NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK

JULY, 2020

PREFACE

It gives me immense pleasure to present the Nigeria Data Protection Regulation (NDPR) 2019: Implementation Framework. The Framework is a necessary step after the issuance of the NDPR in January 2019 and the Guideline for the Use of Personal Data by Public Institutions, May 2020. NITDA's methodical approach to data protection implementation has been the subject of interest around the world because of some unique offerings the Regulation has introduced. The NDPR has pioneered a functional data audit filing process that gives NITDA, as the information technology regulator, a good view of the state of information systems management in the country. It also establishes a public-private partnership regulatory compliance model which has empowered professionals to provide compliance-as-a-service thereby accelerating NDPR implementation across all sectors.

My joy knows no bound because NITDA, working with the excellent blueprint laid by Dr. Isa Ali Ibrahim Pantami, the Hon. Minister of Communications and Digital Economy, has begun making Nigeria a sterling example of data protection implementation in the Global South. We are not however resting on our oars; we are daily reviewing and rejigging the implementation architecture through robust stakeholder engagements. I am glad to say that through our dedicated and methodical approach, NDPR has become an household name in the digital economy sector. This indicates the level of awareness and ownership of the Regulation by Nigerians.

This Framework is a product of robust partnership and stakeholder engagement both within and outside Nigeria. I want to appreciate all our Data Protection Compliance Organisations (DPCO) who reviewed the document in November, 2019; Aissatou Sylla of Hogan Lovells LLP (France) who provided robust global perspectives; the law firm of Udo-Udoma, Belo Osagie for final vetting among many other contributors. I am very proud of our astute and dynamic NITDA staff who prepared the initial draft and managed the stakeholder process to completion.

Kashifu Inuwa Abdullahi, *CCIE*
Director General/CEO, NITDA
1st July, 2020

TABLE OF CONTENTS

CONTENTS

NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK[1]

1. BACKGROUND

1.1 It has been identified that the Personal Data of Nigerians is being processed by unauthorised persons without any lawful basis. This has resulted in processing which could lead to the loss of rights and freedoms of such Nigerian citizens or residents, leading to harm and distress. To curtail such activity, the National Information Technology Development Agency (the 'NITDA') developed the Nigeria Data Protection Regulation (the 'Regulation' or 'NDPR'). The Regulation is made pursuant to section 6(a) and (c) of the NITDA Act 2007 and section 37 of the 1999 Constitution of the Federal Republic of Nigeria 1999 (as amended).

1.2 The NDPR is at present the most comprehensive regulatory guideline on data protection in Nigeria. The NITDA, through a stakeholder model has developed this NDPR Implementation Framework (the 'Framework') as a guide to assist data controllers and data administrators/processors understand the controls and measures they need to introduce into their operations in order to comply with the NDPR.

1.3 The NDPR was issued on 25th January 2019 pursuant to section 6 (a) and (c) of the National Information Technology Development Agency Act 2007 (the 'NITDA Act'). It was made in recognition of the fact that many public and private bodies have migrated their respective businesses and other information systems online. These information systems have thus become critical information infrastructure which must be safeguarded, regulated and protected against personal data breaches. The Government further takes cognizance of emerging data protection laws

[1] Capitalised terms used herein and not otherwise defined herein shall have the meanings assigned to them in the Regulations, unless the context shall otherwise require.

and regulations within the international community geared towards protecting privacy, identity, lives and property as well as fostering the integrity of commerce and industry in the data and digital economy and has realised the imperative importance of developing data protection rules and regulations to protect the personal data of Nigerian citizens and residents.

2. SUMMARY

2.1 The Processing of Personal Data is governed by general principles that Personal Data must be:

a) collected and Processed in accordance with a specific, legitimate and lawful purpose consented to by the Data subject, provided that:
   i) a further Processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest; and
   ii) any person or entity carrying out or purporting to carry out data Processing under the provision of Article 2.1(1) of the Regulation shall not transfer any Personal Data to any person;

b) adequate, accurate and without prejudice to the dignity of the human person;

c) stored only for the period within which it is reasonably needed; and

d) secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

2.2 The NDPR further details those principles as follows:

a) Lawfulness of Processing: The NDPR requires that any processing activity of Personal Data shall be justified on 1 (one) of the following legal bases:

i. consent given by the Data Subject;

ii. the performance of a contract entered into by the Data Subject, or to take steps at the request of the Data Subject prior to entering into a contract;

iii. compliance with a legal obligation to which the Data Controller is subject;

iv. the protection of the vital interests of the Data Subject or another individual; and

v. the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the Data Controller.

b) Data Minimisation - Data Controllers are required to collect the minimum required Personal Data and avoid collecting Personal Data that is not required for the purpose of Processing or that is not directly related to the stated purpose of collection consented to by the Data Subject should not be collected, except the specific purpose of collection is made known to the Data Subject.

c) Accuracy: The NDPR provides that collected and processed Personal Data shall be adequate, accurate and without prejudice to the rights and freedoms of the Data Subject. The NDPR prohibits the abuse or inaccurate representation or use of Personal Data, even if such Personal Data was lawfully obtained. Data Controllers and Administrators are required to simplify the process of Personal Data by the Data Subject in order to achieve the objectives of this principle.

d) Storage and Retention Periods: Data Controllers are required to store Personal Data only for the period it is reasonably required to

so do. Every Data Controller must state and implement data retention schedules and communicate same to the Data Subject or potential clients.

e) Confidentiality and Security: A Data Subject's right to the confidentiality, integrity and availability of his or her Personal Data is sacrosanct with few exceptions or limitations. One of the underpinning principles of the NDPR is that the Data Controller must comply with basic minimum standards of information security management. The Regulation places an onus on all persons who are entrusted with or in possession of Personal Data, including the Data Controller and Data Administrator, to secure Personal Data in their possession. Cross reference Article 2 of the Regulation.

f) Rights of the Data Subjects. The Regulation provides a number of rights for the benefit of Data Subjects, including the following:

i. the right to be informed of the actual or intended Processing activity;

ii. the right to rectify the Personal Data ;

iii. the right to object to the Processing of Personal Data;

iv. the right to request the deletion of Personal Data;

v. the right to request the restriction of the Processing of Personal Data; and

vi. the right to request that Personal Data be transferred to another platform or person (natural or artificial).

g) Compliance and Enforcement: One of the novelties of the NDPR is its compliance framework. The Regulation creates a newly developed class of professionals - Data Protection Compliance Organisations ('DPCOs'). A DPCO is any entity duly licensed by the NITDA for the purpose of training, auditing, consulting and rendering services and products for

the purpose of compliance with the Regulation or any foreign data protection law or regulation having effect in Nigeria (See Article 1.3 (xiii) of the NDPR).

2.2 Application

The NDPR applies to every Data Controller and Data Administrator that processes the Personal Data of natural persons residing in Nigeria or who reside outside Nigeria but are citizens of Nigeria. A Data Controller is a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is Processed or is to be Processed. A Data Administrator on the other hand is a person or an organisation that Processes Personal Data on behalf of the Data Controller. Data Administrator may be used interchangeably with Data Processor.

2.3 Exceptions to the NDPR

The NDPR shall not apply in the following circumstances -

i. the use of personal data in furtherance of national security, public health, safety and order by agencies of the Federal, State or Local government or those they expressly appoint to carry out such duties on their behalf;
ii. the investigation of criminal and tax offences;
iii. the collection and processing of anonymised data; and
iv. personal or household activities with no connection to a professional or commercial activity.

3. COMPLIANCE FRAMEWORK

3.1 Forms of Compliance

i. **Cooperation**: The NITDA will to the extent that is practicable and consistent with the provisions of the Act and regulatory instruments,

seek the cooperation of stakeholders in achieving compliance with the applicable provisions.

ii. **Assistance:** The NITDA may provide technical assistance to stakeholders to help them comply voluntarily with the applicable provisions of the NDPR. This assistance will be provided through the DPCOs.

iii. **Self-Reporting:** The concerned entity will be required to proactively provide information to show compliance with the applicable provisions of the NDPR.

iv. **Monitoring and Analytics:** The compliance framework will ensure the proactive monitoring and evaluation of Personal Data provided by concerned entities by utilising analytic tools to identify patterns that reflect non-compliance.

3.2 Compliance Checklist for Data Controllers and Data Administrators

The following checklist should guide Data Controllers and Data Processors in enhancing compliance and reducing liabilities:

i. within twelve months of incorporation and then on an annual basis conduct a data protection audit: Article 3.1(7) of the NDPR provides what the audit report should contain;
ii. process data only on legally justifiable basis as provided in Article 2.2 of the NDPR;
iii. prepare and publish a privacy policy on every medium of Personal Data collection within 3 months of commencement of business operations. Article 2.5 provides for the publicity and clarity of Privacy Policy, which states- that any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand. The business process of each controller

would determine the medium and mode of publicizing the privacy policy.

iv. For example, an entity that does its business substantially through digital platforms is expected to have a privacy policy on its site and send messages to inform data subject of certain new developments requiring new or different consent. Publicity of the privacy policy may be fulfilled through any one or combination of the following:

- publication on the website;
- publication in a digital media;
- posted at conspicuous parts of the Data Controller's business premises;
- by reading or providing a copy to the Data Subject; or
- publication in any public media.

Where the privacy policy is not provided to or read to the Data Subject, the request for consent should explicitly refer the Data Subject to the privacy policy;

v. design and maintain systems to be data protection compliant: Data Controllers must show that their systems are built with data protection in mind, as provided in Article 2.6. Data Controllers are, therefore, expected to ensure continuous improvement of their information security architecture to prevent possible data breaches.

vi. continuous capacity building for members of staff, contractors, vendors, and relevant third parties;

vii. develop and circulate an internal data protection strategy or policy to help members of staff and vendors to understand the organisation's direction in connection with the collection and Processing of Personal Data and outline the steps they are to take to ensure the organisation's direction is achieved and maintained;

viii. conduct a Data Protection Impact Assessment ('DPIA') in accordance with the provisions of the NDPR: A DPIA is a process to identify, evaluate and minimise possible data protection risks in an existing or new business or organisational activity. Where the organisation intends to embark on a project that would involve the intense use of personal data, a DPIA should be conducted to identify possible areas where breaches may occur and devise a means of addressing such risks. Organisations are expected to conduct a DPIA on their processes, services and technology periodically to ensure continuous compliance;

ix. notify the NITDA of Personal Data breaches within 72 (seventy-two) hours of becoming aware of the breach;

x. appoint a data protection officer in accordance with the provisions of the NDPR and this Framework;

xi. update agreements with third party processors to ensure compliance with the NDPR;

xii. design system and processes to make data requests and access seamless for Data Subjects;

xiii. design systems and processes to enable Data Subjects to easily correct or update their Personal Data;

xiv. design system and processes to enable Data Subjects to easily transfer data to another platform or person (natural or artificial) at minimal costs;

xv. within the first 6 (six) month of incorporation and then on a biennial basis, train members of senior management and employees that collect and/or process Personal Data in the course of their duty, on Nigerian data protection laws and practices;

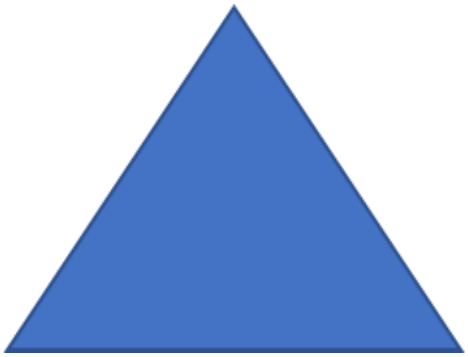
xvi. clearly communicate to Data Subjects the process for objecting to the processing of their Personal Data; and

xvii. outline the procedure for informing Data Subject and for protecting their rights, where an automated decision is being made on their Personal Data.

3.3 Compliance Approach

3.3.1 The compliance approach adopted by the NDPR was arrived at upon consideration of the historical deficits Nigeria has in the implementation of data protection. The approach is intended to bridge these deficits with the aim of ensuring compliance by all stakeholders in a business-friendly manner. The NDPR uses the triangular compliance model set out below:

NITDA (as National DPO)



Data Controller/Administrator **DPCO**

3.3.2 In this model, the NITDA would register DPCOs who will provide training, auditing and compliance services to data controllers and administrators. The criteria for licensing DPCOs is publicly accessible and such licensed DPCOs are listed on the NITDA website. Data Controllers who process the Personal Data of more than 2,000 Data Subjects in the 12-month period preceding 15th March (or such other date the NITDA may stipulate as the deadline for the filing of annual data protection audit reports), are expected to submit a report of their data protection audit to the NITDA on an annual basis.

3.4 Appointment of a Data Protection Officer

3.4.1 A Data Controller is required to appoint a dedicated Data Protection Officer ('DPO') within 6 months of commencing business or within 6 months of the issuance of this Framework, where one or more of the following conditions are present:

a) the entity is a government organ, ministry, department, institution or agency;

b) the core activities of the organisation involve the processing of the Personal Data of over 10,000 (ten thousand) Data Subjects per annum;

c) the organisation processes Sensitive Personal Data in the regular course of its business; and

d) the organisation processes critical national information infrastructure (as defined under the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 or any amendment thereto) consisting of Personal Data.

3.4.2 Notwithstanding the above, an organisation may voluntarily appoint a DPO.

3.5 Data Protection Officer in Multinational Company

The Nigerian subsidiary of a multinational company to which sections 3.4.1 or 3.4.2 above apply, shall appoint a DPO who shall be based in Nigeria and shall be given full access to the management in Nigeria. The DPO of the Nigerian subsidiary may report to a global DPO where such exists.

3.6 Liability of the DPO

Notwithstanding any contractual, civil or criminal liability, the DPO shall not be personally liable for the organisation's non-compliance with applicable data protection laws.

3.7 Qualities of a DPO

A DPO shall be chosen with due regard to the nature of the organisation's Processing activities and the data protection issues that arise within the organisation.

The DPO shall have:

a. professional expertise in Nigerian data protection laws and practices;
b. an in-depth understanding of applicable data protection laws; and
c. requisite knowledge to do the following:
    i. inform and advice the organisation, management, employees and third parties processors of their obligations under the NDPR;
    ii. monitor compliance with the NDPR and with the organisation's own data protection objectives;
    iii. assign responsibilities, raise awareness and train members of staff involved in processing operations;
    iv. advice on data protection impact assessment and monitor its performance; and
    v. liaise with the NITDA and/or the DPCO on data protection matters.

4. HANDLING PERSONAL DATA

4.1 Further Processing

4.1.1 According to Article 3.1(7)m: ***Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, the controller shall provide the Data Subject prior to that further processing with information on that other purpose, and with any relevant further information;***

Where a Data Controller wishes to further process Personal Data initially collected for a defined or limited purpose, the Data Controller shall consider the following:

a) whether there exists a connection between the original purpose and the proposed purpose;
b) the context in which the data was originally collected;
c) the nature of the Personal Data;
d) the possible impact of the new processing on the data subject; and
e) the existence of requisite safeguards for the Personal Data.

4.1.2 The above information shall be provided to the Data Subject before further processing is done. The further processing may be done if:

a) the Data Subject gives consent based on the new information;
b) the further processing is solely for the purpose of scientific research, historical research or for statistical purposes in the public interest; or
c) the further processing is required in compliance with a legal obligation.

4.2 Data Protection Impact Assessment

As stated in section 3.2 (viii) Data Controllers and Data Administrators are required to conduct DPIAs, where applicable. A DPIA is not compulsory for all Processing operations, however, it may be required for the following types of Processing:

a) evaluation or scoring (profiling);
b) automated decision-making with legal or similar significant effect;
c) systematic monitoring;
d) Sensitive Personal Data or Personal Data of a highly personal nature;

e) when Personal Data Processing relates to vulnerable or differently-abled data subjects; and

f) when considering the deployment of innovative processes or application of new technological or organizational solutions.

5. CONSENT

5.1 Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. Consent may be made through a written statement, sign or an affirmative action signifying agreement to the processing of personal data.

5.2 Principles governing Consent

The following principles shall govern the giving and obtaining of consent:

a) Transparency. There must be an explicit privacy policy stating the type of Personal Data collected, how the Personal Data is processed, who processes the Personal Data, the security standard implemented etc.;

b) No implied consent. Silence, pre-ticked boxes or inactivity does not constitute consent; and

c) No bundled consent. Separate data consent request from general terms and conditions. There must be consent for different types of data use class.

5.3 When Consent is required

5.3.1 Consent is required in the following circumstances:

a) for any direct marketing activity, except to existing customers of the Data Controllers who have purchased goods or services;

b) for the Processing of Sensitive Personal Data;

c) further processing;

d) for the Processing of the Personal Data of a minor;

e) before Personal Data obtained in Nigeria is Processed in a country which is not in the Whitelist.

f) before the Data Controller makes a decision based solely on automated Processing which produces legal effects concerning or significantly affecting the Data Subject.

5.3.2 Special category / higher standard consent: Explicit consent is required for the Processing of Sensitive Personal Data.

5.4 Types of Consent

a) Explicit Consent: Subject gives clear, documentable consent e.g. Tick a box, sign a form, send an email or sign a paper

b) Opt-in Consent: you are out, except you choose to opt-in. An example of opt-in consent is set out below:

I want to receive XXX newsletter ☐ If the box is left unticked, you will not receive the XXX newsletter

5.5 Processing of a Child's Data

A child for the purpose of the NDPR shall be any person below thirteen (13) years. A data controller or processor whose processing activity targets children shall ensure its privacy policy is made in a child-friendly form with the aim of making children and their guardians have clear understanding of the data processing activity before grant of consent.

5.6 Valid Consent Guide

a) Make your consent request prominent, concise, separate from other terms and conditions and easy to understand;

b) Include the name of your organisation and any third parties, why you want the data, what you will do with it and the right to withdraw consent at any time;

c) You must ask people to actively opt-in. Don't use pre-ticked boxes, opt-out boxes or default settings;

d) Wherever possible, give granular options to consent separately to different purposes and different types of processing;

e) Keep records to evidence consent- who consented, when, how and what they were told;

f) Make it easy for people to withdraw consent at any time they choose;

g) Keep consent under review and refresh it if anything changes; and

h) Build regular reviews into your business processes

5.6 Consent to Cookies

The Use of cookies on a website or other digital platforms requires consent. The consent must be freely given, informed and specific. Consent for cookies does not necessarily need the ticking of a box or similar methods; the continued use of a website which has met the following requirements suffices as consent.

i. the information must be clear and easy to understand;
ii. provision of the use and purpose of the cookies;
iii. appearance of the identity of the person or entity responsible for the use of the cookies;
iv. withdrawal of consent must be easily accessible and be described in the information; and
v. accessibility of this information by the user.

6. DATA PROTECTION AUDIT

6.1 Data protection audit is a systematic investigation or examination of the records, processes and procedures of Data Controllers and Processors,

to ensure that they are in compliance with the requirements of the NDPR and their data protection policies.

The NITDA may at its discretion:

a) carry out scheduled audits;
b) require report of audits as carried out by an organisation's DPCO; or
c) schedule "spot check" or "special audits" to ascertain compliance or identify breaches.

6.2 Usually these audits or investigations are unscheduled and may be random

6.3 The reasons for conducting a data protection audit include to:

a) assess the level of compliance with the NDPR;
b) evaluate compliance with the organisation's own data protection policy;
c) identify potential gaps and weaknesses in organisation's processes; and
d) give requisite advice and/or remedial actions for identified gaps.

6.4 Audit Periods

6.4.1 On annual basis, a Data Controller or Administrator who processed the Personal Data of more than 2,000 Data Subjects in a period of 12 months shall, not later than the 15th of March of the following year (or such extended period approved by the NITDA), submit a summary of its data protection audit to the Agency.

6.4.2 Non-filing of annual audit report by a Data controller or administrator who processed the personal data of more than 2000 data subjects in a period of 12 months, is a prima facie case of breach.

6.5 Filing Fees

Each Data Controller and Administrator is expected to file its audit report through a DPCO and pay the following amount as applicable[2]:

SN	Number of Data Subjects	Amount
1	Less than 2,000	N10,000
2	2,000 data subjects and above	N20,000

6.6 Content of Audit Report

6.6.1 The data protection audit shall contain the following information:

a) the identity and the contact details of the Data Controller or Administrator;
b) the contact details of the Data Protection Officer;
c) the purpose(s) of the processing for which the Personal Data are intended as well as the legal basis for the processing;
d) the legitimate interests pursued by the Controller or by a third party;
e) the recipients or categories of recipients of the Personal Data, if any;
f) where applicable, the fact that the Data Controller or Administrator intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by the NITDA;
g) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
h) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to Personal Data portability;

[2] The NITDA in its discretion may vary the applicable fees.

i) the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

j) the right to lodge a complaint with a relevant authority;

k) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such Personal Data;

l) the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;

m) the basis for further Processing (where applicable); and

n) where applicable, the basis for the transfer Personal Data to a recipient in a foreign country or international organisation by the Data Controller or Processor, and the existence or absence of an adequacy decision by the Agency.

6.6.2 A standard template for the audit report is attached as Annexure A to this Framework. It should be adopted by DPCOs in the course of audit implementation.

6.7 The Role of DPCOs in Data Audits

In the performance of data audits, DPCOs are responsible for:

a) evaluating the status of compliance by the organization. The NITDA expects DPCOs to base their findings on verifiable documents and practices;

b) appraising Data Subjects rights protection. The DPCO should be satisfied that the organisation has clear processes to protect the rights of the Data Subject;
c) assessing the level of awareness by top management, members of staff, contractors and customers of the NDPR;
d) identifying current or potential non-compliance; and
e) drawing up a remedial plan to remediate identified non-compliances.

6.8 Audit Verification Statement by DPCO

A DPCO shall make the following audit verification as a pre-condition to the filing of an annual audit report or any other report demanded by the NITDA.

I …… Of ……. a licensed Data Protection Compliance Organisation (DPCO) under Article 4.1(4) of the Nigeria Data Protection Regulation (NDPR) hereby make this statement on oath that the Data Audit Report herein filed by …… (Name of Organisation) is conducted in line with the NDPR and that it is an accurate reflection of the organisation's Personal Data management practice.

SIGN LICENSE NUMBER DATE

6.9 DPCO Terms of License

Every licensed DPCO shall:

i. abide by the provisions of the NDPR, this Implementation Framework and other related guidelines and frameworks as may be issued or directed by the NITDA from time to time;
ii. deliver service in a professional and ethical manner;

iii. ensure every information it provides to the NITDA about its client shall be factual and professional;
iv. not mishandle or withhold any Personal Data or asset of its client unlawfully in the course of its relationship with the client;
v. be held liable, if found to have conspired to provide false and misleading information in an audit filing or communication.

6.10 AUDITOR'S CODE OF CONDUCT

Every DPCO shall ensure all its members of staff are aware of the ethical considerations in the performance of an audit under the NDPR. As part of the licensing process, the NITDA shall verify that a DPCO is registered with a professional association that regulates the ethical conduct of its members, in order to ensure a standardised service delivery. The following are basic ethical expectations required of DPCOs in the conduct of their business.

a) Confidentiality - The DPCOs and its Client must execute a binding non-disclosure agreement before embarking on audit process. This will ensure that the information and data of the client is kept confidential.
b) Conflict of Interest - DPCOs shall not audit a client if it amounts to a conflict of interest. For example, a DPCO that designed the data protection system should not conduct a data audit. A DPCO that is engaged to provide financial or systems audit may also perform data audit, provided that such DPCO is neither retained as the outsourced Data Protection Officer nor responsible for the implementation of the data protection compliance of the same organisation.
c) Honesty - DPCOs must state verifiable facts and not conjectures, half-truths or concealed facts. The essence of the audit is not to sanction organisations, but to provide an insight on how the country's cyber and information management practices can be

improved. Any established falsehood in an audit report or communication to the NITDA by the DPCO, and which falsehood was known to the DPCO at the time of preparing such report or communication; is a ground for the immediate withdrawal of the DPCO's license

d) Professionalism - DPCOs must perform the service with the highest level of professionalism and carry out continuous capacity building for its members of staff, which is a prerequisite for relicensing by the NITDA. DPCOs must not undertake any work for which they lack the requisite skills, manpower and capacity.

7. TRANSFER OF PERSONAL DATA ABROAD

7.1 The following information is required where data is being transferred abroad, as stipulated in Article 2.11:

a) the list of countries where the Personal Data of Nigerian citizens and residents is being transferred in the regular course of business;
b) the data protection laws of the relevant data protection office/administration of such countries listed in (i) above;
c) the privacy policy of the Data Controller, which is NDPR-compliant;
d) an overview of the encryption method and data security standards; and
e) any other detail that assures the privacy of Personal Data is adequately protected in the target country.

7.2 The NITDA shall coordinate transfer requests with the office of the Attorney-General of the Federation ('AGF'). A 'white-list' of jurisdictions (the 'White List') has been compiled and is set out in Annexure C to this Framework. Where transfer to a jurisdiction outside the White List is being sought, the Data Controller shall ensure there is a verifiable

documentation of consent to one or more of the exceptions stated in Article 2.12 of the NDPR.

7.3 Data Transfer to subsidiaries or headquarters outside Nigeria

Where an organization seeks to transfer personal data to another entity within its group of companies or an affiliate company, it would suffice for the organization to provide a Binding Corporate Rule which shall be included in the data audit report or submitted separately to the NITDA. The Binding Corporate Rule may be stated in the Company's Data Privacy Policy.

8. RETENTION OF RECORDS

8.1 The Regulation does not explicitly provide for a time period for the retention of data, because the retention period in certain scenarios may be subject to existing laws or contractual agreements. Every data Controller and Administrator shall specify the duration of storage clearly in its terms of service or other binding document.

8.2 Where the retention period of Personal Data is not specified in the contract between the parties or by applicable law, the retention period shall be:

a) 3 (three) years after the last active use of a digital platform
b) 6 (six) years after the last transaction in a contractual agreement
c) Upon presentation of evidence of death by a deceased's relative
d) immediately upon request by the Data Subject or his/her legal guardian where (i) no statutory provision provides otherwise and (ii) the Data Subject is not the subject of an investigation or suit that may require the Personal Data sought to be deleted.

The NITDA would consider the above and other circumstances to determine if the data was stored appropriately and for a reasonable length of time.

8.3 Personal Data that is no longer in use or which has been retained beyond the requisite statutorily required storage period, shall be destroyed in line with global best practices for such operations. Evidence of destruction of data shall be a valid defence against future allegation of breach by a Data Subject.

9. DATA PRIVACY BREACH

9.1 In line with Article 4.1(8) and other relevant provisions, Data Subjects, civil societies or professional organisations or any government Agency may report a breach of this Regulation to the NITDA through any of the advertised channels. Upon receipt of this report, the Director General/CEO of the NTDA may direct action to be taken which may include any of the following:

a) contacting the organisation for enquiry;
b) reviewing earlier filed annual report (if any);
c) issuing a data protection regulation compliance query;
d) commencing administrative action; and
e) prosecution

9.2 Data Controllers have a duty of self-reporting Personal Data breaches to the NITDA within 72 hours of knowledge of such breach . This timeline should be documented in the organisation's data protection policy and data privacy policy.

9.3 A notification of data breach to the NITDA must include the following information:

a) a description of the circumstances of the loss or unauthorised access or disclosure;

b) the date or time period during which the loss or unauthorised access or disclosure occurred;

c) a description of the personal information involved in the loss or unauthorised access or disclosure;

d) an assessment of the risk of harm to individuals as a result of the loss or unauthorised access or disclosure;

e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

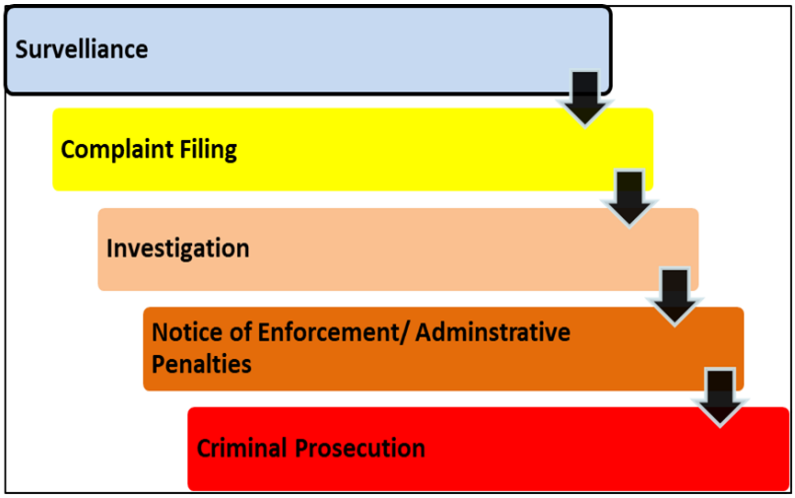
g) a description of any steps the organisation has taken to notify individuals of the loss or unauthorized access or disclosure, and

h) the name and contact information for a person who can answer, on behalf of the organization, the agency's questions about the loss of unauthorized access or disclosure.

9.4 The Data Controller should immediately notify the Data Subject of the Personal Data breach where the personal data breach will likely result in high risks to the freedoms and rights of the data subject.

10. ENFORCEMENT FRAMEWORK

10.1 Forms of Enforcement



10.1.1 Surveillance

Surveillance refers to specific, deliberate monitoring carried out to identify breach of the NDPR. This routine activity arises out of the understanding that operators or parties are legally obliged to perform specific tasks in order to comply with provisions of NDPR, particularly as it affects Data Subjects. Such Controllers may be in deliberate or unconscious breach of the Regulation. Surveillance will aid the NITDA to identify breaches of regulatory instruments or co-opt other stakeholders to identify and report breaches to the Agency.

10.1.2 Complaint Filing

Any person who believes a party is not complying with any of the provisions of the Regulation may file a complaint with the NITDA. Such complaints must meet the following requirements:

a) a complaint must be filed in writing, either on paper or electronically.

b) a complaint must name the Data Controller or Administrator that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable provision(s).

c) the NITDA may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing.

10.1.3 Investigation

The NITDA will investigate any complaint filed against a Data Controller or Administrator when a preliminary review of the facts indicates a possible violation of the provision(s) of the NDPR. The NITDA may by its officers or through designated DPCO, investigate any complaint filed by third parties and may also do so based on a special audit check or "spot check". Investigation may include a review of the policies, procedures, or practices of the concerned entity and of the circumstances regarding any alleged violation. At the time of the initial written communication with the concerned entity, the NITDA will indicate the basis of the audit.

10.1.4 Administrative Sanctions

Where the NITDA has ascertained through the foregoing tools of enforcement or by the Administrative Redress Panel established, pursuant to Article 4.2 of the NDPR, that a party is in breach the NITDA may issue an order for compliance with relevant provisions to curtail further breach. The NITDA or a court of competent jurisdiction may prescribe additional sanction in liquidated monetary sum. A decision on the money value shall be based on the following considerations:

a) Nature, gravity and severity of the breach
b) the number of data subjects affected,
c) damage suffered by data subjects
d) opportunity for curtailment left unexplored and
e) whether the breach is the first by the offending entity.

The NITDA may also issue other administrative orders to include:

a) Suspension of service pending further investigations;
b) Order for parties in breach to appear before a panel to determine liability of officers in line with Article 4.2;

c) Issue public notice to warn the public to desist from patronizing or doing business with the affected party;

d) Refer the parties in breach to other Self-Regulatory Organization for appropriate sanctions.

10.1.5 Criminal Prosecution

Where the NITDA has determined that a party is in breach of the NDPR, especially where such breach affects national security, sovereignty and cohesion, it may seek to prosecute officers of the organization as provided for in section 17(1) and (3) of the NITDA Act 2007. The NITDA shall seek a fiat of the Honourable Attorney General of the Federation or may file a petition with any authority in Nigeria, this may include; the Economic and Financial Crimes Commission, the Department of State Security, the Nigerian Police Force, the Independent Corrupt Practices (and other related offences) Commission or the Office of National Security Adviser.

10.2. Enforcement Process

Enforcement Activity	Description of Action
Documentation of Breach	1. At this stage it is required that a report, memo, petition or complaint is officially submitted to the NITDA through the office of the Director General of the NITDA. 2. The Document must be duly signed by an Officer of the NITDA or the external complainant.

	3. For external complaint, the document must be written and signed by an Individual either in personal capacity or a group (of persons or companies) or registered entity (registered with the CAC). 4. Complaint filing through social media or other digital media shall be accepted if the necessary requirements in section 10.1.2 are observed.
Request for Additional Information and Investigation	If it appears the NITDA is not sufficiently briefed or may need further information to arrive at a conclusion of breach of the NDPR, the following procedure would be employed: i. **"Request for Additional Information"** would be issued to either the complainant, the alleged violator or any other party who may be in a position to provide clarity on facts of the allegation of breach. ii. Invite relevant parties for an "**Investigation Meeting**" to elicit facts to establish or disprove breach. iii. Request for Investigation in partnership with law enforcement agencies.
Continuation or Termination of Enforcement Process	Where the NITDA is satisfied that there is a *prima facie* evidence of breach, the NITDA may: 1. Request for a response from the violator stating the allegations against them; 2. In the event that the NITDA finds the explanations of the

	alleged violator coherent and sufficient, the NITDA may discontinue the enforcement process
Notice of Enforcement	Where the NITDA is satisfied that a breach of NDPR has occurred; 1. The NITDA will then issue a **"Notice of Enforcement"** citing the specific breach and demand mandatory compliance within a specific time frame from the date of the service of notice. 2. The NITDA may issue an administrative fine or penalty in line with extant laws.
Issuance of Public Notice (OPTIONAL)	The NITDA may consider issuing a public statement warning the public and other agencies of Government of the dangers of dealing with a violator who has perpetuated a breach of the NDPR.
Request of Prosecution	A. Where a violator does not take steps to address breach or consult with the NITDA as to what steps to be taken to remedy breach after the period stated in the **"Notice for Enforcement"**; or B. The NITDA may file an official Petition or **Notice of Prosecution** to the Office of the Attorney General of the Federation, stating the following: I. Original complaint; II. Enforcement process initiated by the NITDA; and III. Implication of the action of the violator to the development of ICT in Nigeria. IV. A copy of the notice will be copied to the Presidency and any other relevant organ of government.

11. ESTABLISHMENT OF ADMINISTRATIVE REDRESS PANEL

11.1 Pursuant to Article 4.2 of the Regulation, the NITDA shall establish Administrative Redress Panels (ARP), for the purpose of resolving issues related to the Regulation. The ARP shall be composed of accomplished information technology professionals, public administrators and legal practitioners who shall work with the Agency

11.2 The ARP procedure shall give preference to an online dispute resolution mechanism. Where it is impracticable to adopt such mechanism, the ARP panel shall be convened at a physical venue.

11.3 The ARP shall give its opinion within a stipulated period of time.

11.4 The rules of procedure of the ARP shall be drawn up by a panel of experts. The ARP procedure shall be drafted with the following in mind:

a) principles of fair hearing, fairness and transparency;
b) arguments and case presentations shall be done in writing. The procedure shall limit oral presentation to the barest minimum;
c) the ARP shall in reaching its decision, clearly state the proof of violation, identify some or all the Data Subjects affected by the breach (in an anonymized, pseudonymized or summarized format), the provision of the Regulation violated and any acts of omission or commission which exacerbated the breach; and
d) in reaching its decision, the Panel may consider whether the indicted entity has a reputation for data or other criminal or corporate breaches in the past; the number of employees in the establishment; the impact of the fine on the entity's overall contribution to the economy.

12. THIRD PARTY PROCESSING

12.1 Third Party processors may include Data Administrators and other statutory or non-statutory data recipients whom the Data Controller sends data to for the purpose of delivering service to the Subject.

12.2 Data Controllers are required to publish a list of third parties with whom the Data Subject's Personal Data may be shared. This publication which must also be included in the audit report should include:

a) categories of third-party data recipients e.g. credit reference agencies; payment processors; insurance brokers; anti-corruption agencies etc.;
b) name of the third party;
c) jurisdiction of the third party;
d) the purpose of the disclosure e.g. fraud checking; payment processing; dispute management; risk management; statutory requirement etc.; and
e) the type of data disclosed e.g. name, phone number, address, payment details etc.

12.3 Third Party processors shall be obligated to comply with the NDPR or any other adequate data protection law existent in their country. The third-party processors are required to do the following:

a) process data only based on authorisation expressly granted by the Data Controller through a written agreement that specifies the roles and obligations of each party in respect to data protection;
b) ensure there is adequate information security and process measures to protect the Personal Data being processed;
c) where requested by the Data Subject, the third-party processor shall rectify grant access or delete such Personal Data on the instruction of the Data Controller.

13. DATA PROTECTION IN MDAS

13.1 The NITDA shall deploy strategies and programmes to improve electronic governance in public institutions. All Public Institutions (PIs) shall comply with the *Guidelines for the Management of Personal Data by Public Institutions* in Nigeria 2020, issued by the NITDA in May 2020. The NITDA shall coordinate the process of improving Data Protection in PIs through training and process change management.

13.2 Every PI shall publish a privacy policy on its website and any other digital media platform through which it collects Personal Data. A sample Privacy Policy for PIs is available in Annexure B for guidance.

13.3 Every MDA shall designate a Directorate-level officer as its Data Protection Officer. Such person shall be responsible for:

- informing and advising the MDA on compliance with NDPR and other applicable data protection laws and policies;
- monitoring compliance with the Regulation and with the internal policies of the PI including assigning responsibilities, awareness raising and training members of staff; and
- facilitating the cooperation with relevant stakeholders and acting as the liaison between the PI and the NITDA.

14. RELATIONSHIP WITH THE ATTORNEY-GENERAL OF THE FEDERATION

14.1 In accordance with Article 2.12 of the NDPR, where a Data Controller or Data Administrator seeks to transfer Personal Data to a foreign country or an international organisation, the NITDA shall examine if such country has adequate data protection law or regulation that can guarantee minimum privacy for the Personal Data of Nigerian citizens and residents. Where there is need for further legal cooperation from a target

country, the NITDA may approach the office of Attorney-General for that purpose. In such circumstance, such data transfer and storage processes shall be done under the supervision of the Attorney-General.

14.2 Generally, an adequacy decision shall be issued by the NITDA in respect of transfer to foreign countries if the information specified in paragraph 6 above is satisfactorily provided by the Data Controller or Administrator.

14.3 An adequacy decision permits a cross-border transfer of Personal Data outside Nigeria or the onward transfer from or to a party in a jurisdiction in the White List. The Attorney General of the Federation may in its supervisory role prohibit the transfer of the Personal Data of Nigerian citizens or residents. to certain countries where it is of the opinion that the country's data protection regime is inadequate or incompatible with Nigerian law.

14.4 The White List shall be validated by the Attorney-General of the Federation. A Data Controller or Administrator may transfer Personal Data to any country on the White List provided the organisation complies with the other provisions of the NDPR.

14.5 The transfer of data to any country other than the ones listed, by a Data Controller or Administrator in its request for an adequacy decision, shall be subject to further processes to ascertain the protection of the Personal Data of Nigerian citizens and residents.

15. CONTINUOUS PUBLIC AWARENESS AND CAPACITY BUILDING

The NITDA shall organise or facilitate seminars, workshops, conferences and other information dissemination programmes periodically, to improve public awareness, acceptance and compliance with applicable data protection laws.

16. APPLICATION OF INTERNATIONAL LAWS

Where the NDPR and this Framework do not provide for a data protection principle or process, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and European Union General Data Protection Regulation (EU GDPR) and its judicial interpretations shall be of persuasive effect in Nigeria.

ANNEXURE A

AUDIT TEMPLATE FOR NDPR COMPLIANCE

A. This template is a guideline for Data Controllers and Administrators to show evidence of compliance. The template may be modified in so far as the essence of the reporting is achieved in a concise but comprehensive manner.

B. Responses must be evidenced with documentary evidence.

C. False reporting is a criminal offence. The Data Controller and the DPCO shall be jointly liable except otherwise proven.

D. NITDA may review the audit questions and communicate such update to DPCOs from time to time

No	NDPR Provision	Question	Response	Comments
1		**Accountability and governance**		
1.1	Article 4.1(6) and (7)	Did you process the personal data of: a. more than 1,000 (one thousand) Data Subjects in the last 6 months; or b. more than 2,000 Data Subjects in the last 12 months?		
1.2	Article 1.1 and 1.2	Is your top-management aware of the Nigeria Data Protection Regulation (NDPR) and the potential implication on your organisation?		
1.3	Article 2.6	Have you implemented any information security standard in your organisation before? If YES, specify.		
1.4	Article 2.1(d)	Do you have a documented data breach incident management procedure?		
1.4#5	Article 1.2	Do you collect and process personal information through digital mediums?		
1.6	Article 2.6	Have you organised any NDPR awareness seminar for your members of staff or suppliers?		
1.7	Article 4.1(5)	Have you conducted a detailed audit of your privacy and data protection practices?		

1.8	Article 2.5	Have you set out the management support and direction for data protection compliance in a framework of policies and procedures?		
1.9	Article 2.1	Do you have a Data Protection compliance and review mechanism?		
1.10	Article 2.6	Have you developed a capacity building plan for compliance with data protection for all members of staff?		
1.11	Article 3.1(1)	Do you know the types of personal data you hold?		
1.12	Article 4.1(5)	Do you know the sources of the personal data you hold?		
1.13	Article 4.1(5)	Who do you share personal data with		
1.14	Article 4.1(2)	Who is responsible for your compliance with data protection laws and processes		
1.15	Article 1.3	Have you assessed whether you are a Data Controller or Data Processor?		
1.16	Art 4.1(5)	Have you reviewed your Human Resources policy to ensure personal data of employees are handled in compliance with the NDPR?		
1.17	Article 2.5(d)	Have appropriate technical and organisational measures been implemented to show you have considered and integrated data protection into your processing activities?		
1.18	Article 4.5	Do you have a policy for conducting Data Protection Impact Assessment (DPIA) on existing or potential projects?		

1.19	Article 4.5	Does your DPIA Policy address issues such as: a) A description of the envisaged processing operations b) The purposes of the processing c) The legitimate interest pursued by the controller d) An assessment of the necessity and proportionality of the processing operations in relation to the purposes e) An assessment of the risks to the rights and freedoms of Data Subject f) Risk mitigation measures being proposed to address the risk		
2		**DATA PROTECTION OFFICER/DATA PROTECTION COMPLIANCE ORGANISATION**		
	Article 4.1(4)	Have you appointed a Data Protection Compliance Organisation (DPCO)?		
	Article 4.1(4)	Which kind of service has a DPCO provided for you till date? *Hint- Audit, Data Protection Impact Assessment, Data Breach Remediation etc*.		
	Article 4.1(2)	Does your DPCO also perform the role of your DPO?		
2.1	Article 4.1(2)	Has a Data Protection Officer (DPO) been appointed and given responsibility for NDPR compliance and the management of organisational procedures in line with the requirements of NDPR?		
	Article 4.1(4)	Do you utilise the same DPCO for Data Protection compliance implementation and audit?		
2.2	Article 4.1(3)	Have you trained your Data Protection Officer in the last one year?		
	Article 4.1(2)	Does the Data Protection Officer (DPO) have sufficient access, support and the budget to perform the role?		
	Article 4.1(2)	If the DPO has other job functions, have you evaluated whether there is no conflict of interest?		

	Article 4.1(2)	Does the DPO have verifiable professional expertise and knowledge of data protection to do the following: a) To inform and advice the business, management, employees and third parties who carry out processing, of their obligations under the NDPR b) To monitor compliance with the NDPR and with the organisation's own data protection objectives c) Assignment of responsibilities, awareness-raising and training of members of staff involved in processing operations d) To provide advice where requested as regards the data protection impact assessment and monitor its performance e) To cooperate with the NITDA as the Supervisory Authority f) To act as the contact point for the NITDA on issues relating to data processing		
2.3	Article 2.5	Is there a clearly available mechanism (e.g. webpage, etc.) for data subjects that explains how to contact your organisation to pursue issues relating to personal data?		
3		**DOCUMENTATION TO DEMONSTRATE COMPLIANCE**		
3.1	Article 3.1	Have you documented your data processing activities?		
3.2	Article 2.5	Have you included an appropriate privacy notice in each data collection process, including those done through third parties?		
	Article 4.1(5)	Have you agreed a schedule to review current privacy notices contracts for compliance with NDPR?		
3.3	Article 2.2	Other than the grounds of Consent of an employee, has your organisation recorded other legal grounds on which it processes its employees' data?		
3.4	Article 4.1(5)	Have you identified what personal data is collected and whether this is collected directly from the data subject or via a third party?		
	Article 3.1(7)	Does this inventory include data retention periods or do you have a separate data retention schedule?		

3.5	Article 1.3	Do you have a register of data breaches and security incidents?		
4	**PROCESSING ACTIVITIES**			
4.1	Article 2.2	Have you carried out a comprehensive review of the various types of processing your organisation perform?		
	Article 2.2	Have you identified lawful basis for your processing activities and documented this?		
	Article 2.5	Have you explained the lawful basis for processing personal data in your privacy notice(s)?		
4.2	Article 2.5	Have you reviewed how you seek, record and manage consent?		
	Article 4.1	Have you reviewed the systems currently used to record consent and have you implemented appropriate mechanisms to ensure an effective audit trail?		
4.3	Article 2.4	If your organisation offers services directly to children, have you communicated privacy information in a clear, plain way that a child will understand?		
	Article 2.6	Do you adopt data pseudonymisation, anonymisation and encryption methods to reduce exposure of personal data?		
4.4	Article 1.3(xix)	Have you identified all the points at which personal data is collected: websites, application forms (employment and other), emails, in-bound and out-bound telephone calls, CCTV, exchanges of business cards and, attendance at events etc?		
4.5	Article 3.1 (8)	Do you have procedures for regularly reviewing the accuracy of personal data?		
	Article 3.1(8)	Do you have a system for Data Subjects to erase or amend their personal data in your custody?		
4.6	Article 2.5(d)	Have you identified all the ways in which personal data is stored, including backups?		
	Article 2.1.1(a)	Have you evaluated points where data minimisation can be implemented in your data collection process?		

		Have you reviewed your forms and other data collection tools to comply with the NDPR?		
4.7	Article 2.2	Have you identified the purposes for processing personal data, for determining and authorising internal or external access and all disclosures of data?		
4.8	Article 3.1	Are your organisational procedures checked to ensure that you can preserve the rights of individuals under the NDPR?		
4.9	Article 3.1(7)	Is there a clearly available mechanism (e.g. webpage, etc.) for data subjects that explains how to contact the organisation to pursue issues relating to personal data?		
4.10	Article 2.6	Are all members of staff trained to recognise and deal with subject access requests?		
4.11	Article 3.1(5)	Do you have a procedure for dealing with subject access requests from third parties?		
4.12	Article 4.1(5)	Has your organisation implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively?		
4.13	Article 4.1(5)	Do you have mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms?		
4.14	Article 2.6	Have you trained all members of staff who deal with personal data about their responsibilities and data protection procedures?		
4.15	Article 2.6	Are these responsibilities written into job descriptions?		
4.16	Article 2.7	Have you contracted with any third-party data processors?		
4.17	Article 2.7	If so, are such contracts compliant with the requirements of the NDPR?		
4.18	Article 2.7	Have you agreed a schedule to review current contracts for compliance with NDPR?		
4.19	Article 2.10	Do you transfer personal data to organisations in countries outside the Nigeria?		

4.20	Article 2.10	If so, do you have in place appropriate contracts and methods of ensuring compliance?		
4.21	Annexure C	Are the countries you transfer data to in the White List of Countries with adequate Data Protection laws?		
4.22	Article 2.12	Where the countries are not in the White List have you recorded the basis of transfer?		
4.23	Article 4.1(5)f	Do you have in place adequate information systems security (e.g. as specified in ISO/IEC 27001) and does it include physical, logical, technical and operational measures that ensure the security of processing of personal data?		
4.24	Article 2.6	Are members of staff aware that unauthorised access to information is prohibited?		
4.25	Article 2.6	Are members of staff aware that any Personal Data acquired in the course of their employment remains confidentiality even after their exit the organisation?		

ANNEXURE B

SAMPLE PRIVACY POLICY TEMPLATE FOR PUBLIC INSTITUTIONS

NITDA Privacy Policy

This Privacy policy between the National Information Technology Development Agency of 28 Port Harcourt Crescent, off Gimbiya Street, Garki, Abuja (hereinafter referred to as the ”NITDA”) and you, constitutes our commitment to your privacy on our administrative records, websites, social media platforms and premises.

1.0 Your Privacy Rights

1.1 This Privacy Policy describes your privacy rights regarding our collection, use, storage, sharing and protection of your personal information. It applies to the NITDA website and all database, applications, services, tools and physical contact with us, regardless of how you access or use them.

1.2 If you have created a username, identification code, password or any other piece of information as part of our access security measures, you must treat such information as confidential, and you must not disclose it to any third party.

1.3 We reserve the right to disable any user identification code or password, whether chosen by you or allocated by us, at any time, if in our opinion you have failed to comply with any of the provisions of this privacy policy.

1.4 If you know or suspect that anyone other than you know your security details, you must promptly notify us at dpo@nitda.gov.ng.

2.0 Consent

You accept this privacy policy when you give consent upon access to our platforms, or use our services, content, features, technologies or functions offered on our website, digital platforms or visit any of our offices for official or non-official purposes (collectively the “NITDA Services”). This privacy policy governs the use of the NITDA Services and intervention projects by our users and stakeholders, unless otherwise agreed through a written contract. We

may amend this privacy policy at any time by posting a revised version on our website, or placing such notice at conspicuous points at our office facilities. The revised version will be effective 7 days after publication.

3.0 Your Personal Information

3.1 When you use the NITDA Services, we collect information sent to us by your computer, mobile phone or other electronic access device. The automatically collected information includes but is not limited to data about the pages you access, computer IP address, device ID or unique identifier, device type, geo-location information, computer and connection information, mobile network information, statistics on page views, traffic to and from the sites, referral URL, ad data, standard web log data, still and moving images.

3.2 We may also collect information you provide us including but not limited to-information on web form, survey responses account update information, email address, phone number, organization you represent, official position, correspondence with the NITDA support services, and telecommunication with the NITDA. We may also collect information about your transactions, enquiries and your activities on our platform or premises.

3.3 We may also use information provided by third parties like social media sites. Information about you provided by other sites are not controlled by the NITDA and we are, therefore, not liable for how such third parties use your information.

4.0 What we do with your personal information

The purpose of our collecting your personal information is to give you efficient, enjoyable and secure service. We may use your information to:

a) provide the NITDA Services and support;
b) process applications and send notices about your transactions to requisite parties;
c) verify your identity;
d) resolve disputes, collect fees, and troubleshoot problems;

e) manage risk, or to detect, prevent, and/or remediate fraud or other potentially prohibited or illegal activities;
f) detect, prevent or remediate violation of laws, regulations, standards, guidelines and frameworks;
g) improve the NITDA Services by implementing aggregate customer or user preferences;
h) measure the performance of the NITDA Services and improve content, technology and layout;
i) track information breach and remediate such identified breaches;
j) manage and protect our information technology and physical infrastructure; or
k) contact you at any time through your provided telephone number, email address or other contact details.

5.0 Cookies

Cookies are small files placed on your computer's hard drive that enables the website to identify your computer as you view different pages. Cookies allow websites and applications to store your preferences in order to present contents, options or functions that are specific to you. Like most interactive websites, our website uses cookies to enable the tracking of your activity for the duration of a session. Our website uses only encrypted session cookies which are erased either after a predefined timeout period or once the user logs out of the platform and closes the browser. Session cookies do not collect information from the user's computer. They will typically store information in the form of a session identification that does not personally identify the user.

6.0 How we protect your personal information

We store and process your personal information on our computers in Nigeria. Where we need to transfer your data to another country, such country must have an adequate data protection law. We will seek your consent where we need to send your data to a country without an adequate data protection law. We protect your information using physical, technical, and administrative security measures to reduce the risks of loss, misuse, unauthorized access,

disclosure and alteration. Some of the safeguards we use are firewalls and data encryption, physical access controls to our data centres, and information access authorization controls.

7.0 How We Share your information within the NITDA and with Other Users

7.1 During your interaction with our website or premises, we may provide other Ministries, Departments, Agencies (MDA), other organs of government, private sector operators performing government functions, with information such as your name, contact details, or other details you provide us for the purpose of performing our statutory mandate to you or third parties.

7.2 We work with third parties, especially government agencies to perform the NITDA Services and implement its mandate. In doing so, a third party may share information about you with us, such as your email address or mobile phone number.

7.3 You accept that your pictures and testimonials on all social media platforms about the NITDA can be used for limited promotional purposes by us. This does not include your trademark or copyrighted materials.

7.4 From time to time we may send you relevant information such as news items, enforcement notice, statutorily mandated notices and essential information to aid the implementation of our mandate. We may also share your personal information in compliance with national or international laws; crime prevention and risk management agencies and service providers.

8.0 Security

8.1 We will always hold your information securely. To prevent unauthorised access to your information, we have implemented strong controls and security safeguards at the technical and operational levels. Our website uses Secure Sockets Layer/Transport Layer Security (SSL/TLS) to ensure secure transmission of your Personal Data. You should see the padlock symbol in your URL address bar once you are successfully logged into the platform. The URL address will also start with https:// depicting a secure webpage. SSL applies encryption between two points such as your PC and the connecting

server. Any data transmitted during the session will be encrypted before transmission and decrypted at the receiving end. This is to ensure that data cannot be read during transmission.

8.2 The NITDA has also taken measures to comply with global Information Security Management Systems. We, have, therefore, have put in place digital and physical security measures to limit or eliminate possibilities of data privacy breach incidents.

9.0 Data Confidentiality Rights

Your information is regarded as confidential and will not be divulged to any third party, except under legal and/or regulatory conditions. You have the right to request sight of, and copies of any and all information we keep on you, if such requests are made in compliance with the Freedom of Information Act and other relevant enactments. While the NITDA is responsible for safeguarding the information entrusted to us, your role in fulfilling confidentiality duties includes, but is not limited to, adopting and enforcing appropriate security measures such as non-sharing of passwords and other platform login details, adherence with physical security protocols on our premises, dealing with only authorized officers of the Agency.

10.0 Links to Other Websites and Premises

10.1 Certain transaction processing channels may require links to other websites or organisations other than ours. Please note that the NITDA is not responsible and has no control over websites outside its domain. We do not monitor or review the content of other party's websites which are linked from our website or media platforms.

10.2 Opinions expressed or materials appearing on such websites are not necessarily shared or endorsed by us, and the NITDA should not be regarded as the publisher of such opinions or materials.

10.3 Please be aware that we are not responsible for the privacy practices, or content of these sites.

10.4 We encourage our users to be aware of when they leave our site, and to read the privacy statements of these sites. You should evaluate the security and trustworthiness of any other site connected to this site or accessed through this site yourself, before disclosing any personal information to them.

10.5 The NITDA will not accept any responsibility for any loss or damage in whatever manner, howsoever caused, resulting from your disclosure to third parties of personal information.

11.0 Governing Law

This privacy policy is made pursuant to the Nigeria Data Protection Regulation 2019 and other relevant Nigerian laws, regulations or international conventions applicable to Nigeria. Where any provision of this Policy is deemed inconsistent with a law, regulation or convention, such provision shall be subject to the overriding law, regulation or convention.

ANNEXURE C

COUNTRIES WITH ADEQUATE DATA PROTECTION LAWS

SN	COUNTRY	DATA PROTECTION LAW	COMMENT
1	All EU and European Economic Area Countries	EU- General Data Protection Regulation	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy Latvia, Lithuania, Luxembourg, Malta, Netherlands Norway, Poland, Portugal, Romania, Serbia Slovakia, Slovenia, Spain, Sweden United Kingdom. Every Country has a Supervisory Authority for the implementation of the GDPR in its domain.
2	All African Countries who are signatories to the Malabo Convention 2014	African Union Convention on Cyber Security and Personal Data Protection	The Convention is still open to signature and adoption by AU member countries
2	Algeria	2018 Algerian law on the Protection of Individuals in the Processing of Personal Data	Autorité National de Protection des Données à Caractère Personnel
3	Argentina	Personal Data Protection Law 2000 (Law No. 25,326) applies to any person or entity in the country that deals with personal data.	Agency for Access to Public Information established pursuant to Decree 746 of 2017
	Benin	Benin Digital Code	Autorité de protection des données à caractèrepersonnelles (APDP),
4	Brazil	General Data Protection Law 2018 (LGPD) very similar to GDPR. Brazil also has snippets of privacy laws from the Constitution and other statutes such as Consumer Protection Code 1990; Internet Act 2014 etc.	The Amended LGPD created the National Data Protection Authority (ANPD). The law would take effect in August 2020
5	Mauritius	THE DATA PROTECTION ACT 2017	Mauritius Data Protection Office
6	South Africa	The Protection of Personal Information, Act 4 of 2013	The Information Regulator (DPA)
7	Togo	Protection of Personal data	Togolese Data Protection Authority
8	Tunisia	The Organic Law no. 2004-63 on Personal Data Protection (Tunisian Law)	The National Authority for Protection of Personal Data (DPA)
9	Canada	Private sector is governed by Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 amended in 2008 to include mandatory data breach notification and record-keeping laws. the public sector is governed by the Privacy Act of 1983.	PIPEDA creates the Office of the Privacy Commissioner of Canada
10	Cape Verde	Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013) and Law 132/V/2001, of 22 January 2001.	The National data protection authority in Cape Verde is the Comissão Nacional de Proteção de Dados Pessoais ('Data Protection Authority').
11	China	Information Technology – Personal Information Security Specification is the latest law on privacy in China. It came into effect in May 2018	Cyberspace Administration of China (CAC) is the data protection authority
12	Cyprus	The Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018.	Commission for personal data protection
13	Israel	The Privacy Protection Regulations (Data Security), 5777-2017,	The Israel Privacy Protection Authority (PPA)
14	Japan	Act on the Protection of Personal Information (APPI)	Personal Information Protection Commission Japan
15	Philippines	Republic Act no. 10173	National Privacy Commission
16	Singapore	Personal Data Protection Act of 2012 (No. 26 of 2012) (the Act)	Personal Data Protection Commission

17	South Korea	The Personal Information Protection Act (PIPA)	Personal Information Protection Commission (PIPC)
18	Albania	Law No. 9887 dated 10.03.2008	Information and Data Protection Commissioner (IDP)
19	Andorra	Law 15/2003 of 18	Data Protection Agency of Andorra
20	Austria	GDPR	Austrian Data Protection Authority
21	Bosnia-Herzegovina	The Law on Protection of Personal Data ('Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) (DP Law)	Personal Data Personal Data Protection Agency in Bosnia and Herzegovina
22	Croatia	Implementation of the General Data Protection Regulation	Croatian Personal Data Protection Agency
23	Faeroe Islands	Data Protection Act	Faroese Data Protection Agency
24	Isle of Man	DATA PROTECTION ACT 2018 Data Protection (Application of GDPR) Order 2018 (SD2018/0143) (GDPR Order) Data Protection (Application of LED) Order 2018 (SD2018/0144) (LED Order) GDPR and LED Implementing Regulations 2018 (SD2018/0145) (Implementing Regulations)	Office of the Data Protection Supervisor
25	Jersey	Data Protection (Jersey) Law, 2018 (DPJL) Data Protection Authority (Jersey) Law, 2018 (DPAJL)	Jersey Office of the Information Commissioner (JOIC)
26	Liechtenstein	Data Protection Act (DSG) of 14 March 2002 (LR-No. 235.1)	The Liechtenstein Data Protection Authority / Datenschutzstelle
27	San Marino	Law n. 71 of 1995 Law n. 70 of 1995 reforming Law n. 27 of 1 March 1983	TBD
28	Slovenia	Draft Slovenian Data Protection Act (ZVOP-2)	Information Commissioner of the Republic of Slovenia
29	Switzerland	Swiss Federal Data Protection Act (DPA)	Federal Data Protection and Information Commissioner (FDPIC)
30	Kenya	Data Protection Act 2019	Office of the Data Protection Commissioner
31	United States of America	Swiss-US Privacy Shield Frameworks State laws such as California Consumer Privacy Act	International Trade Administration (ITA) within the U.S. Department of Commerce
32	Guernsey	The Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance) regulates the collection and handling of personal data. The Ordinance has been in force since 1996, but, in 2012/2013 was significantly amended (notably with regard to direct marketing).	
33	Japan	"The Act on the Protection of Personal Information (""APPI"") regulates privacy protection issues in Japan and the Personal Information Protection Commission (the ""PPC""), a central agency acts as a supervisory governmental organization on issues of privacy protection. The APPI was originally enacted approximately 10 years ago but was with recently amendments coming into force on 30 May 2017."	
34	Hong Kong	The Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance) regulates the collection and	

		handling of personal data. The Ordinance has been in force since 1996, but, in 2012/2013 was significantly amended (notably with regard to direct marketing).	
35	Malaysia	The Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.	
36	Mauritius	Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017 or Act), proclaimed through Proclamation No. 3 of 2018, effective January 15, 2018. The Act repeals and replaces the Data Protection Act 2004, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).	
37	Qatar	The Qatar Financial Centre (QFC) implemented QFC Regulation No. 6 of 2005 on QFC Data Protection Regulations (DPL).	
38	Singapore	Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) (the Act) on October 15, 2012. The Act took effect in three phases:	
39	South Korea	Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011	
40	Taiwan	The former Computer Processed Personal Data Protection Law (CPPL) was renamed as the Personal Data Protection Law (PDPL) and amended on May 26, 2010. The PDPL became effective on October 1, 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remained ineffective. The government later proposed further amendment to these and other provisions, which passed legislative procedure and became effective on March 15, 2016.	
41	Turkey	The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD). The LPPD is primarily based on EU Directive 95/46/EC.	
42	United Arab Emirates	The Dubai International Financial Centre (DIFC) implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007 which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law (DPL).	
43	India	On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in Justice K.S.Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in	

		Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2018.[1] However, presently the Information Technology Act, 2000 (the Act) contains specific provisions intended to protect electronic data(including non-electronic records or information that have been, are currently or are intended to be processed electronically).	
44	Uruguay	Data Protection Act Law No. 18.331 (August 11, 2008); Decree No. 414/009 (August 31, 2009) (the Act).	Unidad Reguladora y de Control de DatosPersonales (URCDP)

NB: NITDA may by public notice signed by the Director General/CEO update this list of countries as the need arises