THOUGHTS ON THE FEDERAL INLAND REVENUE SERVICE'S PLANNED DEPLOYMENT OF ITS AUTOMATED TAX ADMINISTRATION SOLUTION

by Abraham Omoufoma Aigba

Introduction

The Federal Inland Revenue Service ("FIRS"), in a Public Notice on the Deployment of Automated Tax Administration Solution ("the Notice") published in the Nation Newspaper of March 31, 2021, gave notice to all taxable persons[1] and the general public of the FIRS' intention to connect its Automated Tax Administration System ("ATAS") to access the data[2] of taxable persons stored in any electronic device maintained by any relevant person(s) or their agents[3], for tax purposes, not earlier than 30 days of the date of publication of the Notice.

The implication of the foregoing is that banks, employers, service providers and all other entities, companies or organizations in possession of the financial information of taxable persons in Nigeria must grant the FIRS access to such information or risk the penalties stated in Section 26(3) of the Federal Inland Revenue Service (Establishment) Act ("the FIRS Act").

A corollary to this, however, may be a possible breach of the data protection/privacy obligations owed by these "relevant persons" to the taxable persons.

This paper seeks to examine dicey issues emanating from the Notice vis-à-vis the extant data protection/privacy laws in Nigeria.

Data Protection Regime in Nigeria

While there are a number of laws regulating data protection in Nigeria, the Nigeria Data Protection Regulation, 2019 ("the NDPR") is the most comprehensive legislation on the subject. In May 2020, the National Information Technology Development Agency ("NITDA") issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 ("the Guidelines") which, amongst other things, regulates the sharing of personal data[4] between public institutions or between private institutions and public institutions. The Guidelines is the focus of this paper.

Prefatorily, it is to be noted that the NDPR protects only the personal data of natural persons. In that context therefore, companies, trustees, business names and other organizations not being natural persons are not protected by the NDPR and by

[1] Which includes individuals, trustees, partnerships, companies, corporations, etc

[2] Which shall include information of taxable persons related to Point of Sale Terminals and other invoicing platforms used by taxable persons

[3] Relevant persons in this regard contemplates the data controllers of the data sought to be connected to the ATAS who by the Notice are also required to grant the FIRS access to all its electronic devices used to store the personal data of taxable persons.

[4] Personal data means any information which of itself or when combined with other information, can be used to identify a specific natural person ("data subject"). In this context, personal data may range from names, email address, location, tax identification number, financial records, name of employer, etc. of data subjects.

extension, the Guidelines. However, they also form the basis of this discourse given that they control the personal data of data subjects who are affected by the Notice.

Sharing of personal data under the Guidelines

The Guidelines permits private institutions to share personal data of interest in their possession with Public Institutions upon request[5] and insofar as the provisions of the Guidelines are satisfied. Some of the specific requirements for the validity of such request are that the request must be signed by the Chief Executive Officer of the Public Institution, state clearly the purposes for which the information is sought from the private institution, provide evidence of the digitalization of the database of the Public Institution and upon an undertaking provided by the Public Institution that it shall protect the information from unauthorized third parties and shall not deanonymize the information shared.[6]

Further, Paragraph 2.6 of the Guidelines mandates Public Institutions desirous of obtaining personal data from private institutions to demonstrate compliance with international information security standards such as ISO 27001:2013, compliance with the NDPR, conduct a Data Protection Impact Assessment and retain the services of a Data Protection Compliance Organization. However, the FIRS is not on NITDA's list of compliant organizations raising the presumption that it is not NDPR compliant.[7]

What is more, Paragraph 5(b) of the Guidelines mandates private institutions to which a request is made to evaluate same with a view to ensuring that it complies with the NDPR and to seek NITDA's clarifications where it is unable to ascertain the propriety of the request. However, paragraph 5(d) seems to negate paragraph 5(b) by stating that the latter paragraph shall not apply where the request is aimed at the enforcement of law. Thus, given that the Notice relates to the enforcement of the FIRS Act, private institutions may be required to comply with the Notice.[8] More so, the NDPR permits the processing or disclosure of personal data where such disclosure is statutorily required or is expressly required by a regulatory body, such as the FIRS.

Conduct of a Data Protection Impact Assessment

One important consideration for the FIRS is to ensure that it conducts a Data Protection Impact Assessment ("DPIA") before it deploys its ATAS, as planned. The importance cannot be overstated. This is driven by the fact that, by deploying its ATAS, the FIRS assumes the role of a data controller to data controllers as they will have access and control of data hitherto controlled by companies and other relevant data controllers. This invariably will put the data of all Nigerians in the control of the FIRS. By Paragraph 1(viii) of the Nigeria Data Protection Regulation, 2019: Implementation Framework, 2020 ("the Implementation Framework), data controllers

[5] In this regard, does the FIRS Notice qualify as a request? This question begs for an answer
[6] See paragraphs 4 and 6 of the Guidelines.
[7] Although this may be attributable to the fact that NITDA's list of complaint Organizations is yet to be updated
[8] This is however a most curious case. Where the presumption that the FIRS is not NDPR compliant is true, should private institutions go ahead to comply with the Notice? Has the FIRS conducted a data protection impact assessment on the planned connection of its ATAS to the servers of private institutions? If the only 'request' made by the FIRS is the Notice, then the request cannot be said to have complied with the Guidelines as, aside mandating private institutions to give it access to their servers, it makes none of the assurances required by the Guidelines and neither does it demonstrate that FIRS' compliance with paragraphs 2, 3, 4 and 6 of the Guidelines.

must conduct a DPIA where they intend to embark on a new activity particularly one that will involve an intense use of personal data.

Given that the data sought to be accessed by the FIRS was initially supplied to the "relevant persons" for purposes other than as now required by the FIRS, it is suggested that both the FIRS and the relevant persons (as data controllers) should collaborate to ensure compliance with Paragraph 4.1 of the Implementation Framework.

It is further suggested that NITDA should exercise its powers under Paragraph 4.2 of the Implementation Framework to request the FIRS to submit its DPIA with respect to the planned deployment of its ATAS.

Compliance with the Notice

Any sharing of personal data with a Public Institutions is required to be by encrypted means or other methods which obscure such data.[9]

In light of the FIRS' Notice under consideration, relevant persons to which the Notice relates may, as a preliminary step, seek assurance from the FIRS with regards to the matters in Paragraphs 2.6, 4 and 6 of the Guidelines[10] and/or may seek advice from NITDA on whether or not to comply with the Notice.

Where this done, the relevant persons/data controllers should isolate the data sought by the FIRS into an encrypted database to which the ATAS may be connected.[11] Taking these steps is precautionary on the data controllers who thus, have given themselves a good defence in the event of breach of their data as a result of the FIRS's processing of their personal data.

Upon compliance with the Notice, data controllers are required to provide NITDA with details of the nature of personal data of data subjects to which they have given the FIRS access to in line with Paragraph 5(c) of the Guidelines.

[9] paragraph 4 (b) and (c) of the Guidelines prohibits the sharing of databases by private institutions with Public Institutions by means other than encrypted or other formats which murks such data.
[10] As well as seek information on FIRS' data protection policies and its compliance with the NDPR
[11] Although not specifically required by either the Notice or the Guidelines, ethics dictates that the data made available to the FIRS should as much as is possible, be accurate.