have implemented different models or regimes of data protection legislation as of January 2018.[xiv]

Over time, regional legal frameworks were also adopted. In 1980, the Organisation for Economic Cooperation and Development (OECD) developed its guidelines, which included

'privacy principles'[xv]; shortly afterwards, the Council of Europe's Convention for the Protection of Individuals concerning Automatic Processing of Personal Data entered into force - this was modernised in 2018.[xvi]

In the early 2000s, protection of data came to a head, when technology firms such as Google and Facebook were regularly reported by the press, because of contentious privacy and data protection practices. In 2010 Facebook acknowledged, following a Wall Street Journal report, that its most common play applications exchanged personal data from users and the details of interactions with external businesses who used advertising information. The report suggests tens of millions of users were affected by the data breach, including those who have enabled the strictest protection in Facebook[xvii].

All data protection framework may have their limitations but they do provide an important and fundamental starting point to ensure that strong regulatory and legal safeguards are implemented to protect personal data.[xviii]A strong data protection framework can empower individuals, restrain harmful data practices, and limit data exploitation. It essential to provide the much-needed governance frameworks nationally and globally to ensure individuals have strong rights over their data, stringent obligations are imposed on those processing personal data (in both the public and private sectors), and strong enforcement powers can be used against those who breach these obligations and protections.

Consequently, experts and profession in data security and management have argued that an effective and fair Data protection framework or regime should ensure that there are limits on the collection of personal data, and it should be obtained by lawful and fair means, as well as being done transparently[xix].

THE NIGERIAN DATA PROTECTION REGULATION 2019

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

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

In addition to the above powers, NITDA released its Nigeria Data Protection Regulation (NDPR) for the protection of personal data of both Nigerians and non-Nigerians in Nigeria on 28 January 2019. This Regulation was the first true legal instrument for data protection in Nigeria and, in some ways, a mirror of the General Data Protection Regulation of the European Union (EU) (GDPR).

NDPR empowers NITDA to register and license the Data Protection Compliance Organization (DPCO) to track, inspect, train and provide data protection compliance advisory services on its behalf[xxi]. However, the DPCOs will be subject to Regulations and Directives of NITDA issued from time to time.

Furthermore, the NDPR applies to all organizations regardless of the type of the organization, whether commercial, non-profit organizations or non-governmental organisations (NGOs). The NDPR imposes criteria on any organisation, irrespective of its geographical location or purpose, for the means of selecting or identifying details of individual citizens residing within Nigeria[xxii]. NDPR also notes that the principles of processing must be the same for all data subjects whose information is collected by any entity regardless of the position of the data subject, thereby prohibiting organisations or businesses, using data from Nigeria, from imposing a double standard.[xxiii]According to Art. 1.2, the NDPR refers to the collection of personal data of natural persons, irrespective of nationality or residency. Consequently, an individual who lives outside Nigeria and who visits Nigeria is deemed to be a 'data subject' under the scope of this provision, given that his or her data is processed during that visit to Nigeria. The NDPR would for instance secure the personal information of a visitor to Nigeria who lives in Italy. The Italian citizen may order garments from his hotel room in Nigeria online. In the meantime, the Swedish website processes her or her details from its server in Sweden.

Nonetheless, the controller will have to comply with the NDPR regulations.[xxiv]Like the GDPR, the NDPR makes it very clear that a data subject's nationality or residency is meaningless in deciding if the NDPR is applicable. The simple evidence that the person is physically present in Nigeria when processing takes place seems to be the deciding factor.[xxv]

Owing to the increased flow of cross-border data, the concept of territoriality in private international law is losing its significance. A rigid interpretation of the concept of territoriality does not operate in the context of the Internet[xxvi]. Although it is relatively straightforward to locate activities in the physical world, it can be impossible to locate activities taking place on the internet. This is because there are no territorial frontiers on the internet, and its geography is interactive. To decide which court has the authority and which rule is valid, connecting factors are given by private international law. The rules regulating the law in effect and the authority of private international law depend on the location of activities and individuals. As a consequence, in an online setting, the connecting factors commonly used in private international law to assess the law and jurisdiction applicable are not always relevant.[xxvii]

The key persons under the regulation are[xxviii]:

(1) The Data Subject - the person whose identity is or may be revealed from the data;

(2) The Data Controller – any person/corporate who determines the purpose and manner for processing the data; and

(3) The Data Processor - any person/corporate who processes the data in any form e.g. storing, reproduction, modification etc.

The NDPR mandates organizations handling data to:

1) Publicize their data protection policies within three months from the date Regulation was issued.[xxix]

2) Conduct a data protection audit within six months from the date of the Regulation and thereafter submit a copy annually to NITDA[xxx]

3) Designate a Data Protection Officer in the organisation or outsource Data Protection to a competent person/firm[xxxi]; and

4) Submit an annual report of its data protection audit not later than the 15th of March every year and the report should cover the period of 12 (twelve) months preceding the date of submission[xxxii].

Besides, the NDPR requires data controllers to implement appropriate protection systems in their custody to protect all personal data[xxxiii]. In compliance with this provision, data controllers are expected to maintain and publish an NDPR-compliant data protection policy and to constantly train and build the ability of data protection and privacy procedures for staff members[xxxiv].NITDA is also expected to set up an Administrative Redress Panel to resolve and redress cases of a violation[xxxv]. This does not, however, derogate from the freedom of the data subject to obtain relief before a competent court.

Personal Data and Processing Personal Data

The definition of personal data in both the NDPR has three main aspects: (a) it is 'any information'; (b) it relates to a 'natural person'; and (c) that person must be 'identified or identifiable'. In the context of technological development, the identifiability factor proves to be the most relevant. A natural person can be considered 'identified' when he or she is distinguished from all other members of a group. In other words, if data can only be connected to a group of individuals as opposed to a single individual, it would generally not be personal.[xxxvi] Accordingly, a natural person is 'identifiable' when that person has not yet been identified but identification is nevertheless possible.

Personal Data according to Article 1.3 of the NDPR 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 name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other

> unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;

The incorporation of online identifiers and genetic factors shows that regulators have taken into account technological advances. Also, the physical object information may qualify as personal data if it can be connected to an individual.[xxxvii] In turn, identifying items that belong to individuals will contribute to a set of data on preferences, behaviour, and interests. When these data are linked to data from other objects, new information that is previously unknown even to the individual himself can be generated. Also, collecting data on objects can allow people to be more easily identifiable. Online device identifiers, applications such as cookie identifiers or radio frequency identification tags may leave traces that may be used to create profiles of individuals when combined with other information obtained by servers, leading ultimately to their identification.

Processing is defined in the same Article 1.3 as follows:

> "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Thus, from the literal interpretation of the NDPR, "processing" means everything from data collection, storage, encryption, use and alteration to its ultimate destruction. It is necessary to remember that 'processing' does not require the controller or processor to take action on the data in this context; only the storage or archiving of the data counts as processing.

All organizations process some personal data; at the very least employee data must be processed. But, likely, some data of customers, members, affiliates or other natural persons is processed. Even in a situation where organizations only co-operate with each other, contact information of the representatives of that organization must be processed. All processing

activities must be lawful and transparent[xxxviii], and data cannot be stored longer than necessary[xxxix].

The NDPR imposes liability on parties transacting on personal data to ensure the other party is accountable to regulators of data protection and does not act in violation of the rights of the data subject.[xl] Every Data Processor or Controller shall be liable for the actions or inactions of third parties which handles the personal data of Data Subjects under the regulation.[xli]

Legitimacy of Data Processing

Under the NDPR, all organizations involved in the processing of personal data must be able to identify and inform the data subject of the legitimate reason they are processing the data on. This information should be available in the privacy statement that is easily available to the data subject. Article 2.2 provides the lawful reasons for processing personal data which are as follows:

(a). The data subject has given his/her consent

(b). Performance of a contract the data subject is a party to

(c). The legal obligation of the controller

(d). Vital interest of the data subject or another person

(e). Public interest and official authority.

If no legitimate reason for data processing can be shown by the controller or processor, the processing is considered illegitimate in which case the data subject can exercise their right to restrict the use of their data[xlii] or complain to NITDA[xliii].

Transparency Principle and Informing the Data Subject

As stated in the NDPR all processing activities must be legitimate and transparent to the data subjects whose personal information is being processed[xliv]. This includes that information on the collection, storage and all other processing activities must be easily accessible and presented in plain language for the data subject.[xlv] Specifically, the data subjects must be made aware of the following:[xlvi]

(a). the identity and the contact details of the Controller;

(b). the contact details of the Data Protection Officer;

(c). the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d). the legitimate interests pursued by the Controller or by a third party;

(e). the recipients or categories of recipients of the personal data, if any;

(f). where applicable, the fact that the Controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Agency;

(g). the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(h). the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability;

(i). the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(j). the right to lodge complaints with a relevant authority;

(k). whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(l). 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 consequences of such processing for the Data Subject;

(m). Where the Controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the Data Subject before that further processing with information on that other purpose and with any relevant further information; and

(n). where applicable, that the Controller intends to transfer personal data to a recipient in a foreign country or international organisation and the existence or absence of an adequacy decision by the Agency.

Consent

Consent must be freely given and informed[xlvii]. Therefore, every data subject, i.e. persons, must be aware of the reasons why his personal data are being collected.[xlviii] The data subject must permit without duress[xlix] and be able to withdraw his or her consent at any time without repercussion for it to be considered freely given[l]. All request for consent by data controllers must be in an intelligible and easily accessible form, using clear and plain language.[li] The NDPR further provides that before a data controller transfers any personal data to a third party, he must obtain the consent of the data subject.

Data Subject's Rights

In the GDPR, the data subjects will have extended rights to their data. These include the right to object or limit to the use of data[lii], right to access all data[liii], right to receive data in a readable format[liv], right for rectification[lv], right to restrict the use of their personal data[lvi],right to data portability[lvii] and the right to be forgotten[lviii].

Furthermore, where personal data are transferred to a foreign country or an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards for data protection in a foreign country. The Data Subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including using and providing a supplementary statement.[lix]

Data Breach Notification Obligation

Ordinarily, the NDPR mandates all data controllers and processors to develop security measures to protect personal data in their custody. Such measures include protecting systems from hackers, setting up firewalls, storing data securely with access to specifically authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff. But no matter how watertight, there may be instances where a breach of the security can occur. In such situations, the NDPR outlines the

obligations of the data controller and data processors to the data subject as well as actions that should be taken.

Firstly, a personal data breach is defined in Article 1.3 of the NDPR as follows:

> ...a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The definition provided by the NDPR covers both accidental and intentional cases of a data breach and the notification obligation extends to even accidental deletion or corruption of a data set in addition to the more obvious theft, misuse, interception and so forth.

Documentation

Documentation is a key requirement stated in the NDPR and it even goes as far as naming some of the required documents and they are necessary for demonstrating compliance in case of a complaint, incident or audit. The regulation states that the data controller must be able to demonstrate such items as consent given by the data subject[lx] and data processing activity log[lxi]. The required documentation may be executed in electronic form or with the help of privacy software, which may be a cost-effective way to fulfil the requirements of NDPR for a small organization.[lxii] Recently increasing amounts of specialized software for mapping personal data, consent management tools have been developed and brought to market.

Transfer of Data to Third Party Countries

The NDPR envisages cases where data may have to be transferred to third party countries or international organisations[lxiii]. According to Article 2.11 of the regulation, any transfer of Personal Data in this regard is subject to the supervision of the Honourable Attorney General of the Federation (HAGF) who would typically consider the reflection of Nigerian laws and approach to data protection in these foreign territories. A transfer may also be approved if NIDTA concludes that the third-party destination of the data ensures adequate protection.

If neither NIDTA nor the HAGF is certain as to the adequacy of safeguards for data processing in a foreign country or an international organisation, the data controllers may still be able to process and transfer data provided anyone of set conditions are met.[lxiv]

Increased Exposure and Attribution of Personal and Corporate Liability for Breach

The NDPR provides that companies may only store, use, transfer or process information subject to the minimum standards stipulated above. Garrulous privacy policies which are difficult to access or understand will not meet the requirement of prior consent are to be reviewed[lxv]. Additionally, it is not enough to state that the responsibility for protecting personal data is contracted to a third party, it is important to note that any such transfer of the responsibility must be governed by a contract which meets the minimum requirements. The NDPR specifically defines parties to include directors, shareholders, servants and privies of the contracting party[lxvi]. Accordingly, the distinction between legal and natural persons to limit due diligence is irrelevant.

More importantly, companies who by their services have to mill through data to provide reports or use data in the course of product production have to confirm that personal information controlled or transmitted in such circumstances are sourced without breach of data protection requirements outlined above to prevent exposure to business crippling fines.

Penalties and Fines

In addition to any possible criminal liability, the NDPR provides sanctions for breach of data privacy rights. Where the breach is by a Data Controller dealing with over 10,000 Data Subjects, the penalty would be 2% of the Data Controller's Annual Gross Revenue for the preceding year or 10 million Naira, whichever is greater[lxvii]. For a Data Controller dealing with less than 10,000 Data Subjects, the applicable fine would be 1% of the Data Controller's Annual Gross Revenue for the preceding year or N2million naira, whichever is greater[lxviii].

CHALLENGES TO THE ENFORCEMENT OF THE REGULATIONS

One of the reasons for the fanfare that the Regulation has generated in some quarters is the expectation that the said NDPR could make Nigeria compliant with (at least) minimum data protection standards. This expectation is probably heightened by the fact that the new Nigerian law is also tagged a 'Regulation' just like the 'General Data Protection Regulation'. Unfortunately, this may not necessarily be the case. As mentioned in earlier parts of this article, the right to data protection is a right which is not expressly listed in the traditional body of

human rights known or recognized under Nigerian law and NITDA's efforts in drafting this legal document must be saluted in the light of this fact. However, a question that begs to be answered is whether the NDPR is capable of making Nigeria (at least minimally) data protection compliant[lxix].

It would appear that a lot of attention has not been given to the fact that the Regulation is subsidiary legislation drafted by NITDA (an agency of the executive arm of government) according to powers it was granted under the NITDA Act. Therefore, should there be a conflict between another Act of Parliament and the Regulation that Act of Parliament will prevail even though it conflicts with the Regulation? A practical example of an Act of parliament that may conflict with the Regulation (and would be given precedence and priority over the Regulation) is the Nigerian Cyber Crimes Act[lxx] which provides for retention schedules, the release of personal data according to court orders, data interception by the government through technical means, statutory fines etc. and the Nigerian Cyber Crimes Act (being an act of parliament) takes precedence over the NDPR (subsidiary legislation). Therefore, this has the effect of watering down the potency and applicability of the NDPR and is an argument in favour of the proposition that the regulation's impact in practice may be very limited.

One of the critical issues that the NDPR has not addressed overtly is the question of which agency will function as a data protection supervisory authority. From the language of the Regulation, it would appear that NITDA has appointed itself as the data protection supervisor, the regulation in another breath gives some supervisory powers to the Attorney General of the Federation in respect of data transfers outside Nigeria. The explanatory memorandum of the NITDA Act (which is the Act of parliament which regulates the affairs of NITDA) provides, among other things, that NITDA is established to plan, develop and promote the use of Information technology in Nigeria. The writer argues that in the light of the purpose for which NITDA has been established, the same body cannot be saddled with functioning as a data protection supervisory authority and there is the need to have an independent body whose sole task will be to function as a data protection supervisory authority for Nigeria.

Another challenge that the NDPR may have to contend with is the authority of NITDA to enforce the Regulation particularly the enforcement of the fines that have been listed in the said

Regulation. Being subsidiary legislation, NITDA, in the opening paragraph of the Regulation, traces the legal justification for drafting the Regulation to Section 6(c) of the NITDA Act which provides among other things that "NITDA shall develop Regulations for electronic governance and monitor the use of electronic data interchange…" It is arguable that at no point has the legislature delegated powers to charge fines to NITDA thereby making the charging of fines *ultra vires* and beyond the powers so vested by the legislature. The courts have held in quite many cases that the actions of a government official should not exceed the powers vested in the said authority[lxxi]. In applying this principle to the charging of fines by NITDA, it is arguable that while NITDA is authorized "to develop regulations for electronic governance", it is not authorized to charge fines and it may only take one legal action to render the provisions on fines null and void. It must also be noted that the Regulation can only be applied to companies dealing with IT and the importation of technology following the powers granted to NITDA under the NITDA Act. NITDA may therefore not have the powers to enforce the Regulation against banks (for instance) who will be subject to the supervision of the Central Bank of Nigeria.

A potential clog in the wheel of the NDPR and its attempt at data protection compliance in Nigeria is the unanswered question of whether the regulation will apply about personal data processing carried out by the government and its agencies. Curiously, the Regulation does not make any mention of processing activities carried out by the government.

The right to data portability is also a unique demand for NDPR. A person has rights to get all his/her personal data in a common structured format and then transfer this data to other register controller's systems. One aspect of this data portability is that a person has rights to transfer the data directly from one register controller to another if technically possible. The right to data portability does not mean that register controllers or processors should design and implement compatible systems. When the systems are different, the personal data can be transferred e.g., using external memory storage and then loading it to another register controller's system.[lxxii] Another challenge is that not all data can be transported to another controller's system. The example application contains e.g. contracts between data controllers and consumer customers. The data is important from a business point of view to a data controller and it has a so-called business purpose for the processing and storing it. The example application has been built to

provide e.g., contract data as PDF files, which can be given to the customers when needed. Users might have qualifications, e.g., certifications for dangerous work. The earlier mentioned certifications are sometimes a person's data and can be considered to be transported between different companies. A typical situation is e.g., when a contractor rents its employees to another company's projects. Naturally, there should be then a feature for this kind of data portability, because it will simplify trading employees between projects.

One responsibility for register controllers is to notify registered persons of data breaches the data of which has been leaked. This responsibility is missing in the NDPR. The right is in force if a breach causes great risks for an individual's rights and freedom. The aforementioned risks are, for example, identity thefts, credit card frauds or other criminal activities. The notification is not compulsory if the leaked personally identifiable information was encrypted and encryption keys were not leaked. An organization can use social media for informing of the data breach if otherwise, it might cause too big a load of work.[lxxiii]

CONCLUSION

With the rise of emerging communication technologies in recent decades, more focus has been given to the debate regarding data security and privacy. An increasing number of people are particularly worried about the processing of personal data by big technology companies. If the complexity of the problem becomes more complicated, they fear the exploitation of new and emerging technologies. Thus, policymakers were required to enable laws, which protect the privacy of the citizens. Regarding Nigeria, the first instrument concerning this field is the Data Protection Regulations 2019. The NDPR seeks to protect the rights and freedoms of individuals when processing personal data, as well as to control the processing of data within Nigeria and data transfers to third countries or foreign states, according to the recital to the Regulations. It applies to all businesses and organisations, whether or not they are established or operating in Nigeria, that store, manage or process Nigerian data. The NDPR has both extra-territorial and national jurisdictions, as does the EU GDPR.

Generally, the main goal of the new legislation is to protect Nigerian citizens from organizations that use personal data unlawfully. Sanctions for data breaches have also been

increased, and organizations have new requirements e.g., for data breach notifications. The organizations failing to comply with the NDPR will face penalties of a fixed sum or percentage of their global annual turnover. The new NDPR rules should also help organizations to prepare correct policies and procedures to handle cybersecurity incidents. Also, NDPR will change the way organizations process and store personal data. As noted earlier, the rights of Nigerians are to be extended and the NDPR applies to all organizations that process personal data of Nigerians.

While it is in its early stages of application, it is expedient for companies in Nigeria to begin to outline the protocol for data protection and adopt technology that enables seamless incorporation of protective measures into their operations. Organizations must consider what personal data they process and how they should protect it. Even organizations outside Nigeria but operating in Nigeria territory or deals with Nigerians must apply the requirements of the regulation. Furthermore, every organization must handle personal data lawfully and transparently. Besides, the processing of personal data must have a real purpose. When personal data is no longer required, organizations should remove it.

REFERENCES

1. Arthur C, "iPhone Keeps Record of Everywhere You Go" *The Guardian* (April 20, 2011) <https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>

2. Banisar D, "National Comprehensive Data Protection/Privacy Laws and Bills 2019" (*SSRN*, November 30, 2019)

3. Brkan M, "Data Protection and Conflict-of-Laws: A Challenging Relationship" (2016) 2 European Data Protection Law Review (EDPL) 324

4. Brook C, "Data Controller vs. Data Processor: What's The Difference?" (*Digital Guardian*, August 11, 2020) <https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference>

5. Bygrave L, "Digital Rights Management and Privacy - Legal Aspects in the European Union" in Eberhard Becker and others (eds), *Digital Rights Management : Technological, Economic, Legal and Political Aspects* (Springer Berlin Heidelberg 2003)

6. De Hert P and Czerniawski M, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context" (2016) 6 International Data Privacy Law 230

7. De Hert P and Gutwirth S, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action" in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Science 2009)

8. Fioretti J, Nasralla S and Murphy F, "Max Schrems: The Law Student Who Took on Facebook" *Reuters* (October 7, 2015) <https://www.reuters.com/article/us-eu-ireland-privacy-schrems/max-schrems-the-law-student-who-took-on-facebook-idUSKCN0S124020151007>

9. Fruhlinger J, "Social Engineering Explained: How Criminals Exploit Human Behavior" (*CSO Online*, September 25, 2019) <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>

10. Gellman R, "Fair Information Practices: A Basic History" (2014)

11. Greenleaf G and Cottier B, "2020 Ends a Decade of 62 New Data Privacy Laws" (2020) 163 Privacy Laws & Business International Report 24

12. Gutwirth S, Leenes R and De Hert P, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

13. Hallinan D, "Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?" (2019) 5 European Data Protection Law Review 293

14. Hon WK, Millard C and Walden I, "The Problem of 'Personal Data' in Cloud Computing - What Information Is Regulated? The Cloud of Unknowing, Part 1" (2011) 1 International Data Privacy Law 211

15. Hoofnagle CJ, Van der Sloot B and BorgesiusFZ, "The European Union General Data Protection Regulation: What It Is and What It Means" (2019) 28 Information & Communications Technology Law 65

16. Hustinx P, "Data Protection in the European Union" (2005) 2 Privacy &Informatie 62

17. Jay R and others, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017)

18. Kuner C and others, "The Language of Data Privacy Law (and How It Differs from Reality)" (2016) 6 International Data Privacy Law 259

19. Kurth HA, "Nigeria Issues New Data Protection Regulation" (*Privacy & Information Security Law Blog*, April 5, 2019)

20. Mäkinen J-S, "The Background and Nature of Data within EU Data Protection Law with Reference to New Technology" [2016] Oikeus, tietojaviesti: Viestintäoikeudenvuosikirja 2015 103

21. Masse E, "Data Protection: Why It Matters and How to Protect It" (*Access Now*, January 25, 2018) <https://www.accessnow.org/data-protection-matters-protect/>

22. Peralata E, "As Apple Faces Lawsuit, Microsoft Says Windows Phones Collect Data, Too" (*NPR*, April 26, 2011) <https://www.npr.org/blogs/thetwo-way/2011/04/26/135743908/windows-phones-collect-data-too-says-microsoft?sc=tw?sc=tw>

23. Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (Privacy International 2018)

24. Reed C, *Internet Law: Text and Materials* (Cambridge University Press 2004)

25. RiccardiJL, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?" (1983) 6 Boston College International & Comparative Law Review 243

26. Salami E, "The Nigerian Data Protection Regulation 2019: Overview, Effects and Limits" (*datenschutz-notizen | News-Blog Der Datenschutz Nord Gruppe*, April 2, 2019) <https://www.datenschutz-notizen.de/the-nigerian-data-protection-regulation-2019-overview-effects-and-limits-3522349/>

27. Steel E and Fowler G, "Facebook in Privacy Breach" *Wall Street Journal* (October 18, 2010) <https://www.wsj.com/articles/SB10001424052702304772804575558484075236968

28. Svantesson DJ, *Private International Law and the Internet* (Kluwer Law International BV 2016)

29. Tikkinen-Piri C, Rohunen A and Markkula J, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies" (2018) 34 Computer Law & Security Review 134

30. UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (United Nations 2016)

ENDNOTES

[i] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Accessed: February 4, 2021).

[ii]David Banisar, "National Comprehensive Data Protection/Privacy Laws and Bills 2019" (*SSRN*, November 30, 2019) https://ssrn.com/abstract=1951416accessed February 4, 2021.

[iii]Full text of the NDPR can be found here: https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf

[iv]Hunton Andrews Kurth, "Nigeria Issues New Data Protection Regulation" (*Privacy & Information Security Law Blog*, April 5, 2019) https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/accessed February 4, 2021.

[v]Estelle Masse, "Data Protection: Why It Matters and How to Protect It" (*Access Now*, January 25, 2018) <https://www.accessnow.org/data-protection-matters-protect/> accessed February 4, 2021.

[vi]In the EU, data protection and privacy is treated as a fundamental human right (Article 16 of the Treaty on the Functioning of the European Union (TFEU) as well as to Article 8 of the Charter of Fundamental Rights of the European Union)

[vii]Jenna-Sofia Mäkinen, "The Background and Nature of Data within EU Data Protection Law with Reference to New Technology" [2016] Oikeus, tietojaviesti: Viestintäoikeudenvuosikirja 2015 103 https://researchportal.helsinki.fi/en/publications/the-background-and-nature-of-data-within-eu-data-protection-law-waccessed February 5, 2021; Lee Bygrave, "Digital Rights Management and Privacy - Legal Aspects in the European Union" in Eberhard Becker and others (eds), *Digital Rights Management : Technological, Economic, Legal and Political Aspects* (Springer Berlin Heidelberg 2003) p. 420.

[viii]Peter Hustinx, "Data Protection in the European Union" (2005) 2 Privacy &Informatie 62.

[ix]Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action" in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Science 2009) p. 3

[x]UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (United Nations 2016) p. 2 https://www.tralac.org/images/docs/9500/data-protection-regulations-and-international-data-flows-implications-for-trade-and-development-unctad-april-2016.pdfaccessed February 4, 2021.

[xi]Chris Jay Hoofnagle, Bart Van der Sloot and FrederikZuiderveenBorgesius, "The European Union General Data Protection Regulation: What It Is and What It Means" (2019) 28 Information & Communications Technology Law 65.

[xii]Datenschutzgesetz [Data Protection Act], Oct. 7, 1970, HESSISCHESGESETZ-UND VERORDNUNGSBLATT I; John Lee Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?" (1983) 6 Boston College International & Comparative Law Review 243, 247 https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1510&context=iclraccessed February 4, 2021.

[xiii]Robert Gellman, "Fair Information Practices: A Basic History" (2014) https://bobgellman.com/rg-docs/rg-FIPshistory.pdfaccessed February 5, 2021.

[xiv]Graham Greenleaf and BertilCottier, "2020 Ends a Decade of 62 New Data Privacy Laws" (2020) 163 Privacy Laws & Business International Report 24 https://ssrn.com/abstract=3572611accessed February 4, 2021.

[xv] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[xvi] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 128th Session of the Committee of Ministers, 18 May 2018, CM (2018)2-final. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

[xvii]Emily Steel and Geoffrey Fowler, "Facebook in Privacy Breach" *Wall Street Journal* (October 18, 2010) <https://www.wsj.com/articles/SB10001424052702304772804575558484075236968> accessed September 2, 2020.

[xviii]Christopher Kuner and others, "The Language of Data Privacy Law (and How It Differs from Reality)" (2016) 6 International Data Privacy Law 259 https://academic.oup.com/idpl/article-pdf/6/4/259/9598016/ipw022.pdfaccessed February 6, 2021.

[xix]Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (Privacy International 2018) p. 15 https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdfaccessed February 4, 2021.

[xx] Section 6(c), National Information Technology Development Agency Act

[xxi]Art. 3.14, Nigerian Data Protection Regulation 2019

[xxii]Art. 1.2(a)

[xxiii]Art. 1.2(c)

[xxiv]MajaBrkan, "Data Protection and Conflict-of-Laws: A Challenging Relationship" (2016) 2 European Data Protection Law Review (EDPL) 324, 339 https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=58&id=&page=accessed February 6, 2021.

[xxv]Rosemary Jay and others, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017) p 74

[xxvi]Serge Gutwirth, Ronald Leenes and Paul De Hert, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) pp. 8-9

[xxvii]Chris Reed, *Internet Law: Text and Materials* (Cambridge University Press 2004). pp. 217-219

[xxviii]Art. 1.3, NDPR

[xxix] Art. 3.1

[xxx] Art. 3.1.5

[xxxi] Art. 3.1.2

[xxxii] Art. 3.1.7

[xxxiii] Art. 2.6

[xxxiv] Art. 3.1.3

[xxxv] Art. 3.2

[xxxvi]Bygrave (n. 7) p. 426

[xxxvii]W Kuan Hon, Christopher Millard and Ian Walden, "The Problem of 'Personal Data' in Cloud Computing - What Information Is Regulated? The Cloud of Unknowing, Part 1" (2011) 1 International Data Privacy Law 211 https://academic.oup.com/idpl/article-pdf/1/4/211/2179526/ipr018.pdfaccessed February 4, 2021.

[xxxviii] Art. 2.1(1)(a)

[xxxix] Art. 2.1(1)(c)

[xl] Art. 2.1(2) & (3)

[xli] Art. 2.4(b)

[xlii] Art. 2.13.10

[xliii]Art. 3.2.1

[xliv]Art. 2.13.6

[xlv] Art. 2.13.12

[xlvi] Art. 2.13.6

[xlvii]Art. 1.3

[xlviii]Art. 2.3(i)

[xlix]Art. 2.3(ii)

[l]Art. 2.3(ii)(c)

[li]Art. 2.3(ii)(b)

[lii] Art. 2.8

[liii] Art. 2.13.1

[liv]Art. 2.13.12

[lv] Art. 2.13.11

[lvi] Art. 2.13.10

[lvii] Art. 2.13.14

[lviii] Art. 2.13.8

[lix]Art. 2.13.7

[lx]Art. 2.3(ii)(a)

[lxi] Art. 2.1(1)

[lxii]Christina Tikkinen-Piri, Anna Rohunen and JouniMarkkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies" (2018) 34 Computer Law & Security Review 134 https://www.sciencedirect.com/science/article/pii/S0267364917301966accessed February 4, 2021.

[lxiii] Art. 2.11

[lxiv]Art. 2.12

[lxv]Art. 2.5

[lxvi] Art. 2.4

[lxvii] Art. 2.10(a)

[lxviii] Art. 2.10(b)

[lxix]Emmanuel Salami, "The Nigerian Data Protection Regulation 2019: Overview, Effects and Limits" (*datenschutz-notizen | News-Blog Der Datenschutz Nord Gruppe*, April 2, 2019) https://www.datenschutz-notizen.de/the-nigerian-data-protection-regulation-2019-overview-effects-and-limits-3522349/accessed February 4, 2021.

[lxx] Section 38-39 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015

[lxxi]*NOSDRA v. Mobil Prod. (Nig.) Unltd.* (2018) 13 NWLR (Pt. 1636) 334 where the Court of Appeal held that a regulatory agency cannot impose fines if the enabling Act does not empower it to do so

[lxxii]Dara Hallinan, "Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?" (2019) 5 European Data Protection Law Review 293 https://edpl.lexxion.eu/data/article/14695/pdf/edpl_2019_03-006.pdfaccessed February 5, 2021.

[lxxiii]Ibid.