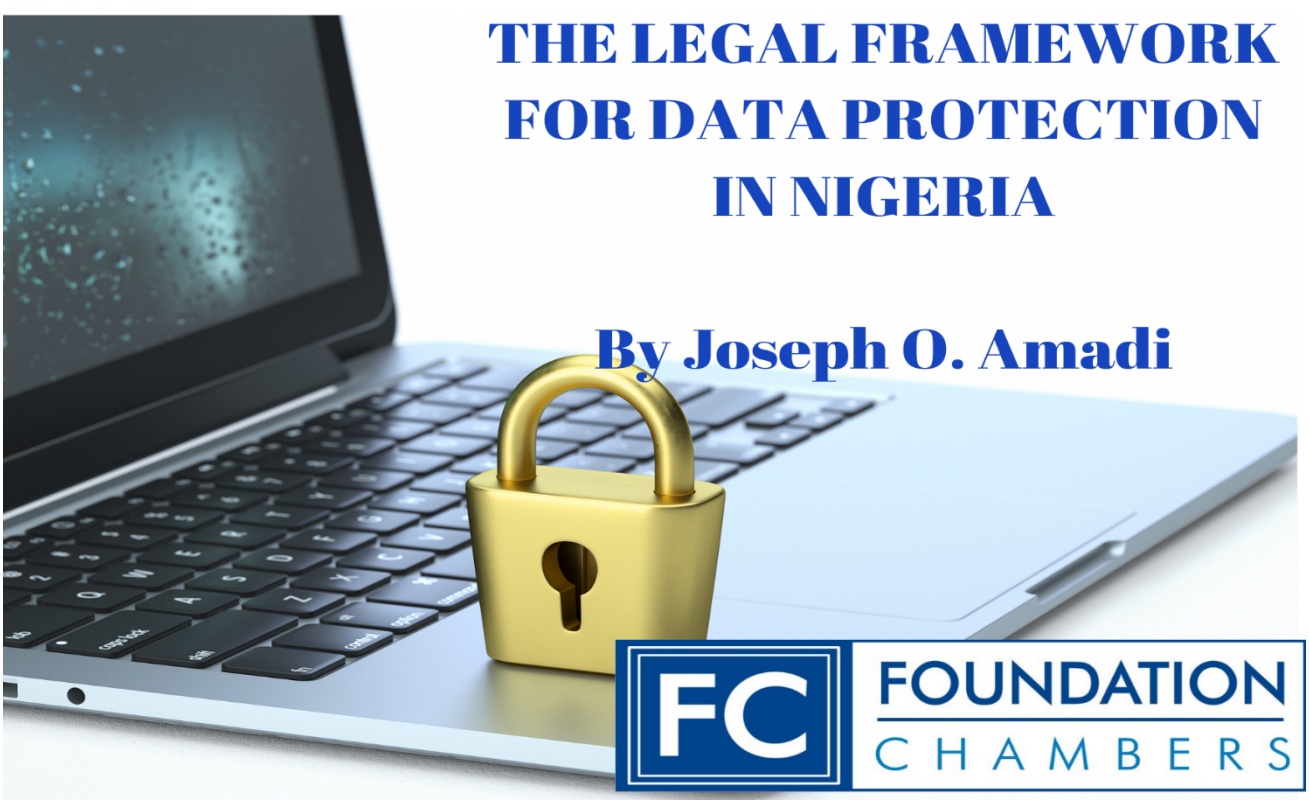

THE LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA
By Joseph O. Amadi

Introduction

On the 4th of February 2022, President Muhammadu Buhari approved the establishment of the Nigeria Data Protection Bureau (NDPB), which has as its main function, ensuring compliance with the Nigeria Data Protection Regulations 2019. The Bureau was created in furtherance of the Federal Government's National Digital Economy Policy and Strategy (NDEPS). The policy seeks to ensure that the basic individual rights to privacy and the protection of personal data are maintained by Data Administrators and Data Controllers.

With the creation of this new Bureau, many speculate on whether the Federal Government's actions are worthwhile, given the existence of the National Information Technology Development Authority (NITDA), which was created by virtue of the National Information Technology Development Act of 2007. The National Data Protection Regulations 2019 ('the Regulations'), was issued by the NITDA. The primary objectives of the Regulations are:

a. To safeguard the rights of natural persons to data privacy;
b. To foster safe conduct for transactions involving the exchange of Personal Data;
c. To prevent manipulation of Personal Data; and
d. To ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

The establishment of a new Federal Government Agency (NDPB) to enforce the Regulations issued by an already existing Federal Government Agency (NITDA) therefore seems to be a duplication of functions.

Under the Regulations, all Data Administrators and Data Controllers are required to act with utmost care in the collection, structuring, storage, adaptation, destruction of personal data, to ensure that there is no breach of personal data. According to the Regulations, a breach of personal data, can be said to have occurred, when there is 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.

Personal Data is defined by the Regulations to mean any information relating to an identified or identifiable natural person ('Data Subject'). The term 'identifiable natural person' refers to 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. An identifier can be a name, address, a picture, an email address, bank account details, posts on social networking websites such as Facebook, Twitter, LinkedIn, etc, medical records, and even other unique identifiers such as MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII), etc. Sensitive Personal Data, on the other hand, refers to data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

The Regulations also provide that, a simple but conspicuous privacy policy must be displayed in any medium through which personal data is being collected or processed such as a website or form. The Privacy Policy must state the following:

a. what constitutes the data subject's consent;
b. a description of collectable personal information;
c. the purpose of the collection of the personal data;
d. access, if any, by third parties to the personal data being collected; and
e. the purpose of such access amongst others.

There is no doubt that Data Security is an important aspect of data protection, especially with the rampancy of online hacking activities and internet fraud. It is therefore pertinent that Data Administrators and Controllers adopt top-notch data security apparatus and tools, such as defragmentation, password protection, system migration, database backups and data recovery, anti-malware software, amongst others, to secure personal data.

The Regulations also stipulate sanctions for default of its provisions. Breach of data privacy rights of a data subject attracts a penalty of 2% of the annual gross revenue for the preceding year of a data controller dealing with more than 10,000 data subjects, or a fine of Ten Million Naira, whichever is greater. A data controller dealing with less than 10,000 subjects, who infringes the data privacy rights of a subject is liable to pay 1% of its annual gross revenue for the preceding year or a fine of Two Million Naira, whichever is greater.

The Regulations further protect the rights of a Data Subject by stipulating that all information relating to the processing of personal data must be given to the Data Subject in a clear, concise and transparent manner. A Data Controller is, thus, expected to provide any information relating to the processing of personal data requested by a Data Subject, and such information is expected to be given to the Data Subject free of charge. According to the Regulations, the Data Subject has the right to request the following information from the Data Controller:

a. the reason for the processing of his or her personal data;
b. the recipients of such personal data;
c. the period for which the personal data will be stored;
d. whether the provision of the personal data is a statutory or contractual requirement;
e. whether such personal data will be transferred to a foreign country; and
f. the safeguards in place in that foreign country to ensure the protection of such personal data.

Under the Regulation, the Data Subject also has the right to request the deletion of the personal data provided to a controller where the data is no longer required or where consent to continue to keep such personal data is withdrawn by the data subject.

Also worth noting is the fact that the Regulations mandate all Public and Private Organisations in Nigeria, that control data of natural persons, to publish their data protection policy within three months of the issuance of the Regulations and conduct an audit of its privacy and data protection practices within six months of the issuance of the Regulations.

Conclusion

It is viewed that the creation of the NDPB is an unnecessary strain on sparce government resources, given the existence of the NITDA. There is a Data Protection Bill, 2020, which is currently being considered by the National Assembly, due to the various local and international conversations surrounding data privacy and protection. The Bill, when passed into law, will create a regulatory framework for the protection and processing of personal data, to safeguard the rights and freedoms of Data Subjects which are guaranteed under the Nigerian Constitution. The Bill also proposes the establishment of a Data Protection Commission to implement and monitor compliance. The creation of such a Commission will increase the number of Federal Government Agencies regulating the collection and protection of data in Nigeria. This increase will be rather unwarranted and superfluous as emphasis should be on strengthening of existing agencies rather than on creation of new ones.