ÆLEX

THE NITDA DATA PROTECTION REGULATION: A WATERSHED IN THE PROTECTION OF PERSONAL DATA IN NIGERIA

FLORENCE BOLA-BALOGUN

fbola-balogun@aelex.com

Florence is an Associate and a member of the firm's Corporate/Commercial Practice Group

ADEMOLA ADEYOJU

aadeyoju@aelex.com

Ademola is an Associate and a member of the firm's Corporate/Commercial Practice Group

INTRODUCTION

Through the years, Nigeria has lacked comprehensive legislation which protects against the misuse and mismanagement of personal data. However, on 28th January 2019, the National Information Technology Development Agency's (NITDA) took a bold step towards changing this narrative when it published the Data Protection Regulation ("the Regulation").

Scope and Application of the Regulation

The Regulation is made under the powers of NITDA[1] to develop regulations for electronic governance and to monitor the use of electronic data interchange and other forms of electronic communication transactions.

The Regulation applies to transactions intended for or requiring the processing of personal data. It also applies to all Nigerians who are resident within and outside Nigeria, and to non-Nigerians resident in Nigeria.

Highlights of the Data Protection Regulation

Personal Data is defined in the Regulation as the information relating to an identified or identifiable natural person[2]. These may include a name, a photo, an email address, bank details, medical information, computer internet protocol (IP) address and any other information specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. However, personal data does not include companies' information. Processing means any operation on personal information such as collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure or dissemination.[3]

The Regulation also provides for Data Controllers who shall be persons responsible for determining the manner in which personal data would be processed. A Data Controller

[1] Section 6 (c) and Section 32 of the National Information Technology Development Agency Act
[2] Section 1.3 of the NITDA Data Protection Regulation
[3] Section 1.3 of the NITDA Data Protection Regulation

("Controller") must understand the legal basis for processing[4] the information before it proceeds to obtain personal information. For the processing of data to be considered as being lawful, at least one of the following must apply as the processing;

a. has been consented to by the data subject
b. is for the performance of a contract
c. is required for compliance with a legal obligation
d. is required for protection of the vital interest of a data subject or another natural person, or
e. is necessary for the performance of a task carried out in the public interest.[5]

The Controller is required to give specific information to a Data Subject[6] before obtaining any personal information to ensure that the Data Subject gave informed consent.[7]

The obligation of the Controller does not end at the collection stage but extends to the storage of the Personal Data as he must ensure the security of the data, which can be done by protecting systems from hackers, setting up firewalls or developing an organisational policy on handling personal data.[8]

Following in the footsteps of the European Union's General Data Protection Regulation (GDPR), the Regulation imposes an obligation on the Data Controller to ensure that its third-party processors adhere to the Regulation.[9]

Rights of Data Subject

The Regulation recognises the right of a Data Subject to a deletion of personal information, restriction in processing the information, right to rectify and to have the

[4] Section1.3 of the NITDA Data Protection Regulation defines processing as any operation on personal information such as collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure or dissemination
[5] Section 2.2 of the NITDA Data Protection Regulation
[6] Section 1.3 of the NITDA Data Protection Regulation defines a Data Subject as any person who can be identified, whether directly or indirectly, by particular reference to an identification number or by physical, physiological, mental, economic, cultural or social identity or a combination of any of these factors.

[7] Section 2.13.6 of the NITDA Data Protection Regulation
[8] Section 2.6 of the NITDA Data Protection Regulation
[9] Section 28(1) of the GDPR and Section 2.8 of the NITDA Data Protection Regulation

information in a portable format, and also the right to transfer the information to another Data Controller.[10] Besides, the Data Subject has the right to object to the processing of personal information where it is for marketing purposes.[11]

Enforcing the Rights of Data Subjects

The Regulation further empowered NITDA to set up an Administrative Redress Panel to receive allegations from Data Subjects; investigate the allegations; where necessary, issue administrative orders; and determine appropriate redress. The investigation and determination of the remedy by the Administrative Redress Panel must be done within 28 days.[12]

The Regulation further provides that the privacy right of a Data Subject should be interpreted to advance, and never to restrict the safeguards the Data Subject is entitled to.[13]

Transfer of Data to Third-Party Countries

The Regulation provides for the transfer of data to third-party countries.[14] It vests supervisory powers on the Attorney General of the Federation to determine third-party countries with adequate data protection laws for possible data transfer to such countries.

However, where the Attorney General has not decided on such countries, the Data Controller may process the information where:

a. The Data Subject has consented to the processing;
b. It is for the performance of a contract in favour of the data subject
c. It is for the public interest;
d. It is for the establishment, exercise or defence of legal claims; or
e. It is to protect the vital interests of the Data Subject or other persons

[10] Section 2.13 of the NITDA Data Protection Regulation
[11] Section 2.8 of the NITDA Data Protection Regulation
[12] Section 3.2 of the NITDA Data Protection Regulation
[13] Section 2.9 of the NITDA Nigeria Data Regulation
[14] Section 2.10 and 2.11 of the NITDA Data Protection Regulation

The Regulation also impose the following compliance obligations on both private and public entities as follows:[15]

1. They are to display a conspicuous privacy policy on all medium for collection and processing of personal data.[16]
2. Within three months[17] from the issuance of the Regulation, they are to publish their data protection policies.[18]
3. They are to designate a Data Protection Officer to ensure adherence to the Regulation.[19]
4. Within six months after the date of issuance of this Regulation, they are to conduct a detailed audit of their respective privacy and data protection practices.

Where a Company processes more than 2000 Data Subjects within a period of 12 months, it must submit a summary of a data protection audit to the NITDA on 15th March of every year.

Penalty

The Penalty for failing to comply with the Regulation is dependent on the number of Data Subjects that a company processes[20]:

a) More than 10,000 Data Subjects - payment of the fine of 2% of Annual Gross Revenue or 10 million Naira whichever is greater;

b) Less than 10,000 Data Subjects - payment of the penalty of 1% of the Annual Gross Revenue or 2 million Naira whichever is greater.

[15] Section3 of the NITDA Data Protection Regulation
[16] Section 2.5 of the NITDA's Data Protection Regulation
[17] NITDA announced the release of the Regulation on Friday, 25th January 2019 – see https://sundiatapost.com/2019/01/25/nitda-unveils-it-guidelines-calls-for-strict-compliance/ accessed on 30th January 2019. Therefore, the three months will lapse on 24th April 2019
[18] Section 3.1 of the NTDA Data Protection Regulation
[19] Section 3.1.2 of the NITDA's Data Protection Regulation
[20] Section 2.10 of the NITDA Data Protection Regulation

Our Thoughts

The Regulation was made a few months after the European Union's General Data Protection Regulation (GDPR) came into effect. The GDPR can be described as the most revolutionary introduction to the regulatory landscape of data privacy, particularly because its jurisdiction extends beyond the European Union and applies to all businesses, regardless of location, who by virtue of their business relationship with entities in the EU, process the personal data of EU residents.

The Regulation has adopted or replicated some of the key provisions of the GDPR, including the processing and handling of personal data for clearly specified business purposes, application of the data protection provisions to all residents, and imposing obligations on entities to protect data with corresponding penalties for a contravention of the data protection provisions.

Nonetheless, the Regulation is not as comprehensive and extensive as the GDPR and there is a question on if the timeline for effectiveness of the Regulation is practicable. The Regulation is required to come into effect when it is signed by the NITDA Board; it is to be noted that the Regulation was issued on the 28th of January 2019, and it mandates companies to comply with its provisions from the date of issuance of the Regulation.

This is a remarkable contrast from the GDPR which provided for a two-year period within which member states of the European Union (EU) were to comply with it. Considering that this legislation on data protection is entirely new to Nigeria, it may take some time for companies and business to fully comply with it.

Nonetheless, the introduction of the Regulation is a marked change from the status quo to the extent that personal data shall only be collected for specified, explicit and legitimate purposes, and shall not be used in a manner that is incompatible with those purposes. It also imposes an obligation on entities to only collect personal data that is

adequate, relevant and limited to what is necessary for the purposes for which they are processed.

If the Regulation is duly enforced and complied with, it will be in substantial compliance with the GDPR and may provide more comfort to Nigerian entities doing business in the EU or with EU entities. It is also expected that familiarity with the application of the Regulation will make the implementation of the Data Protection Bill (currently pending at the National Assembly) easier if it is eventually passed into law.

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana.

Contact us at:
4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria
Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,
E-mail: lagos@aelex.com
To see our other office locations, please click **HERE**
www.aelex.com

You may also visit our social media pages: