GUIDELINES FOR THE MANAGEMENT OF PERSONAL DATA BY PUBLIC INSTITUTIONS IN NIGERIA, 2020

Issued as a Guideline for the Implementation of the Nigeria Data Protection Regulation (NDPR), 2019, within Public Institutions in Nigeria

May, 2020

PART ONE

1.1 BACKGROUND

a. Protection of personal personal data has assumed an international human rights status. Paragraph 12 of the Universal Declaration of Human Rights (1948) provides that "***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation***."

b. Similarly, the International Covenant on Civil and Political Rights (1966) also provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

c. In Nigeria, Section 37 of the Constitution of the Federal Republic of Nigeria 1999, as amended, provides that "***The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected***."

d. Consequently, the need to protect personal data is highlighted by the various laws and regulations which have stipulated various forms of protection for personal data. These laws include the Child Rights Act and the Freedom of Information Act, among others.

e. Specifically, the Nigeria Data Protection Regulation (NDPR) issued in January 2019 pursuant to Section 6 (a and c) of the National Information Technology Development Agency (NITDA) Act 2007 provides the first comprehensive regulatory framework for data privacy protection in Nigeria. The NDPR outlines the scope, objectives, principles, international transfer, sanctions for non-compliance among others.

f. The Presidential launch of the National Digital Economy Policy and Strategy in November 2019 emphasizes e-Governance implementation as a means of improving governance and deepening democracy. The collection, use, storage, access, security and transfer of personal data is fundamental to a successful implementation of the digital economy objective.

1.2 PURPOSE

The purpose of this Guideline is to provide guidance to Public Officers on how to handle and manage personal information in compliance with the NDPR, acknowledging that Governments at all levels are the biggest processors of personal data of Nigerians and in Nigeria.

1.3 AUTHORITY

This Guideline is issued pursuant to Section 6 of the NITDA Act 2007 and the NDPR 2019.

1.4 APPLICATION

a. This Guideline applies to all Public Institutions in Nigeria, including Ministries, Departments, Agencies, Institutions, Public Corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, while processing the personal data of a data subject.

b. This Guideline shall operate for the purpose of the implementation of the Nigeria Data Protection Regulation, 2019. This therefore implies that the principles and core requirements for protection of personal data remains applicable. This Guideline governs the roles and responsibilities of public officers and public institutions with regards to the processing and management of personal data.

PART TWO
2.0 Guidelines

2.1 Processing of Personal Data

a. All Public Institutions are under an obligation to protect personal data in any incidence of processing of such data. Processing in the context of this Guideline means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, viewing, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

b. All forms of personal data of a Nigerian citizen, resident or non-Nigerian individual who has interactions with public institutions, or such public institutions have access to the personal data in furtherance of a statutory or administrative purpose, shall be protected in accordance with the NDPR or any other law or regulation in force in Nigeria.

2.2 Basis for Processing of Personal Data

Processing of personal data shall be lawful and legitimate on any of the following basis:

a. clear consent of the data subject for one or more specific purposes;

b. performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. compliance with a legal obligation to which the institution is subject;

d. protection of the vital interests of the data subject or of another natural person;

e. processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller;

f. legitimate interest of the data subject;

g. processing of personal data by a public institution must be founded on Public, Legal and Vital interest and the determination of these bases shall be subject to the following:
    i. the processing is directly or collaterally linked to the performance of a mandate stipulated by an Act of the National Assembly;

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

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

h. No public institution shall change or expand the purpose for which the data was originally collected or used without an express instrument from a statutory authority or the consent of the data subject first sought and had.

2.3 Requirement of Consent

In the following circumstances, consent shall be required for the purpose of processing personal data, even where another legal basis for processing also applies:

a. for any direct marketing or communication activity, except to existing customers of the Institution who have accessed a good or a service and given consent earlier;

b. for the processing of sensitive personal data such as health, ethnic, political affiliation, religious beliefs, trade union membership, biometric, genetic and sexual orientation;

c. where personal data is used for purposes other than those initially specified to the data subject;

d. where personal data relating to a child is processed, in which case, consent is given by the parent or guardian;

e. before personal data is processed outside Nigeria; and

f. before the data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject.

2.4 Higher Standard for Sensitive Personal Data

A higher standard of consent-seeking method applies to the processing of sensitive personal data. Such specific and higher consent method shall include a direct, unambiguous and distinct communication of request for consent by any electronic means or in writing, based on the circumstances of each case.

2.5 Exceptions

The exception to the above may be cases of health emergency, national security and crime prevention.

2.6 Information Security

Every Public Institution shall put measures in place to ensure the confidentiality, integrity, availability and resilience of data. Public Institutions that seek to process the personal data of Nigerians from another Public Institution, a private entity or an international organisation shall demonstrate the following:

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

b. compliance with the provisions of the NDPR;

c. conduct of a Data Protection Impact Assessment and submission of same to NITDA; and

d. retention of a Data Protection Compliance Organisation (DPCO) to guide it in the use of the personal data and for compliance purposes.

2.6 Designation of a Data Protection Officer (DPO)

a. Every Public Institution shall, within 90 days of the issuance of this Guideline, designate an official who shall act as the DPO for the Institution. The DPO shall:
    i. be a senior level officer reporting directly to the Management;

    ii. not be involved with other activities that would likely prejudice his judgment or advice to the institution on data protection management; and

    iii. be trained in the general principles and management of personal data within 90 days of appointment.

b. The duties of the DPO include:
    i. getting board and management buy-in into data protection implementation for the institution;

    ii. developing and constantly reviewing business case for data protection implementation;

    iii. inculcating data protection as a culture in the Institution;

    iv. understanding the data processing activities of each operational unit of the Institution;

    v. constant training and capacity development for staff, licensees, contractors and stakeholders on data protection and management;

vi. advising the Management on practices that could trigger breaches; and

vii. interpreting the roles of different units in the light of data privacy protection.

c. The DPO shall be assisted by officers with certification, knowledge and experience in law, data protection and privacy, information technology, cybersecurity and related fields.

2.8 Appointment of a DPCO

Every Public Institution shall retain the service of a DPCO. The DPCO shall provide data protection audit, training and compliance services to the Institution. The list of licensed DPCOs shall be as published by NITDA. In addition to the functions stated in the NDPR, the DPCO shall be responsible for:

a. evaluating status of compliance by the Institution. NITDA expects DPCOs to base their judgment on verifiable documents and practices in the establishment;

b. appraising Data Subjects Rights Protection. The DPCO should be satisfied that the auditee has clear processes to protect the rights of the data subject. For example, a Data Subject Access Request form shows intent of transparency and accountability;

c. assessing level of awareness by top management, staff, contractors and customers on the NDPR;

d. identifying current or potential non-compliances;

e. drawing out a remedial plan to remediate identified non-compliances; and

f. every Public Institution may state further criteria to qualify DPCOs as long as the entity performing such duty shall be those licensed by NITDA.

2.9 Privacy Policy

All Public Institutions with data processing responsibilities and functions shall have a privacy policy that provides the following details:

a. what constitutes the Data Subject's consent;

b. description of collectable personal information;

c. purpose of collection of Personal Data;

d. description of technical methods used to collect and store personal information, cookies, JWT, web tokens etc.;

e. access (if any) of third parties to Personal Data and purpose of access;

f. a highlight of the principles stated in the NDPR;

g. available remedies in the event of violation of the privacy policy;

h. the time frame for remedy;

i. any other information relevant to the document; and

j. the mode or medium adopted for data subjects to exercise their rights for providing verifiable consent for the processing of their personal data.

The policy shall be given wide publicity through the mediums accessible for majority of the patrons of the service of the Institution, such as website, digital media, posted at conspicuous parts of business premises, by reading to the affected data subjects; or publication in any public media.

3.0 Rights of a Data Subject

3.1 No person shall:

a. be denied a privilege, access or right accorded by a law of Nigeria on the basis that such person refuses or fails to provide certain personal information to a government entity except such denial is based on a law passed by the National Assembly;

b. be tracked, traced, or be subject to automatic or digital decisions without a law of the National Assembly or consent of the subject; and

c. be denied access to judicial interpretation or redress as regards the use of his/her data, so long as no judicial prohibition shall be sought except to obscure the particular information of the litigant until a final decision is made by the court of competent jurisdiction.

3.2 Public Institutions who seek to access and use the personal data legally collected, stored by another statutory body shall:

a. conduct and submit a Data Protection Impact Assessment (DPIA) through a licensed DPCO to NITDA which shall consider and give a feedback within 15 working days after the final version of the DPIA has been submitted;

b. publish a public notice stating the intent to use personal data of Nigerians, the basis for the use, legal or public interest to be served, affected categories of people, commitment to data privacy protection, means of contacting the Public Institution and any other information as may be necessary or directed by NITDA or any law in existence. Such notice shall be published in four national daily newspapers, the Public Institution's website, social media handles and other appropriate media. The notice shall be published at least 30 days (1 calendar month) before the data is used; and

c. establish information security architecture and processes to assure the security and protection of the privacy of the data subjects.

4.0. Use of Technology for Processing of Personal Data

a. all databases containing personal data must be stored in digital databases with restricted or controlled access within 60 days from the issuance of this Guideline;

b. all processed personal data with personal identifiers of data subjects can only be shared with Public Institutions through encrypted formats or other cryptographic methods that protect personal data from being easily accessible by unauthorized third parties;

c. sharing of databases either through emails, hardcopies and files in any other format in non-conformity with paragraph 4.b is hereby prohibited and constitutes a breach of this Guideline;

d. all other data controllers with personal data of interest to Public Institutions for any basis as identified in Paragraph 2.2, shall create separate encrypted platform to process such data and must not under any circumstance grant access to backend of databases except for criminal investigation by a law enforcement agency or in obedience to a judicial order; and

e. data controllers shall anonymize or pseudonymize all personal data to be shared with third parties for processing for purposes of predictive analysis, forecasting, mapping or intelligence gathering, in so far legal basis has been established for the request in line with paragraph 2.2 of this Guideline

5.0 Obligation of Data Controllers to Share Personal Data with Public Institutions

a. Any data controller, whether public or private, with personal data of interest to any PI is obliged to process such data insofar as the request complies with all the provisions of this Guideline.

b. Where a request is made to a data controller to process any personal data on behalf of any Public Institution for the purposes of public or vital interest, the data controller shall evaluate the request to ensure it complies with provisions of these guidelines or shall seek clarification from NITDA within seven (7) days from receipt of such request.

c. Where a data controller is satisfied that the request to process data with a PI meets the requirements set out in this regulation, the data controller shall provide details of such transaction to NITDA, stating the following:
   i. the purpose for which data is to be processed;
   ii. duration for such processing;
   iii. type and classes of personal data to be shared; and
   iv. evaluation statement showing that the request complies with provisions of this Guideline.

d. Processing of personal data for the purpose of security or law enforcement is exempted from the application of Paragraph 2.

6.0 Processing of Personal Data for Public, Legal or Vital Interest by a Data Controller on Behalf of a Public Institution

Any PI seeking to process personal data in public, legal or for vital interest of a data subject shall:

a. ensure such request is endorsed or signed by a Governor of the Sate, Minister of the Federal Republic or the Chief Executive Officer of the PI;

b. state clearly the purpose for such processing and disclose the vital or public interest to be served by such processing;

c. provide a clear description of the output sought and manner the output shall be applied for the benefit of data subject;

d. provide proof of compliance of system requirements as required under Paragraph 4; and
e. provide an undertaking to:
   i. protect the information shared;
   ii. avoid any attempt to deanonymize the information shared; and
   iii. refrain from using the data for any other purpose.

7. 0 Breach

a. Breach or non-compliance with provisions of this Guideline is an offense in line with the provisions of Section 17 of the NITDA Act 2007 and the NDPR 2019.

b. Principal officers of Public Institutions processing personal data or Public Institution that may have requested for processed data shall be personally liable for breach of this Guideline or misuse of information shared from personal data, either while in office or after the expiration of term in office.

8.0 Administrative Redress Panel (ARP)

Parties may approach the ARP established by Article 4.2 of the NDPR, 2019 to seek redress following a determination of breach by NITDA.

PART THREE

9.0 Supplementary Definitions

Public Institution in this regulation refers to a Ministry, Department or Agency of the Federal Government, State Government Local Government or any venture funded either completely or partly by government or a company with government shareholding either at the State and Federal levels.

Principal Officer refers to any person responsible for leadership, management or administration of a Public Institution, upon whose directive officers are mandated to act or discharge their duties.

Personal data means any information allowing the identification of the data subject. This includes but not limited to information such as- 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, including but not limited to a name, address, a photo, an email address, bank details, posts on social networking websites or applications, medical information, and any other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.

THIS INSTRUMENT WAS SIGNED THIS 18TH DAY OF MAY, 2020

Kashifu Inuwa Abdullahi, CCIE
Director General/CEO
National Information Technology Development Agency (NITDA)
Nigeria's Chief Information Technology Officer (CITO)