Nigeria Data Protection Regulation: A Step in the Right Direction



In an economy where it is said that data is the new oil, protecting data is as urgent as it is crucial. From employee record retention policies, to crime detection and patient data, personal data continues to play a prominent role in our evolution. This trend has necessitated promulgation of data protection legislation by governments across the world.

*The Nigeria Data Protection Regulation (the Regulation) recently enacted by National Information Technology Development Agency (NITDA/the Agency) is the most comprehensive generally applicable legislation on data protection in Nigeria. The Regulation became effective on the 25th day of January, 2019, and is brought pursuant to Section 6 (a) and (c) of the NITDA Act, 2007 which provides that;  
the Agency shall create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto; the Agency shall develop guidelines for electronic governance and monitor the use of electronic data interchange 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.*

The Regulation make wide-ranging provisions covering key aspects of the operations of personal data including data processing, lawful processing of personal data, procurement of consent, due diligence, data security, privacy policy, rights of data subjects, implementation of the regulation and penalties for non-compliance.

On this basis, it has now become imperative for existing and prospective local and global companies that utilize personal data (Data Controller and Data Processor defined below) of natural persons residing in Nigeria or residing outside Nigeria, but are Nigerian citizens, to conduct a review of the Regulation with a view to determining the extent of its applicability to their current operations. At the minimum, we expect that existing/prospective companies that utilize/intend to utilize personal data, will now begin to put compliance structures in place, possibly starting with the review and subsequently update of their data protection and privacy policies. I share below some of the key legal issues thrown up by the Regulation:

**Who the Regulation is applicable to?**  
The Regulation applies generally to Data Controllers and Data Processors. The Regulation has defined a Data Controller as a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed. Whereas the Data Processor though not expressly defined under the Regulation, but could be implied to mean a person or organization that processes personal data.  
The data processed must belong to an identifiable person, one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, referred to as the “Data Subject”.

The Regulation affects even those that hold and process large amounts of consumer data: technology firms, marketers, and the data brokers who connect them, but the hardest hit will be on firms whose business models rely on acquiring and exploiting personal data.

**Consent**

The primary objective of the Regulation is to ensure that personal data provided consistently by Data Subjects during the course of their daily interactions on the websites of Data Controllers, are lawfully consented to by the Data Subject before they are processed.  
The Regulation defines “Processing” as 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

From the foregoing, consent is a key issue that the Data Controller must take note of in processing of personal data. The Regulation provides that consent of the Data Subject consent terms must be clear, unambiguous and expressly obtained vide a written declaration or by electronic means; sometimes by ticking a box and stating that you agree to the terms and conditions/ privacy policy as a user of the website. It further provides that, personal data collected and processed must be for specific and lawful reasons, in accordance with the laid down procedures in the Regulation and with the express consent of the Data Subject.   
In the light of the above, due diligence must be applied in obtaining consent from a Data Subject, and no consent shall be given, sought or obtained for the propagation of wrongs actions, including but not limited to anti-social conducts, criminal acts, etc  
It is germane to state that, if consent is obtained for a particular purpose and the Data Controller intends to use the personal data for another purpose, prior to processing information, the Data Subject should be informed of the other purpose and any other relevant information.

**Right of Data Subjects’**

Users of Company websites now have some level of protection in terms of their personal data obtained from companies vide those websites. The Regulation makes provision for certain rights available to Data Subjects, and it includes;   
Right to withhold consent for certain uses of data;  
Right to request that they delete their information from websites altogether;  
Right to request for access to and rectification of personal data;  
Right to restriction of processing personal data concerning the Data Subject;  
Right to object to processing of personal data;  
Right to data portability.

**What Data Controllers need to do?**

The Regulation provides certain compliance procedures that Data Controllers need to comply with, upon issuance of the Regulation, they include;  
They shall within three (3) months of the issuance of this Regulation, make available their data policies to the public and it must be in compliance with the Regulation;

Availability of a Data Protection Officer as a member of the staff or outsourced to ensure adherence to the Regulation;

Training to improve capacity of the Data Protection Officers;

Within six (6) months after issuance of this Regulation conduct a detailed audit of its privacy and data protection practices. The information from the audit includes, but not limited to the policies and procedures of the organization for monitoring and reporting violations of privacy and data protections, policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

In addition to the aforementioned guidelines, Data Controllers shall also display a simple and conspicuous privacy policy on their websites or any other medium through which personal data is collected or processed. The Regulation makes provision for relevant details that make up the privacy policy.

**Enforcement/Penalties**

In a bid to ensure strict compliance of the privacy rights of Data Subjects, the Regulation provides for penalties in event of a breach of the data privacy rights of any Data Subject. The penalty is in two categories depending on the amount of Data Subjects the Data Controller deals with;  
a) in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million naira whichever is greater;   
b) in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million naira whichever is greater.

It further provides for the set-up of an Administrative Redress Panel that performs the following duties: Investigation of allegations of the breach of a provision in the regulation, Invitation of the alleged party to respond to the allegations and Issuance of administrative orders pending the conclusion of the investigation. However, the decision of the Administrative Redress Panel does not affect a Data Subject who intends to seek redress in court.

**Conclusion**  
The advent of the Regulation is a step in the right direction that would aid in providing some degree of safety to personal data. Although, nearly five (5) months after the Regulation became effective, protecting personal data still remains a difficult task, which requires an effective regulatory framework. In this regard, those tasked with the responsibility of ensuring maximum compliance of the Regulation, still have their work cut out for them in developing a data protection regime capable of attaining adequate security of data.