ALP NG & Co.
AFRICA LAW PRACTICE NG & COMPANY
WWW.ALP.COMPANY

An Overview of the Legal Framework of Data Protection in Nigeria

Folajomi Fawehinmi

Introduction

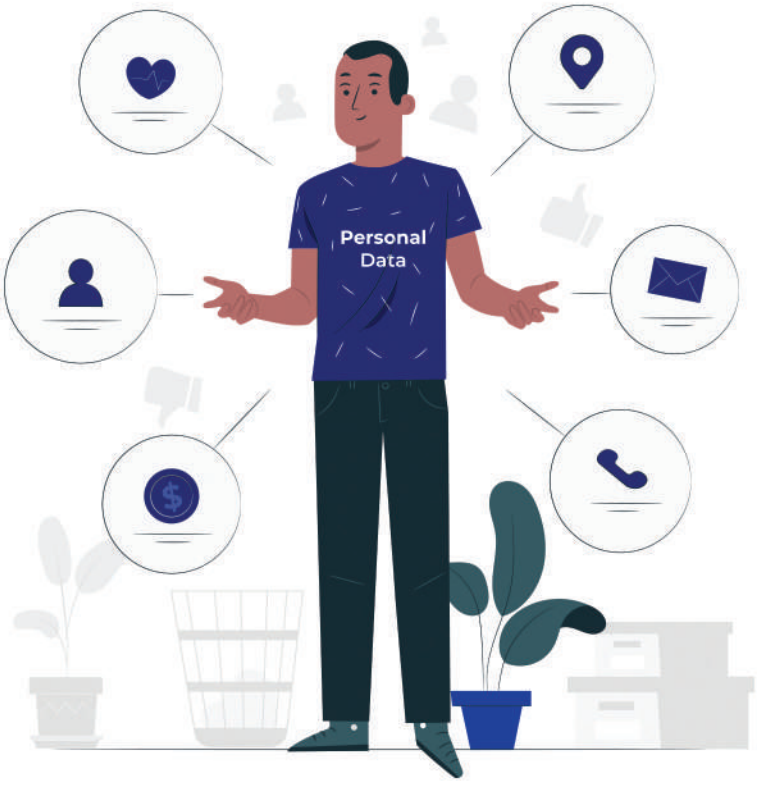
We live in an information age with a considerable proportion of global citizens now having easy access to internet enabled devices such as phones, tablets, laptops etc. Crucially, when we visit many online websites, we are often required to meet certain conditions precedent before we can access the services available on the website. For example, to create an email account on Hotmail, Yahoo, or Gmail, first time registration requires input from the would-be user of specific personal information including their personal address, phone number, date of birth, occupation and next of kin to form the basis of their security information. It is widespread practice that most websites which offer online services require personal data to create online accounts through which purchases, and other concurrent engagements can be undertaken online by the consumer. The average individual has access to many online platforms which require the use of personal data, such as social media accounts (e.g., Instagram and Facebook); email accounts; banking or finance applications; online vendor platforms such as Amazon and Jumia; betting agencies such as Betway, Naira Bet etc.

The widespread imposition on consumers to provide personal data prior to using online services on different platforms creates a very real risk of misuse of personal data which can lead to various infractions such as identity theft, illegal sharing of personal information with third parties and the rise in spam phone calls and emails when the personal data of users is illegally sold to companies which engage in electronic marketing. Across the international community, we have seen a spike in the number of jurisdictions enacting data protection regulations to protect the rights of citizens over their personal data, by raising the expected standards of data protection methods that businesses must have in place to protect the personal data of their users and to improve the ethical standards across board.

Defining Personal Data

Before examining the framework for legal protection in Nigeria, it is important to understand the legal meaning of the term "personal data." Personal data is defined by Nigerian Data Protection Regulations, 2019 as

> *"…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, 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, Personal Identifiable Information (PII) and others;*[1]



As can be noted from the above definition, personal data or information refers to a very broad category of information which can be exclusively linked to a specific individual or natural person.

[1] See Part 1.3 (XIX) of the 2019 Nigeria Data Protection Regulations

[2] Please note that this list is not exhaustive but merely identifies some other laws which contain provisions relevant to data protection in Nigeria.

Legal Safeguards

The protection of personal data is safeguarded by the constitutional right to privacy under section 37 of the Nigerian Constitution. This right has been further protected and provided for in the Data Protection Regulation 2019 ("NDPR" or "the Regulations") which is a subsidiary legislation made further to the National Information and Technology Development Agency Act 2007 (NITDA Act).
Other laws which contain ancillary provisions to cover data privacy protection include:

a. The Child Rights Act 2003.

b. Freedom of Information Act 2011.

c. The Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations 2011; and

d. Cybercrimes (Prohibition, Prevention Etc.) Act 2015.

e. Central Bank of Nigeria Consumer Protection Framework 2016.

f. The Credit Reporting Act 2017.

The NDPR

Under the NITDA Act, the National Information and Technology Development Agency is empowered to issue guidelines and policies for the purpose of monitoring the use of electronic data exchange. The NDPR regulations were created by the National Information and Technology Development Agency (NITDA).

Purpose

The objective of the Regulations is to protect the rights of natural persons to data privacy, encourage the safe handling of transactions which involve the exchange of personal data, and prevent acts of manipulation relating to personal data. A natural person is defined as any person residing in Nigeria (or residing outside Nigeria but who is a Nigerian Citizen). Also, the Regulations provide compliance requirements on all private or public organizations in Nigeria for the collection, processing, and use of personal data of any natural persons.

Scope of Regulations

The preamble to the regulation, states that it applies to all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria; the Regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria; and the Regulation shall not operate to deny any Nigerian or any natural person the privacy rights they are entitled to under any law, regulation, policy, contract for the time being in force in Nigeria or in any foreign jurisdiction.

Definitions

Certain expressions in this article are used frequently and for ease of reference they include the following:

Data Controller

means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed.
Simply put, a "Data Controller" is an entity that collects the Personal Data of its users for specific reasons incidental to the use of their services. Examples include online vendors like restaurants and supermarkets, social media websites such as Facebook, Instagram, Twitter etc., email platforms like Gmail, Hotmail, employers of labour, public institutions and many more.

Data Subject

means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Data Administrator

"means a person or an organization that processes data".

Key Provisions of the NDPR

The salient provisions of the NDPR are as follows:

• The personal data of a data subject must only be collected lawfully and must be adequate, accurate and respect the dignity of the human person.

• Consent of the subject must have been obtained voluntarily prior to the collection without the use of fraud, coercion, or undue influence. Before the consent is obtained, the specific purpose of collection of Personal Data must be made known to the data subject for it to be deemed lawful. The Data subject must also be informed of his/her right to withdraw consent at any time. The data controller must display in a simple and conspicuous manner, its privacy policy.

• Upon collection, the data must be stored only for the period necessary and must be secured against foreseeable hazards such as theft, cyberattack, viral attack, dissemination, manipulation of any kind, damage by rain, fire, or exposure to other natural elements.

Key Provisions of the NDPR

• Where data is to be transferred to another jurisdiction, the transfer must be done under the supervision of the Attorney General of the Federation (AGF). However, in the absence of the approval of the AGF, transfers may take place where the consent of the data subject has been obtained, the transfer is necessary for the performance of a contract or public interest purpose, or for a defence of legal claims.
• Private Institutions must employ a Data Processing Officer to ensure strict compliance with the provisions of the NDPR.

Data Audit Compliance

The NDPR mandates organisations that process the personal data of more than 1000 data subjects in a period of six (6) months and more than 2000 data subjects in a period of twelve (12) months to conduct and submit to the NITDA, through a licensed Data Protection Compliance Officer (DPCO), a detailed audit of its privacy and data protection practices annually, specifically before 15 March of each year.
The NDPR provides that the Data Protection Audit Report (DPA Report), which is to be accompanied by a verification statement by the DPCO, must contain the following information:

a. personally identifiable information the organization collects on employees of the organization and members of the public.

b. any purpose for which the personally identifiable information is collected.

c. any notice given to individuals regarding the collection and use of personal information relating to that individual.

d. any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual.

e. whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent.

f. the policies and practices of the organization for the security and the proper use of personally identifiable information.

g. organization's policies and procedures for privacy and data protection.

h. the policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies; and

i. the policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

Penalties

Any Company who is found to be in breach of the data privacy rights of any Data Subject shall be liable, in addition to any other criminal liability, to the following:

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: or

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.

Although the NDPR does not provide the specific fine to be paid as a penalty for failure to submit the DPA Report within the statutory timeline, previous non-compliance notices issued by the Agency show that the fine levied may be up to 2% of a company's annual gross revenue of the preceding year.

Conclusion

The NDPR has enabled Nigeria to take a step forward in improving the safeguarding of their citizens rights to privacy. However, more effort must be made by government agencies to sensitize institutions as to the importance of data protection and ensure adequate training and reorientation of institutions who collect and process personal data of data subjects. In addition, we must note that the penalty applicable for breach of an individual's privacy rights under law is a fine against the erring institution, which offers no direct recourse to the affected person. Going forward, the privacy policies of institutions could include the payment of a fixed sum as compensation or damages for illegal sale or sharing of personal information. Notwithstanding that the regulations do not give a personal right to recourse; aggrieved persons may still seek redress by filing a civil suit for conversion of private property or breach of contract (confidentiality).

Author

FOLAJOMI FAWEHINMI
Associate
Corporate, Commercial and Business Advisory
T: +234 1 700 257 0 Ext 112
E: ffawehinmi@alp.company