NIGERIAN PUBLIC INSTITUTIONS –
WHAT YOU NEED TO KNOW AND WHAT YOU NEED
TO DO TO COMPLY WITH THE GUIDELINES FOR THE
MANAGEMENT OF PERSONAL DATA BY PUBLIC
INSTITUTIONS ISSUED BY THE NITDA IN MAY 2020

www.uubo.org
subscribe: dp@uubo.org
Introduction

The National Information Technology Development Agency (the “NITDA”) on 18th May 2020, issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 (the “Guidelines”) to provide detailed guidance to public officers on the processing and management of personal data in compliance with the Nigeria Data Protection Regulation 2019 (the “NDPR”).

We have, in this guidance note, adopted a question and answer format to highlight the key provisions of the Guidelines and provide a compliance guide to aid public institutions in complying with their obligations under the Guidelines.

1. What is the scope of the Guidelines?

   a. The Guidelines apply to all public institutions in Nigeria that process the personal data of Nigerian citizens, Nigerian residents or foreigners who have interactions with public institutions. The Guidelines also apply to public institutions that have access to personal data for statutory or administrative purposes.

   b. A “Public Institution” under the Guidelines includes ministries, departments, agencies, institutions, public corporations, publicly funded ventures, and incorporated entities with government shareholding either at the federal, state or local government level.

2. Does the NDPR apply to our operations in addition to the Guidelines?

   Yes, the NDPR is applicable to all public institutions, and its provisions will be read together with the provisions of the Guidelines.

3. What are the immediate steps that we need to take to comply with the Guidelines?

   a. Appoint a data protection officer (the “DPO”) on or before 16th August 2020;

   b. Train the DPO within 90 days of appointment;

   c. Publish a privacy policy which is accessible to data subjects (if one does not exist)\(^1\);

---

\(^1\) The privacy policy should be published through the mediums accessible to a majority of the public institution’s data subjects. This can be achieved by publishing the privacy policy on its website or any public/digital media, pasting it at conspicuous parts of its business premises, or providing a copy to data subjects etc.
d. Ensure that on or before 17th July 2020, all databases containing personal data are stored in digital form with restricted or controlled access. This means that all physical documents containing personal data have to be digitalised. We would recommend that any public institution that is unable to meet this deadline discuss such issue with the NITDA in order to obtain a dispensation or agree on a timeframe for compliance. The grant (or otherwise) of such a request is entirely subject to the discretion of the NITDA;

e. Encrypt personal data or store it in a form that prevents unauthorised access, before sharing with another public institution; and

f. anonymise or pseudonymise all personal data to be shared with third parties for processing for the purpose of predictive analysis, forecasting, mapping or intelligence gathering.

### Are the lawful and legitimate bases of processing under the NDPR the only means by which we can process personal data?

In addition to the lawful and legitimate bases for the processing of personal data under the NDPR, the Guidelines allows public institutions to process personal data:

a. in furtherance of the legitimate interest of the data subject. In the absence of guidance on what constitutes the legitimate interest of the data subject, we would recommend that public institutions rely on the other bases for the processing of personal data, or seek the guidance of the NITDA or a Data Protection Compliance Organisation (“DPCO”) where it is not clear whether an intended processing activity is in the legitimate interest of the data subject; and

b. based on the public interest, legal interest or the vital interest of the data subject. The determination of whether processing is based on the public interest, legal interest or the vital interest of the data subject is subject to whether the intended processing activity is:

   i. directly or collaterally linked to the performance of a mandate stipulated by an Act of the National Assembly;

   ii. necessary for the promotion of security or welfare of citizens, justifiable in a democratic and free society; or

   iii. based on a directive of the President in furtherance of the powers vested in that office by the Constitution or a legal instrument.

### Are there instances where we are mandatorily required to obtain the consent of the data subject?

With the exception of health emergencies, national security or crime prevention, public institutions are required to obtain the consent of a data subject:

a. for new direct marketing or communication activity;

---

2 The privacy policy should be published through the mediums accessible to a majority of the public institution’s data subjects. This can be achieved by publishing the privacy policy on its website or any public/digital media, pasting it at conspicuous parts of its business premises, or providing a copy to data subjects etc.
What measures do we have to put in place to process, or continue processing personal data for other public institutions, a private entity or an international organisation?

Public institutions seeking to access and use the personal information collected or stored by another statutory body, private entity or international organisation need to put measures in place to ensure the confidentiality, integrity, availability and resilience of personal data. More specifically, public institutions need to:

a. comply with international information security standards such as ISO 27001:2013 or similar standards;

b. comply with the provisions of the NDPR;

c. retain a DPCO to:
   i. conduct a data protection impact assessment⁶ and submit a report of the assessment to the NITDA; and
   ii. guide the public institution in the use of the personal data and compliance with applicable laws; and

d. publish a privacy notice in 4 national daily newspapers, its website, social media accounts and other appropriate media at least 30 days before the personal data is used (this applies only to access and use of personal data from other public institutions).

Can we be penalised for not complying with the Guidelines?

7.1 Yes, a public institution can be penalised for non-compliance with the Guidelines. Where the public institution is found to be in breach of the Guidelines, it will be liable to a fine of:

a. NGN 200,000 in the case of a first conviction; and

---

⁶ The request for consent to process sensitive personal data must be direct, unambiguous and in written or electronic form, depending on the circumstance.
⁷ The consent of the child's parent or guardian is required.
⁸ This is a process that helps to identify and minimise the data protection risks of a project.
7.2 Unless the chief executive officer of the public institution or any officer acting in that capacity proves that the act or omission constituting the breach/non-compliance took place without his or her knowledge, consent or connivance, such chief executive officer or any officer acting in that capacity shall if convicted be liable to:

a. NGN 200,000 or imprisonment for a term of 1 year or to both such fine and imprisonment, in the case of a first conviction; and

b. NGN 500,000 or imprisonment for a term of 3 years, or both such fine and imprisonment, in the case of a second and subsequent convictions.

7.3 Principal officers of public institutions processing personal data or public institutions that may have requested processed personal data are personally liable for non-compliance with the Guidelines or misuse of the information shared. This liability continues even after the officer vacates that office.

7.4 Where a public institution that is a data controller is found to have breached the rights of a data subject, the public institution shall in addition to any other criminal liability, be liable to a fine of:

a. 2% of annual gross revenue of the preceding year, or the payment of the sum of 10 million Naira, whichever is greater – in the case of public institutions dealing with the personal data of more than 10,000 data subjects; or

b. 1% of annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater - in the case of public institutions dealing with the personal data of less than 10,000 data subjects.

Conclusion

Public institutions should endeavour to comply with the Guidelines, as this will encourage compliance by members of the public, especially organisations in regulated sectors, and will show a government that is leading by example.

If you are in doubt about what steps to take at this time in order to ensure compliance with the Guidelines, kindly seek advice from a DPCO. Our firm is a NITDA-licensed DPCO and we will be glad to assist you in this regard.

This guidance note is for general information purposes only and does not constitute legal advice and does not purport to be fully comprehensive. If you have any questions or require any assistance or clarification on how the subject of this guidance note applies to your organisation, or require the services of a Data Protection Compliance Organisation, please contact Jumoke Lambo at jumoke.lambo@uubo.org; dp@uubo.org or uubo@uubo.org.