[DRAFT]

NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK

November, 2019

(Version 2)

NIGERIA DATA PROTECTION REGULATION 2019:

IMPLEMENTATION FRAMEWORK

NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK

1. Background:

It has been identified that the personally Identifiable information of Nigerian citizens is being processed by unauthorized individuals without their consent. This not only exposes Nigerian citizens data being processed unlawfully, it could also result in processing which could lead to the loss of rights and freedoms of such citizens, leading to harm and distress. To curtail such activity, NITDA has developed the Nigerian Data Protection Regulation (the 'Regulation', 'NDPR'). The NDPR is at present, the most robust data protection framework in Nigeria. In response to stakeholders encouraging NITDA to ensure the effective implementation and enforcement of the Regulation, we have also developed the NDPR Implementation Framework as a guide to assist Data Controllers and Data Administrators understand the controls and measures they need to introduce into their environments to comply with the NDPR.

2. SUMMARY OF THE NDPR

The NDPR was issued on 25th January 2019 pursuant to Section 6 (a) and (c) of the NITDA Act, 2007. The NDPR 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 atrocious breaches. The government further takes cognizance of emerging data protection regulations within the international community geared towards security of lives and property and fostering the integrity of commerce and industry in the data economy.

The principles of the NDPR are enumerated as follows:

a) **Lawfulness and Legitimacy**: Article 2.1(1a) provides that Personal Data shall be collected and processed in accordance with specific, legitimate and lawful purposes consented to by the Data Subject.

b) **Specific Purpose**: Article 3.1(7c) mandates the Data Controller to expressly inform the Data Subject of the purpose(s) of the processing for which the Personal Data are intended as well as the legal basis for the processing. The Data Controller is now required to inform the data subject of breach of his or her personal data within seven working days after discovering the breach.

c) **Data Minimization:** Data Controllers are required to collect the minimum required data and avoid collecting data that is not required for the purpose of processing. Data that is not directly related to the business purpose of collection consented to by the Data Subject should not be collected. No data shall be obtained except the specific purpose of collection is made known to the Data Subject. This principle relates also to the principle on purpose of collection.

d) **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 (Art. 2.1(b)). The NDPR prohibits the abuse or inaccurate representation of personally identifiable data, even if such data was obtained with lawful basis. Data Controllers and processors are required to simplify the process of personal data by the Data Subject in order to achieve the objectives of this principle.

e) **Storage and Security:** Data Controllers are required to store data only for the period they are reasonably required to so do. Every data controller must state and implement data retention schedules and communicate such to the data subjects or its potential clients. The Regulation does not explicitly provide for a time period because that detail in certain scenarios may be subject to existing laws or contractual agreements. However, where the time frame for storage of the personal data is not specified, the following shall be adopted:

i. *3 years after the last active use of a digital platform*
ii. *6 years after the last transaction in a contractual agreement*
iii. *Upon presentation of evidence of death by a deceased's relative*
iv. *Immediately upon request by the Data Subject or his/her legal guardian where no statutory provision provides otherwise*

The Regulation also places the onus of security on the Data Controller and Processor. Art. 2.1(d) provides- ***personal data shall be 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.***

f) **Confidentiality, Integrity and Availability:** Article 3 of the Regulation enumerates the rights of the data subject. The right to confidentiality, integrity and availability of own data is sacrosanct with few exceptions or limitations. One of the underpinning principles of the NDPR is that data control must comply with basic minimum standards of information security management. The Regulation specifies the role of the Controller and the Data subjects.

g) **Compliance and Enforcement**: One of the novelties of the NDPR is its compliance framework. The Regulation creates a nouveau class of professionals- Data Protection Compliance Organisations (DPCOs). A DPCO is any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection Law or Regulation having effect in Nigeria (See Article 1.3 (xiii) of the NDPR).

This Framework is therefore aimed at amplifying the NDPR in order to ensure that enforcement of the Regulation is fair and just to all parties.

2.2 Objectives of the NDPR

The objectives of the NDPR are-

a) to safeguard the rights of natural persons to data privacy;

b) to foster safe conduct for transactions involving the exchange of Personal Data;

c) to prevent unauthorized and criminal use of Personal Data; and

d) to ensure that Nigerian businesses remain competitive in international trade through the safe guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

The NDPR applies to every Data Controller and Data Administrator. A Data Controller is defined by the Regulation as 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 is a person or an organization that processes data on behalf of the Data Controller. Data Administrator is used interchangeably with Data Processor.

2.3 Exceptions to NDPR

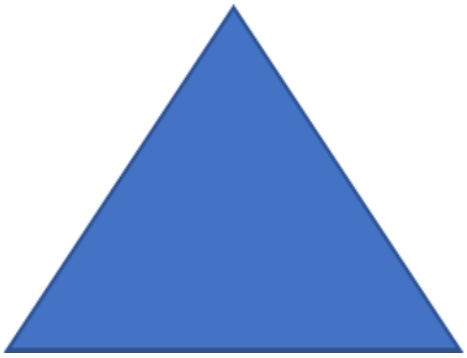
The NDPR shall not apply in the following circumstances-

i. Use of personal data in furtherance of national security, public safety and order by Agencies of government or those they expressly appoint to carry out such duties on their behalf.
ii. Criminal and Tax Offence Investigation- The NDPR shall not act in anyway to limit the powers of criminal investigators and prosecutors.
iii. The NDPR does not apply to the use of personal data in domestic affairs. However, where family members, friends or relatives use personal data to commit a crime against the Data Subject, such shall be subject of police investigation and criminal prosecution.

3. COMPLIANCE APPROACH

The approach adopted by the Nigeria Data Protection Regulation (NDPR) considers the Nigerian context and seeks to be implemented in an non-obstructive, compliance promoting approach. The NDPR uses a triangular compliance model.

NITDA (as National DPO)



Data Controller **DPCO**

In this model, NITDA would register Data Protection Compliance Organisations (DPCOs) which will provide auditing and compliance services for Data Controllers. The criteria for licensing DPCOs would be publicly accessible and such licensed DPCOs will be listed on NITDA website. Data Controllers who process personally identifiable information of more than 2000 Data Subjects are expected to submit a summary of their data protection audit to the Agency on an annual basis.

3.1 Criteria for Licensing as DPCO

A DPCO may be one or more of the following;

- Professional Service Consultancy firm
- IT Service Provider
- Audit firm
- Law firm

Which has Data Protection certification or experience in addition to any one of the following-

a) Data Science
b) Data Protection and privacy
c) Information Privacy
d) Information Audit
e) Data Management
f) Information security
g) Data protection legal services
h) Information Technology Due Diligence
i) EU GDPR implementation and compliance
j) Cyber Security/Cyber Security law
k) Data Analytics
l) Data Governance

DPCOs are licensed to provide one or more of these services;

a) Data protection regulations compliance and breach services for Data Controllers and Data Administrators
b) Data protection and privacy advisory services
c) Data protection training and awareness services
d) Data Regulations Contracts drafting and advisory
e) Data protection and privacy breach remediation planning and support services
f) Information privacy audit
g) Data privacy breach impact assessment
h) Data Protection and Privacy Due Diligence Investigation
i) Outsourced Data Protection Officer etc.

3.2 When Appointment of a Data Protection Officer is Required

A Data Controller is required to appoint a dedicated data protection officer 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 organization relate to usual processing of over ten thousand personal data sets per annum;
c) The organization processes sensitive personal data in the regular course of its business; and
d) The organization processes critical national databases consisting of personal data.

3.3 Data Protection Officer in Multinational Company

A DPO appointed for the purpose of compliance with the NDPR must be based in Nigeria and be given full access to the management in Nigeria. such Nigerian DPO may give reports to a global DPO where such exists.

4. COMPLIANCE FRAMEWORK

4.1 Forms of Compliance

i. **Cooperation**: NITDA will, to the extent 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:** NITDA may provide technical assistance to stakeholders to help them comply voluntarily with the applicable provisions. This will be through the DPCOs

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

iv. **Monitoring and Analytics:** The compliance framework will ensure the proactive monitoring and evaluation of data provided by concerned

entities by utilizing analytic tools to identify patterns that reflect non-compliance.

4.2 Compliance Checklist for Data Controllers

The Data Controller is the focal point in the data protection value chain. Most responsibilities for compliance lie with the Data Controller. The following checklist would guide Controllers to reduce liabilities and fines.

i. Conduct of Information audit: Article 3.1(7) of the NDPR provides what the audit report should contain.

ii. Legally justifiable basis for processing: Article 2.2 specifies five legal bases for processing of personal data they are- Consent of Data Subject; performance of contract; legal obligation; protection of vital interest or public interest. In addition to the explicitly mentioned bases, Legitimate Interest is another basis for processing personal data. A controller must identify upon which basis he is processing the personal data.

iii. Clear information on data processing: Article 2.5 provides for Publicity and Clarity of Privacy Policy. It states- *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.

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 privacy policy may be fulfilled through any one or combination of the following:

- Website
- Digital media
- Posted at conspicuous parts of business premises
- By reading to the affected data subjects
- Publication in any public media

Whichever mode or medium adopted shall provide a means of exercising verifiable consent of the data subject.

iv. Design System to be data protection compliant: Data Controllers must show that their systems are built with data protection in mind. Article 2.6 provides- *Anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling Personal Data…* Breach of data privacy is a strict liability offence. Data Controllers are therefore expected to ensure continuous improvement of their information security architecture to prevent possible data breaches.

v. Awareness creation on data protection: continuous capacity building for staff, contractors, processors and relevant third parties is a core duty of the Data Controller.

vi. Develop and Circulate an internal Data Privacy Strategy or Policy to help staff and vendors to understand the Controller's direction in respect of managing personal data.

vii. Conduct Data Protection Impact Assessment (DPIA): Where the organization intends on embarking 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 device means of addressing such risks. Organisations are also required to conduct DPIA on their processes, services and technology periodically to ensure continuous compliance.

viii. Process of notification of appropriate authority in the event of data breach: Every controller must stipulate a process for notifying NITDA on identified data breaches within seventy-two hours of the breach.

ix. Appoint a Data Protection Officer or assign an appropriate person who has responsibility to the top-most hierarchy of the Organisation in respect of data protection.

x. Update agreement with third party processors to ensure compliance with the NDPR.

xi. Design system to make data request and access easy for Data Subjects

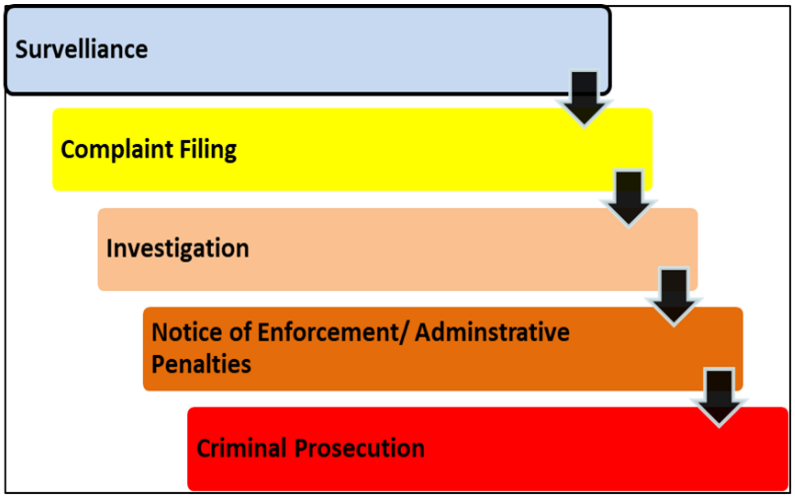
xii. Design system to enable Data Subjects easily correct or update information about themselves.

xiii. Design system to enable Data Subjects easily transfer (port) data to another platform at minimal costs.

xiv. Process for objection to processing of personal data is clearly communicated to Data Subjects

xv. Procedure for informing and protecting rights of Data Subject where automated decision is being made on personal data

5. ENFORCEMENT FRAMEWORK



5.1 Forms of Enforcement

5.1.1 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 NITDA to identify breaches of regulatory instruments or co-opt other stakeholders to identify and report breaches to the Agency**.**

5.1.2 Complaint Filings

A Compliance Officer or any person who believes a party is not complying with any of the provisions of this Regulation may file a complaint with 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. NITDA may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing.

5.1.3 Investigations

NITDA will investigate any complaint filed against a concerned entity when a preliminary review of the facts indicates a possible violation of the provision(s) of any regulatory instrument. 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, NITDA will indicate the basis of the audit.

5.1.4 Administrative Sanctions

Where 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 of the NDPR, NITDA may issue an order for compliance with relevant provisions to curtail further breach. 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. NITDA may also issue other administrative orders to include:

    i. Suspension of service pending further investigations;

    ii. Order for parties in breach to appear before a panel to determine liability of officers in line with Article 4.2;

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

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

5.1.5 Criminal Prosecution

Where NITDA has determined that a party is in grave 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(1,3) NITDA Act 2007. NITDA shall seek a fiat of the Honorable Attorney General of the Federation (HAGF) or may file a petition with any prosecuting authority in Nigeria, this may include; the Economic and Financial Crimes Commission (EFCC), the Department of State Security (DSS), the Nigerian Police Force (NPF), the Independent Corrupt Practices Commission (ICPC) or the Office of National Security Adviser (ONSA).

6. 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 NITDA through the office of the Director General of NITDA. 2. The Document must be duly signed by an Officer of 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).
Request for Additional Information and Investigation	If it appears 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 NITDA is satisfied that there is a *prima facie* evidence on a breach, NITDA may: 1. Request for a response from the violator stating the allegations against them; 2. In the event that NITDA finds the explanations of the alleged violator coherent and sufficient NITDA will respond to the allegation and enforcement will be terminated
Notice of Enforcement	Where NITDA is satisfied that a breach of NDPR has occurred; 1. 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. NITDA may issue an administrative fine or penalty in line with extant regulation
Issuance of Public Notice (OPTIONAL)	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 NITDA as to what steps to be taken to remedy breach after the period stated in the **"Notice for Enforcement"**; or B. 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 NITDA; and III. Implication of the action of the violator to the development of ICT in Nigeria. IV. A copy of the notice would be copied to the Presidency and any other relevant organ of government.

7. HOW PERSONAL DATA IS TO BE HANDLED

According to Article 2.1.1(a)(i) Data Controllers are to ensure data collected is specific; legitimate; adequate; accurate; stored for the period reasonably needed; purpose of collection stated; secured and explicit, unambiguous consent granted by the Data Subject.

7.1 Further Processing

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 data initially collected for a defined, 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) Possible impact of the new processing on the data subject; and
d) Existence of requisite safeguards for the data subject

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

gives consent based on the new information or the processing is required in compliance with a legal obligation.

7.2 Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is an assessment done to ascertain the possible implication of certain business decisions in relation to the provisions of the NDPR. DPIA is not compulsory for all processing operations, however, it may be required for the following types of data processing.

a. Evaluation or scoring (Profiling);

b. Automated decision-making with legal or similar significant effect;

c. Systematic monitoring;

d. Sensitive data or data of a highly personal nature;

e. When 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.

8. DIGITAL CONSENT

'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 (Article 1.3iii). Consent may be made through a statement- written, sign or an affirmative action signifying agreement to the processing of personal data.

8.1 Types of Consent

a) Implied Consent: participating and volunteering of data in certain conditions can be an implied consent.
b) Explicit Consent: Subject gives clear, documentable consent eg. Tick a box, sign a form, send an email or sign a paper

c) Opt-out Consent: you are in, except you choose to opt-out.

e.g *I don't want to receive XXX newsletter* ☐

If the box is left unticked, you will receive the XXX newsletter

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

8.2 Consent Requirement under NDPR

a) ***Transparency***: There must be an explicit privacy policy stating type of data collected, how processed, who processes, security standard etc;

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

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

d) ***Access to data***: Subject can request and receive data he gave, how such is being used, who has access to it. Data Controllers must keep consent records; and

e) ***Special category / higher standard consent***: Sensitive personal data such as ethnic, political affiliation, religious beliefs, trade union membership, biometric, sexual orientation, health and such like requires specific, higher consent method. A tick of a box would not suffice.

8.3 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 organization 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 contract- 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 them if anything changes; and
h) Build regular reviews into your business processes

(Source: *UK Information Commissioner's Office*)

8.4 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 do not necessarily need the ticking of a box or similar methods, the continued use of a website which has met the following requirements would suffice as consent:

- The information must be clear and easy to understand;
- the purpose of the use of the cookies must be provided;
- the identity of the person or entity which is responsible for the use of the cookies must appear;
- the possibility of withdrawal of consent must be easily accessible and be described in the information; and
- this information must always be accessible for the user.

9. DATA PROTECTION AUDIT

Data Protection Audit is a systemic investigation or examination of records, process and procedure of Data Controllers and Processors to ensure they are in compliance with the requirements of the NDPR and in accordance with the

organisation's data protection policies, processes and procedures. The NDPR requires data Controllers and Administrators to keep and produce a peculiar class of records, logs or databases in accordance with stipulated rules. Failure to maintain these records in the manner provided may lead to harm to others, violation or the commission of a crime.

NITDA may, on its own, carry out scheduled Audits, or may require report of Audits as carried out by DPCOs and may schedule "spot check" or "Special Audits" to ascertain compliance or to identify breaches. Usually these audits or investigations are unscheduled and maybe at a "tipoff "or may be random to ensure compliance with the NDPR and related laws.

The NDPR provides two types of Audits- Initial Data Audit and Annual Data Audit. The Initial Data Audit is provided in Article 4.1(5) while the Annual Data Audit is an audit showing the continuing state of data processing in the organization.

The reasons for conducting data protection audit include:

- ✓ assess the level of compliance with the NDPR
- ✓ evaluate compliance with the organisation's own data protection policy
- ✓ identify potential gaps and weaknesses organisations processes
- ✓ Give requisite advise and/or remedial actions for identified gaps

9.1 Audit Periods

Article 4.1(7) addresses the period when audit report is to be filed by Data Controllers. The Article provides as follows:

> ***(7) On annual basis, a Data Controller who processed the Personal Data of more than 2000 Data Subjects in a period of 12 months shall, not later than the 15th of March of the following year, submit a summary of its data protection audit to the Agency. The data protection audit shall contain information as specified in 4.1(5).***

Non-filing of Annual Audit report by a Data Controller is a *prima facie* case of breach. 15th of March is the Latest date for filing of Annual Data Audit Report.

9.2 Audit Filing Fees

Each Controller is expected to file the audit report and pay the following amount as applicable:

Filing Fees for Annual Audit Reports

1.	Filing of Report of less than 5,000 Data Subjects	N10,000
2	Filing of Report of 5,000 Data Subjects and above	N20,000

9.3 Content of Audit Report

The data protection audit shall contain information as specified in Article 3.1(7) of the Regulation. for clarity, the report shall contain the following:

a) the identity and the contact details of the Controller;

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 Controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by 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 Data Portability;

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 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) 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; and

n) Where applicable, that the Controller intends to transfer Personal Data to a recipient in a foreign country or international organization and the existence or absence of an adequacy decision by The Agency.

A draft standard template for the audit report is attached as Annexure A in this Framework, the final, Stakeholders agreed version would be adopted by Data Protection Compliance Organisations (DPCO) in the course of Audit implementation.

9.4 ROLES OF DPCOs IN DATA AUDITS

The DPCO as an agent of NITDA in the implementation of the NDPR has critical roles to play to ensure the objectives of the Regulation are met. In the performance of data audits, DPCOs are responsible for:

a) Evaluating status of compliance by the organization. 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) Assess level of awareness by top management, staff, contractors and customers on the NDPR.
d) Identify current or potential non-compliances
e) Draw out a remedial plan to remediate identified non-compliances

9.5 AUDITING UNFAMILIAR SYSTEMS OR OPERATIONS

When a DPCO is contracted to audit a system, it is not conversant with in order to practically ascertain the veracity of the claims of the auditee, such scenario is referred to as *Black Box Auditing.* The Auditor's role in such organization is to ensure that the roles in Paragraph 9.4 is properly carried out and further verify that data breach or incident management process is properly documented and relevant staff are trained and aware of their responsibilities.

9.6 AUDIT VERIFICATION STATEMENT BY DPCO

A DPCO shall make the following Audit Verification Statement as a pre-condition to the filing of an Annual Audit Report or any other report demanded by 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 (DAR) 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***

9.7 AUDITOR'S CODE OF CONDUCT

Every DPCO shall ensure all its staff are well aware of the ethical considerations in the performance of Audit under the NDPR. NITDA shall ensure DPCOs become registered with professional associations that regulate ethical conducts of their members and to ensure standardized delivery of services. The following are basic ethical expectations required of DPCOs in the conduct of their business.

a) Confidentiality:

   DPCOs shall handle the information and data of their client in the most confidential manner. A binding non-disclosure agreement shall be signed before embarking on the audit and implementation process.

b) Conflict of Interest:

   DPCOs shall not audit a client where the doing of such would lead to manifest conflict of interest. For example, a DPCO that designed and implemented the data protection system should not conduct the data audit

   A DPCO that is engaged to provide financial or systems audit may also perform data audit, however, such must not have been retained as the outsourced Data Protection Officer or be responsible for the implementation of the data protection compliance.

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 have an idea of where the country's cyber and information management practices can be improved.

   Any established falsehood found in a report or communication to NITDA by the DPCO is a ground for immediate withdrawal of license

d) Professionalism

Auditors must perform the service with the highest level of professionalism. Continuous capacity building of staff is a prerequisite for relicensing by NITDA. DPCOs must not undertake any work for which they lack the requisite skills, manpower and capacity.

10. TRANSFER OF DATA ABROAD

Where data is being transferred abroad as stipulated in Article 2.11, the following information is required-

i. The List of Countries where Nigerian citizens personally identifiable information are transferred in the regular course of business.

ii. The Data Protection laws and contact of National Data Protection Office/Administration of such countries listed in i) above.

iii. The privacy policy of the Data Controller, compliant with the provisions of the NDPR.

iv. Overview of encryption method and data security standard

v. Any other detail that assures the privacy of personal data is adequately protected in the target country.

NITDA shall coordinate transfer requests with the office of the Attorney-General of the Federation. A 'white-list' of jurisdictions shall be compiled and published on official media of communication. 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.

10.2 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 NITDA. The Binding Corporate Rule may be stated in the Company's Data Privacy Policy.

11. RETENTION OF RECORDS

The length of storage of data shall be determined by:

a) The contract term agreed by parties;
b) Whether the transaction type has statutory implication;
c) Whether there is an express request for deletion by the Data Subject, where such Subject is not under an investigation which may require the data; and
d) The cost implication of storage of such data by the Data Controller.

Every data Controller shall specify the duration of storage clearly in its Terms of Service or other binding document. NITDA would consider the above and other circumstances to determine if the data was stored appropriately and for a reasonable length of time.

Personal Data that is no longer in use and after 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 defense against future allegation of breach by a Data Subject.

12. REPORT OF DATA PRIVACY BREACH

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

- Contact the Organisation for enquiry;
- Review of earlier filed annual report (if any);
- Data Protection Regulation Compliance Query;
- Administrative Action; and
- Prosecution

Data Controllers and Administrators also have a duty of Self-Reporting Data Breaches. The NDPR requires Data Controllers and Administrators to have policies and procedures for monitoring and reporting violations of privacy and data protection policies (See Article 4.1(5)j). Data Controllers and Administrators have a duty to report to NITDA within 72 hours of their knowledge of the breach.

Notification of Data Breach to NITDA must include the following information:

i. A description of the circumstances of the loss or unauthorized access or disclosure
ii. The date or time period during which the loss or unauthorized access or disclosure occurred
iii. A description of the personal information involved in the loss or unauthorized access or disclosure
iv. An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure
v. 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
vi. A description of any steps the organization has taken to reduce the risk of harm to individuals
vii. A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure, and
viii. 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

13. ESTABLISHMENT OF ADMINISTRATIVE REDRESS PANEL

In line with Article 4.2 of the Regulation, NITDA shall establish Administrative Redress Panels (ARP). The ARP shall be composed of accomplished IT professionals, Public administrators and lawyers who shall work with the Agency for the purpose of resolving issues related to the Regulation.

The ARP procedure shall give preference to online dispute resolution mechanism. Where it is impracticable to adopt such mechanism, the ARP panel shall be constituted and shall give its opinion within a stipulated period of time.

The rules of procedure of the ARP shall be drawn up by a Panel of experts. The ARP Procedure shall however be designed 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.
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 its establishment; the impact of the fine on its overall contribution to the economy. Nothing in this provision shall however limit the powers of the ARP to discharge its duties as expected of a typical quasi-judicial panel

14. THIRD PARTY PROCESSING

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

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

a) Categories of Third-party data recipients e.g. Credit Reference Agencies; Payment Processors; Insurance Brokers; Anti-Corruption Agencies etc.

b) Third Party Name
c) Third Party Jurisdiction
d) Purpose of disclosure e.g. Fraud Checking; Payment Processing; Dispute Management; Risk Management; Statutory Requirement etc.
e) Type of Data Disclosed e.g. Name, phone number, address, payment details; salary details etc.

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-

i. Process data only based on authorization expressly granted by the Data Controller through a written agreement that specifies roles and obligations of each party in respect to data protection.
ii. Ensure there is adequate information security and process measures to protect personal data being processed in respect of the Controller.
iii. Where requested by the Data Subject, the third party processor shall delete such data on the instruction of the Data Controller.

15. DATA PROTECTION IN MDAs

NITDA shall deploy strategies and programmes to improve electronic governance in public institutions. Federal Public Institutions (FPIs) shall be given more time to comply with the Regulation. NITDA shall coordinate the process of improving Data Protection in FPIs through training and process change management.

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 organization including assigning responsibilities, awareness raising and training staff

- facilitating the cooperation with relevant stakeholders and acting as point of contact with NITDA.

Every FPI shall incorporate a Privacy Policy with its website and digital media platform to assure the privacy of the Data Subjects interacting with the FPI. A sample Privacy Policy for government Agencies and institutions is available in Annexure A for guidance.

16. RELATIONSHIP WITH ATTORNEY-GENERAL OF THE FEDERATION

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

Generally, Adequacy Decision shall be issued by NITDA in respect of transfer to foreign countries if the information specified in paragraph 6 above are satisfactorily provided by the Data Controller. The Office of the Attorney General may in its supervisory role prohibit the transfer of Nigerian private data to certain countries where it is of the opinion that the country's data protection regime is inadequate or incompatible with the Nigerian law.

NITDA shall generate a list of countries with acceptable data protection laws, this list shall be validated by the Attorney-General. Where a Data Controller seeks to transfer to any country other than the ones listed, then such shall be subject to further processes to ascertain the protection of Nigerian citizens' data

17. CONTINUOUS PUBLIC AWARENESS AND CAPACITY BUILDING

NITDA shall engage in continuous organization of seminars, workshops, conferences and other information dissemination programmes to socialize the NDPR and improve its public acceptance and compliance.

18. APPLICATION OF INTERNATIONAL LAWS

Where the NDPR and this Framework does not provide for specific details on the implementation of Data Protection, the European Union General Data Protection Regulation (EU GDPR) and its judicial interpretations shall of persuasive effect in Nigeria.

19. Definition of Terms

Data subject: Data subjects are individuals who can be identified using personal identifiable information related to them.

Data Processor: Data Processor means the Data Administrator as defined in Art. 1.3 of the NDPR. Data Processor is any person or organization that processes personal data on the instruction of the Data Controller or by virtue of relationship with the data controller.

White list of countries: These are countries that have provided a basic data protection law upon which the rights of Data Subjects can be enforced in such country or in the international courts.

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 Controller and DPCO shall be jointly liable except otherwise proven.

No	NDPR Provision	Question	Response	Comments
1		**Accountability and governance**		
1.1	Art. 1.1 and 1.2	Is your top-management aware of the Nigeria Data Protection Regulation (NDPR) and the potential implication on your organisation?		
1.2	Art. 2.6	Have you implemented any information security standard in your organisation before? If YES, specify.		
1.3	Art. 2.1(d)	Do you have a documented data breach incident management procedure?		
1.4	Art. 1.2	Do you collect and process personal information through digital mediums?		
1.5	Art. 2.6	Have you organised any NDPR awareness seminar for your staff or suppliers?		
1.6	Art. 4.1(5)	Have you conducted a detailed audit of your privacy and data protection practices?		
1.7	Art. 2.5	Have you set out the management support and direction for data protection compliance in a framework of policies and procedures?		
1.8	Art. 2.1	Do you have a Data Protection compliance and review mechanism?		
1.9	Art. 2.6	Have you developed a capacity building plan for compliance with data protection for all staff?		
1.10	Art. 3.1(1)	Do you know the types of personal data you hold?		
		Specify the number of data subjects you handle approximated to the nearest thousand.		
1.11	Art. 4.1(5)			

		Do you know the sources of the personal data you hold?		
1.12	Art. 4.1(5)	Who do you share personal data with		
1.13	Art. 4.1(2)	Who is responsible for your compliance with data protection laws and processes		
1.14	Art. 1.3	Have you assessed whether you are a Data Controller or Data Processor?		
1.15	Art 4.1(5)	Have you reviewed your Human Resources policy to ensure personal data of employees are handled in compliance with the NDPR?		
1.16	Art. 2.5(d)	Have appropriate technical and organisational measures been implemented to show you have considered and integrated data protection into your processing activities?		
1.17	Art. 4.5	Do you have a policy for conducting Data Protection Impact Assessment (DPIA) on existing or potential projects?		
1.18	Art. 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**		
	Art. 4.1(4)	Have you appointed a Data Protection Compliance Organisation (DPCO)?		
	Art. 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*.		
	Art. 4.1(2)	Does your DPCO also perform the role of your DPO?		

2.1	Art. 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?		
	Art. 4.1(4)	Do you utilise the same DPCO for Data Protection compliance implementation and audit?		
2.2	Art. 4.1(3)	Have you trained your Data Protection Officer in the last one year?		
	Art. 4.1(2)	Does the Data Protection Officer (DPO) have sufficient access, support and the budget to perform the role?		
	Art. 4.1(2)	If the DPO has other job functions, have you evaluated whether there is no conflict of interest?		
	Art. 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 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 NITDA as the Supervisory Authority f) To act as the contact point for NITDA on issues relating to data processing		
2.3	Art. 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	Art. 3.1	Have you documented your data processing activities?		
3.2	Art. 2.5	Have you included an appropriate privacy notice in each data collection process, including those done through third parties?		

	Art. 4.1(5)	Have you agreed a schedule to review current privacy notices contracts for compliance with NDPR?		
3.3	Art. 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	Art. 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?		
	Art. 3.1(7)	Does this inventory include data retention periods or do you have a separate data retention schedule?		
3.5	Art. 1.3	Do you have a register of data breaches and security incidents?		
4		**PROCESSING ACTIVITIES**		
4.1	Art. 2.2	Have you carried out a comprehensive review of the various types of processing your organisation perform?		
	Art. 2.2	Have you identified lawful basis for your processing activities and documented this?		
	Art. 2.5	Have you explained the lawful basis for processing personal data in your privacy notice(s)?		
4.2	Art. 2.5	Have you reviewed how you seek, record and manage consent?		
	Art. 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	Art. 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?		
	Art. 2.6	Do you adopt data pseudonymisation, anonymisation and encryption methods to reduce exposure of personal data?		
4.4	Art. 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	Art. 3.1 (8)	Do you have procedures for regularly reviewing the accuracy of personal data?		
	Art. 3.1(8)	Do you have a system for Data Subjects to erase or amend their personal data in your custody?		
4.6	Art. 2.5(d)	Have you identified all the ways in which personal data is stored, including backups?		
	Art. 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	Art. 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	Art. 3.1	Are your organisational procedures checked to ensure that you can preserve the rights of individuals under the NDPR?		
4.9	Art. 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	Art. 2.6	Are all staff trained to recognise and deal with subject access requests?		
4.11	Art. 3.1(5)	Do you have a procedure for dealing with subject access requests from third parties?		
4.12	Art. 4.1(5)	Has your organisation implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively?		
4.13	Art. 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	Art. 2.6	Have you trained all staff who deal with personal data about their responsibilities and data protection procedures?		
4.15	Art. 2.6	Are these responsibilities written into job descriptions?		
4.16	Art. 2.7	Have you contracted with any third-party data processors?		

4.17	Art. 2.7	If so, are such contracts compliant with the requirements of the NDPR?		
4.18	Art. 2.7	Have you agreed a schedule to review current contracts for compliance with NDPR?		
4.19	Art. 2.10	Do you transfer personal data to organisations in countries outside the Nigeria?		
4.20	Art. 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	Art. 2.12	Where the countries are not in the White List have you recorded the basis of transfer?		
4.23	Art. 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?		

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 NITDA) and you, constitutes our commitment to your privacy on our administrative records, websites, social media platforms and premises.

1.0 Your Privacy Rights

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.

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. 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 these Conditions. If you know or suspect that anyone other than you know your security details, you must promptly notify us at info@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 “NITDA services”). This Policy governs the use of NITDA services and intervention projects by our users and stakeholders unless otherwise agreed through 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

When you use NITDA Services, we collect information sent to us by your computer, mobile phone or other electronic access device. The automatically collected information includes but 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.

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

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

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:

Provide NITDA services and support;

Process applications and send notices about your transactions to requisite parties;

Verify your identity;

Resolve disputes, collect fees, and troubleshoot problems;

Manage risk, or to detect, prevent, and/or remediate fraud or other potentially prohibited or illegal activities;

Detect, prevent or remediate violation of Laws, Regulations, Standards, Guidelines and Frameworks;

Improve NITDA Services by implementing aggregate customer or user preferences;

Measure the performance of the NITDA Services and improve content, technology and layout;

Track information breach and remediate such identified breaches;

Manage and protect our information technology and physical infrastructure;

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 centers, and information access authorization controls.

7.0 How We Share your information within NITDA and other users

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.

We work with third parties, especially government agencies to perform 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.

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

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

We will always hold your information securely. To prevent unauthorized access to your information, we have implemented strong controls and security safeguards at the technical and operational levels. This site 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.

NITDA has also taken measures to comply with global Information Security Management Systems (ISMS) we 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 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

Certain transaction processing channels may require links to other websites or Organisations other than ours. Please note that 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. Opinions expressed or materials appearing on such websites are not necessarily shared or endorsed by us, and NITDA should not be regarded as the publisher of such opinions or materials. Please be aware that we are not responsible for the privacy practices, or content of these sites. 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. 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.

COUNTRIES WITH ADEQUATE DATA PROTECTION LAWS

SN	COUNTRY	SUMMARY OF LAW	REMARK
1	All EU Countries	The GDPR principles apply and are adequate	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
2	Angola	Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).	DPL establishes *Agência de Proteção de Dados* (APD) as Angola's Data Protection Authority.
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.	National Authority: ***Agency for Access to Public Information*** established pursuant

			to Decree 746 of 2017
4	Australia	Federal Privacy Act 1988 is based on 13 APPs (Australian Privacy Principles) that cover transparency and anonymity; the collection, use and disclosure of data; maintaining the quality of data; and the data subject's rights. Australia has regional and sectoral privacy laws supplementing the FPA.	
5	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
6	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

7	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').
8	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 in China
9	Ghana	Data Protection Act 2012	Data Protection Commission (Under the Ministry of Communications)
10	South Africa	Protection of Personal Information Act 4 of 2013	Information Regulator
11	Iceland	EU GDPR	
12	Norway	EU GDPR	
13	Israel	Israeli Privacy Law	Has the EU Adequacy decision
14	New Zealand	Privacy Act 1993	
15	Switzerland	Federal Act on Data Protection of 19 June 1992	
16	Uruguay	Data Protection Act Law No. 18.331	
17	Japan	Act on the Protection of Personal Information (APPI)	

18	Uruguay	Data Protection Act Law No. 18.331	
19	United States of America (companies certified under the US privacy shield)	California Consumer Privacy Act;	The USA has a potpourri of sectoral, state and international contracts to protect personal information
20	Kenya	Data Protection Act 2019	

REFERENCES

EU General Data Protection Regulation 2016

Data Protection Act 1998

https://www.cmpe.boun.edu.tr/