GEPLAW Focus

GEORGE ETOMI & PARTNERS

A Monthly Publication of the George Etomi & Partners Editorial Team

Volume 15 Issue 5

DATA PROTECTION- A COMPARATIVE LOOK AT THE GDPR AND THE NIGERIAN REGULATIONS

OVERVIEW

With the advent of globalization, the protection of data of citizens has become as important as the protection of territories, the inability of a nation to protect its citizen's data could have dire consequences.

The content of “data” has evolved from mere personal bio data and phone numbers to a range of web data such as location, IP address, cookie data and Radio Frequency Identification (RFID) tags, and personal identifiable information like health and genetic data, biometric data, racial or ethnic data, political opinions, sexual orientation and so on.

Multinationals such as Google and Amazon have been able to successfully influence the decisions of consumers and end-users through the use of 'data analytics' tools. This is done by turning information on the various aspects of a consumer's life into computerized data and exploiting this data through targeted marketing and behavioral analysis, to conduct business. This exercise has come to be known as “Datafication”. Through this datafication process, the Company makes profit from merely collating information that was shared unwittingly or negligently by most consumers to market their products and make further revenue.

Data has become a highly profitable commodity to most major Companies, and it has ushered in the danger of exploitation, illegal mining and storage of data. The globalization of the Nigerian economy and business transactions means that information is readily available; in addition, most users are required to fulfill Know Your Customer (KYC) requirements stipulated by the law before they can utilise most platforms on the internet. However, there is a lack of a comprehensive, clear-cut regulation or law that effectively covers Data Protection in Nigeria. What

we have are several regulations by the public sectors and commissions that deal with consumer information, stating how the said information should be used and the penalties for wrong use.

Most global economies seem to have acknowledged the importance of protecting its citizens from being exploited via mis-use of their data and have been able to effectively collate comprehensive laws solely for data protection. South Africa for example has the Protection of Personal Information Act (POPIA) 2013, which has provided clear-cut guidelines on the processing and use of personal information. Most importantly, the European Union (EU) has recently revamped its data protection laws, passing the new General Data Protection Regulation, which ensures that the personal details of its citizens remain private and adequately protected, no matter where it is being used or by whom it is being accessed.

The EUROPEAN UNION (EU) GENERAL DATA PROTECTION REGULATION MAY 2018

The General Data Protection Regulation (GDPR) passed by the EU came into effect on 25th May 2018. The regulation mandates that companies that collect, store or process large amounts of information on residents of the EU, to be more transparent about what data they have, what they use it for and whom they share it with. The GDPR applies to any organization that collects, processes, manages or stores the data of European citizens, this includes most major online services and businesses that collect, process, manage or store data.

The GDPR, seeks to ensure that customers have control over the way their data is obtained and used by including safeguards to protect the rights of the consumers whose data the company has access to. The regulation achieves this by primarily expanding the scope of what companies must consider as personal data. Article 4 of the GDPR states “personal data” is any information relating to an identified or identifiable natural person, the regulation further defines an identifiable natural person as one who can be identified directly or indirectly by reference to an identifier such as a name, an identification number or other online identifier. The implication of this is that personal data could now include identifiers such as mobile device IDs and IP addresses.

The GDPR also requires companies to keep a close track of the data they have stored on EU residents, and specifies that where an EU resident decides that they need a company to delete his data, send him copies of the data, or correct an error in the data, the companies are mandated to comply. The regulation goes further to ensure that EU residents can object to specific ways in which a company may use their data and the residents can stipulate that such data would only be used for a particular purpose.

Where a data breach occurs in a company that collects or stores data of its customers, the regulation states that the said company must notify subjects of the data within 72 hours of the breach. This is something which very few companies currently practice. In the United States, for example, during the Equifax breach which exposed the personal information of millions of people in the US and

beyond, the company spent the first few weeks working to stop the attack and then planning how to deal with the damage before informing the public.

The GDPR clearly shifts the control of data into the hands of the consumers. The regulation recognizes the recent high value of data in the 21st century global economies and that data is the driving force of most major e-commerce companies, thus it seeks to regulate the way companies exploit such data, considering the fact that it is used for monetary gain.

The Current Situation in Nigeria

Unlike the European Union that has a single regulation governing the methods and control of data protection, Nigeria has no named Data Protection Act, dealing specifically with the protection of consumer data, rather, there are a number of laws which can be inferred to deal with data protection. They include;

1. Constitution of the Federal Republic of Nigeria 1999 (as amended) which governs the nation as whole;
2. Various industry specific regulations including;
    a. the Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission (NCC),
    b. National Information Technology Development Agency (NITDA) Guidelines on Data Protection,
    c. Cybercrimes (Prohibition, prevention Etc.) Act 2015, and
    d. The Nigerian Communications Commission Registration of Telephone Subscribers (RTS) Regulation 2011 amongst others.

These laws will be briefly discussed to highlight the role they play in attempting to regulate the use of data in Nigeria.

- Constitution of the Federal Republic of Nigeria 1999

Section 37 of the Nigerian Constitution provides that *"the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected"*. Asides from this law being the grundnorm and providing a general protection of fundamental human rights of citizens, there is no Law or Act of Assembly dealing exclusively with Data protection in Nigeria.

- Consumer Code of Practice Regulations 2007

This code was issued by the Nigerian Communications Commission, (NCC) to regulate the activities of telecommunication companies in Nigeria. It provides that all licensees (i.e. telecommunication service providers) must take reasonable steps to protect customer information against *"improper or accidental disclosure"* and must ensure that such information is securely stored. It also specifies that customer information must *"not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations"*.

- National Information Technology Development Agency (NITDA) Guidelines on Data Protection

The NITDA is the national authority responsible for planning, developing, and promoting the use of information technology in Nigeria. The agency, in performing this duty, issues guidelines which prescribe the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information.

The Guidelines regulate all organizations or persons that control, collect, store and process personal data of Nigerian residents within and outside Nigeria. However, the agency is only empowered to regulate a specific category of data commonly known as Personal Data or Object Identifiable Information (OII).

- Cybercrimes (Prohibition, prevention) Act 2015

This Act provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria including identity theft, cybersquatting, hacking and child pornography. It also allows the interception of electronic communication by way of Court Order; where there is reasonable ground to suspect that the content of any electronic communication is reasonably required for the purposes of criminal investigation or proceedings.

- Nigerian Communications Commission RTS (Registration of Telephone Subscribers) Regulation 2011

The Regulation provides some form of protection to data collected, collated, retained, and managed by telecommunication companies operating in Nigeria and independent registration agents in view of their obligations to collate and retain data of subscribers under the Regulation.

Section 9 of the Regulation provides that subscribers information contained in the Central Database shall be held on a strict confidentiality basis and no person or entity shall be allowed access to any subscriber's information that is on the Central Database except as prescribed by the Regulation.

There is a clearly a challenge with having various regulations seeking to perform similar functions or geared towards achieving the same goal. First, there exists a lack of clarity on the extent of protection; the effectiveness of each regulation is questionable due to multiplicity of duties and the overarching need to focus more on which agency/body has the legal rights to do what, rather than the actual implementation of the said laws.

A CASE FOR A GENERAL DATA PROTECTION REGULATION/LAW FOR NIGERIA

After a brief survey of all these regulations, it is clear that the law is still left wanting, questions can be raised as to which law takes precedence, aside the Constitution, or provides a comprehensive cover for customers and consumers. Nigeria is an emerging economy with immense potential, and for it to be on the same level of commerce with the developed economies, it is about time the nation takes the need for data protection and the effects of abuse of same on its citizenry very serious.

There is currently no comprehensive data privacy or personal information protection law in Nigeria that sets out detailed provisions on the protection of the privacy of citizens, or takes into cognizance the peculiarity of the internet and the unique approach it requires in assuring that it is a safe place for all players to freely carry on their business.

The European Union, by creating such a landmark regulation, has emphasized the need for the introduction of a sole Data Protection Regulation in Nigeria. This does not mean Nigeria should follow suit and churn out a new Bill for ascent by its Legislature, rather the GDPR could serve as an eye opener and conversation starter as to the extent to which data is being exploited and why it needs to be protected at all costs.

The use of the internet has evolved from just a platform to share information, to a largely commercial and social media platform and is gradually placing itself at the center of everything, and there is an admittedly urgent need for Nigeria to protect its citizens.

There are a good number of foreign-based companies and Nigerian startups whose businesses are built on collecting and collating customer data, this includes the telecommunication companies that have an inordinate amount of customers' personal information, due to Know Your Customer regulations, which are in place. Thus, without stringent laws or regulations properly put in place, Nigerians will continue to be exposed daily to exploitation by these companies and possible data breaches, further reducing the already wavering trust in e-transactions and the internet as a catalyst for development in the country.

Thus, it would be a valuable idea, like the EU, for Nigeria to come up with a regulation specifically modeled to fit the data operations in the country, rather than subscribing to already promulgated laws of other states.

CONCLUSION

The importance of data protection as a whole cannot be over-emphasized, especially in the era of the internet, where data is one of the most valuable assets of most e-commerce and social media companies. The European Union as a whole recognized the possibilities of exploitation by these big companies, and has acted accordingly by updating its data protection regulations, thereby ensuring that it covers all relevant areas on data management.

Nigeria on the other hand lacks a robust data management structure. Various government agencies, sector regulators and private companies collect and disseminate citizens' private data with little respect for their rights. Citizens have little or no control over what is collected, how it is used or disseminated and have no specified or clear course of action should their data be abused.

Whilst there are penalties for breaches and non-compliance with a lot of these regulations and laws, failure to comply with the data protection provisions are only treated as a breach of the Regulations rather than a violation of the individual subscriber's right to privacy, which is actionable at the instance of the affected subscriber. This limitation can be said to absolutely diminish the potency of the provisions and more importantly disregard the fundamental human rights of the consumer. This therefore increases the need for the Government, now more than ever, to promulgate a law in furtherance of the protection of citizens.

With the increasingly important role that data plays in the country's emerging digital economy, a single data protection law should be enacted into law that protects the citizens, giving them control over the use or non-use of their data and guarantying their rights to seek adequate redress in court for any breach occasioned by an act or omission of the companies or operators.