NIGERIA HAS A DATA PROTECTION REGIME

Ngozi Aderibigbe

Friday, May 25, 2018 is not just any another date on the calendar of EU corporates. It is the date when the EU General Data Protection Regulation takes effect. Much like the Millennium Bug (Y2K bug) saw the world counting down with anxiety to the first moments of the year 2000, organisations in the EU are consumed with frenzied activities to ensure compliance with the GDPR before the D-day. Compliance with the GDPR comes at a cost. Non-compliance will cost even much more. EU organisations are therefore revising, upgrading and rechecking their processes to ensure strict compliance with the stringent provisions of the GDPR.

In Nigeria, the situation is the exact opposite. Corporates pay little or no attention to data protection laws – local or foreign. In fact, there is a growing misconception among Nigerian businesses that Nigeria has no tangible data protection regime.

It needs to be clarified that Nigeria has a data protection regime that is valid, enforceable and arguably matches up to international standards.

As with many countries of the world, Nigeria's data privacy regime takes it earliest reference from the country's constitution. **Section 37 of the 1999 Constitution** protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication. Data protection and privacy is an extension of the constitutional right of citizens to privacy.

Besides the Constitution, there are several other legislations that contain provisions that touch on the protection of privacy rights. **The Child Rights Act, 2003** reiterates the constitutional right to privacy as relates to children. The **Freedom of Information Act No. 4 of 2011**, which in the whole is an Act to enable public access to public records and information, prevents a public institution from disclosing personal information to the public unless the individual involved consents to the disclosure. **The Cybercrimes Act, 2011** prevents the interception of electronic communications and imposes data retention requirements on financial institutions. **The Consumer Code of Practice Regulations, 2007** issued by the Nigerian Communications Commission (which regulates the telecommunications industry) requires telecommunication operators to take reasonable steps to protect customer information from accidental disclosure. It also restricts the transfer of customer information. **The Consumer Protection Framework** issued by the Central Bank of Nigeria in 2016 contain provisions that restrict financial institutions from disclosing personal information of their customers.

As yet, the most relevant, crucial and comprehensive single legislative instrument on data protection is the **Guidelines on Data Protection (version 4.0) ("NITDA Guidelines" or "the Guidelines")** issued by the National Information Technology Development Agency ("NITDA").

Is the NITDA Guidelines on Data Protection Enforceable?

NITDA was established by the National Information Technology Development Agency (NITDA) Act, 2007, as the statutory agency with responsibility to develop information technology in Nigeria. Specifically, the NITDA Act empowers NITDA to **"develop guidelines for electronic data interchange and other forms of electronic communication".**[1] It is in furtherance of this specific mandate that NITDA published the NITDA Guidelines on Data Protection (version 4.0) in 2013.

It is important to correct any impression that suggests that the provisions of the NITDA Guidelines are anything but law, or that its application does not extend to private sector organisations. These positions are not correct. Although the drafting style of the NITDA Guidelines is not particularly brilliant - as its provisions are somewhat tangled, leading to ambiguity and providing little clarity – yet, in every material sense, the NITDA Guidelines qualifies, and is enforceable as a subsidiary legislation.

A subsidiary legislation has been defined by the **Interpretations Act of 1964** as any order, rules, regulations, rules of court or bye-law made in exercise of powers conferred by an Act. The Court of Appeal has also enunciated that **"a subsidiary legislation is made or enacted under and pursuant to the power conferred by a principal legislation or enactment. It derives its force and efficacy from the principal legislation…"**[2] Clearly, subsidiary legislations have the same force of law as the principal legislation and are therefore equally binding. Thus, compliance with the NITDA Guidelines on Data Protection is a requirement of law, not a matter of choice.

Whilst NITDA has not been particularly emphatic on compliance with NITDA Guidelines, it must be said that NITDA's apparent docility does not undermine the legal weight of the NITDA Guidelines. In fact, NITDA may have begun to arouse itself to its regulatory duties as it recently cautioned organisations against the risk of noncompliance with the EU General Data Protection Regulation and in the same breath drew attention to the 2013 NITDA Guidelines.[3] **Section 1.2 of the NITDA Guidelines** is self-authenticating. It affirms: **"a breach of the Guidelines shall be deemed to be a breach of the Act."**[4] Thus, until such a time as the 2013 NITDA Guidelines are revised, this subsidiary legislation remains enforceable

Does the NITDA Guidelines apply to Private Sector Organisations?

NITDA Guidelines prescribe minimum data protection standards for all organisations or persons that control, collect, store or process personal data of Nigerian residents and citizens within and outside Nigeria.

[1] Section 6(c) NITDA Act.
[2] Njoku v. Iheanatu (CA/PH/EPT/454/2007).
[3] This public notice by NITDA made on 19th February, 2018

The scope of persons who are bound by the NITDA Guidelines is clearly specified within the Guideline in these words:

> **"These guidelines are mandatory for Federal, State and Local Government Agencies and institutions as well as other organizations which own, use or deploy information systems within Federal Republic of Nigeria"**

Section 1.4 of the Guidelines further confirms that "**the Data Protection Guidelines shall apply to all data controllers** [defined below] **in public and private sector as defined in these guidelines".** It also applies to foreign organisations that process personal data of Nigerian citizens.

Overview of NITDA Guideline

(a) **Basic Concepts**

The NITDA Guidelines define the following terms which are fundamental to understanding the provisions of the Guidelines.

i. Personal data: this is any information relating to an identified or identifiable natural person, whether it relates to his or private, professional or public life. It includes any information which can be used to distinguish or trace an individual's identity, such as names, addresses, photographs, email address, bank details, social networking details, medical information or computer IP address.

ii. Data Controller: refers to the person or entity who, whether alone or with another, determines the purposes and means of processing personal data. Generally speaking, the organisation which collects personal data is the Data Controller.

iii. Data subject: refers to an identifiable person or one who can be identified directly or indirectly by reference to an identification factor. The Guidelines contemplate only natural persons as data subjects.

iv. Processing of Personal Data: Processing or personal data refers to any operation which is performed on personal data. It includes collecting, recording, organising, storage, adapting, retrieving, consulting, transmission, dissemination of data. In practical terms, every way in which an organisation handles personal data amounts to processing.

v. Sensitive Personal Data: this includes data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, and criminal records. These sets of data are classified as special and have more stringent conditions attached to their collection and processing.

(b) Principles of Data Protection

The provisions of the Guidelines coalesce into eight principles which are specifically identified in section 4 of the Guidelines. These principles are discussed below:

a. **Principle 1: Personal data must be processed fairly and lawfully**
Data Controllers are required to process personal data in the manner prescribed by the Guidelines. This includes disclosing to data subjects the purpose for which data is being collected and, if personal data is to be transferred to a third party outside the country, notifying data subjects of such transfer.

To comply with this principle, organisations are advised to provide general data protection and privacy policy statements to provide information on what data the organisation collects, why the collection is made and how the data collected would be used. The policy statement should also include information on who such data might be shared with. Where CCTV footages are taken, the data collector's privacy policy statement should be prominently displayed.

b. **Principle 2: Personal Data should be used only in accordance with the purpose for which it was collected**

Data controllers have a duty to ensure that data collected for one purpose is not used for a different purpose. This principle prevents the use of personal data in any manner different from the purpose disclosed to the data subject at the point of collecting the data. To avoid breach of this principle, organisations are advised to a wide description of the purpose for the data collection in their general data protection and privacy policy statements.

c. **Principle 3: Personal data must be adequate, relevant and not excessive**
This principle prevents organisations from obtaining data without a real or specific purpose. Only data which is specific to the stated purpose should be collected.

d. **Principle 4: Personal data must be accurate and where necessary kept up to date**

Data Controllers are required to have in place arrangements that enables data subjects to update their personal data.

e. **Principle 5: Personal data must be kept for no longer than is necessary**

Data Controllers must ensure that personal data is not retained for longer than necessary, with reference to the purpose for which the data was obtained. Although the Guidelines do not prescribe a timeframe for data retention, this principle places a burden on data controllers to develop a retention policy for personal data.

f. **Principle 6: Personal data musts be processed in accordance with the rights of data subjects**

Organisations, as data controllers, must respect the rights of Data subjects. These rights include a right to obtain information on the purpose of data collected and to request a copy of their personal data in a usable from data controllers. Such a request should be responded to promptly and the data provided to the data subject within seven days of the request. Data subjects are also entitled to the opportunity to object to the processing of data for direct marketing purpose.

g. **Principle 7: Appropriate technical and organisational measures must be established to protect the data**

All Data Controllers are required to implement technical and organisational measures to ensure security of personal data. The Guidelines prescribe some organisational measures including, developing an organisational policy for handling personal data, personnel training on data protection, conducting privacy and data protection assessments, appointing a Data Security Officer to have direct responsible for ensuring the organization's adherence to data protection policies, etc. Technological solutions necessary to avoid data security breaches, e.g. data encryption, setting up firewalls, are also recommended.

h. **Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection.**

Data Controllers have an obligation to ensure that personal data is not transferred to a country which does not ensure, at the least, the same level of protection as imposed by the Guidelines.

It needs to be mentioned that the burden of compliance with Guidelines is on the Data Controller. When personal information is transferred to a third party for processing, the obligation to ensure compliance with the Guidelines remain on the Data Controller. Data Controllers are therefore required to enter into contracts with third-party data processors to restrain the third-party data processor from dealing with the data otherwise than as instructed by the data controller and imposing such restrictions on transfer of personal data to outside the country as the Guideline imposes on the data controller.

WHAT ORGANISATIONS MUST DO TO COMPLY

(A) Have a Data Protection Audit conducted for your organization:

Organisations are required to have conducted a detailed audit of their data protection and privacy policies within 12 months after the date of adoption of the Guidelines, i.e. by September 2014, to ensure compliance with the Guidelines. This Audit should identify the personal data which the organization collects on employees and members of the public and how this data is used. It should also audit third party contracts that require transfer of personal data to such third parties.

(B) Assign a Data Security Officer

The Data Security Officer would have responsibility to ensure that the company's processes are in compliance with the data protection rules.

(C) Develop a general data protection and privacy policy statement

In line with the requirement for fair processing of personal data, organisations need to have carefully drafted data protection and privacy policy statement which would meet the requirements under the Guidelines.

(D) Train employees about handling data

It is important that key employees who handle personal data are trained on how to deal with such data. It is particularly important the HR personnel within the organization receive the requisite training.

For further Information on this subject please contact

Ngozi Aderibigbe
Email: ngoziaderibigbe@jacksonettiandedu.com

Jackson, Etti & Edu
RCO Court
3-5 Sinari Daranijo Street
Victoria Island, Lagos, Nigeria
Tel: 234-1-2915427, 2623700-1, 4626841
Fax: 234-1-2717889, 2623702