NIGERIA DATA PROTECTION ACT (NDP ACT) 2023

GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (GAID) 2025

NDPC/NDP ACT-GAID/01/2025

ARRANGEMENT OF ARTICLES

AUTHORITY

PREAMBLE

Article 1: The Objectives and Application

Article 2: Material Context of Data Processing and Priority of the NDP Act

Article 3: Statutory Remedy in Respect of Double or Multiple Regulatory Framework on Data Protection

Article 4: Cooperation between the Commission and a Public Authority

Article 5: Evaluation of Exemptions to the NDP Act

Article 6: Data Processing by Individuals for Household or Personal Purposes

Article 7: General NDP Act Compliance Measures by Data Controllers and Data Processors

Article 8: Designation of Data Controllers and Data Processors of Major Importance

Article 9: Registration as a Data Controller or Data Processor of Major Importance

Article 10: Filing of NDP Act Compliance Audit Returns with the Commission

Article 11: Designation of a Data Protection Officer

Article 12: Position of the Data Protection Officer

Article 13: Submission of Internal Semi-Annual Data Protection Report by a Data Protection Officer

Article 14: Credential Assessment of a Data Protection Officer
Article 15: Principles of Personal Data Protection
Article 16: Lawful Bases of Data Processing
Article 17: Reliance on Consent
Article 18: Data Processing Which Requires Consent
Article 19: Consent to Cookies and other Tracking Tools
Article 20: Lawfulness of Purpose and Reliance on Consent and Other Lawful Bases
Article 21: Reliance on Contract
Article 22: Reliance on Legal Obligation
Article 23: Evaluation of Lawful Bases of Data Processing
Article 24: Reliance on Vital Interest
Article 25: Reliance on Public Interest
Article 26: Reliance on Legitimate Interest
Article 27: Consideration Regarding Information to Data Subjects
Article 28: Data Privacy Impact Assessment
Article 29: Monitoring, Evaluation and Maintenance of Data Security System
Article 30: Schedule for Internal Sensitisation and Training on Privacy
Article 31: Deployment of a Data Processing Software by a Data Controller or Data Processor
Article 32: Measures Against Privacy Breach Abetment
Article 33: Data Breach Notification
Article 34: Data Processing Agreement
Article 35: Benchmarking with Interoperable Data Privacy Measures
Article 36: Exercise of Right to Rectification
Article 37: Exercise of Right to Data Portability
Article 38: Exercise of Right to be Forgotten
Article 39: Exercise of Right to Lodge a Complaint with the Commission
Article 40: Data Subject's Standard Notice to Address Grievance

Article 41: Data Ethics, Privacy and Dignity of the Human Person

Article 42: Application of Global Best Practice on Data Ethics

Article 43: Emerging Technologies

Article 44: Parameters for Assessing Privacy and Public Interest in Emerging Technologies

Article 45: Cross-Border Data Transfer

Article 46: Capacity Building in Data Protection and Continuous Professional Development Credits

Article 47: Jurisdiction of Court and Access to Justice

Article 48: Evidence of Compliance with the NDP Act

Article 49: Consideration of Time-Bound and Non-Time-Bound Obligations

Article 50: Supplementary Regulations, Directives and Schedules

Article 51: Review of Administrative and Financial Obligations under Special Grounds

Article 52: Definitions

SCHEDULES

Schedule 1 - Principles of Data Protection

Schedule 2 - NDP Act Compliance Audit Returns

Schedule 3 – Data Protection Officer Assessment

Schedule 4 - Data Privacy Impact Assessment

Schedule 5 - Guidance on Cross-border Data Transfer

Schedule 6 - Data Subject's Vulnerability Indexes

Schedule 7 - Guidance Notice on Registration of Data Controllers and Processors of Major Importance

Schedule 8 - Legitimate Interest Assessment Template

Schedule 9 - Data Subject's Standard Notice to Address Grievance

Schedule 10 - NDP Act Compliance Audit Returns Filing Fee

LIST OF ABBREVIATED TERMS

Alternative Dispute Resolution (ADR)

Annual Credential Assessment (ACA)

Application Hosting Platforms (AHP)

Basic Privacy Checklist (BPC)

Compliance Audit Returns (CAR)

Confidentiality Integrity and Availability (CIA)

Data Privacy Impact Assessment (DPIA)

Data Processing Agreement (DPA)

Data Processing Service Unit (DPSU)

Data Processing Software (DPS)

Data Protection Officer (DPO)

Emerging Technologies (ETs)

Nigeria Data Protection Act-General Application and Implementation Directive (NDP Act-GAID)

Interoperable Data Privacy Measures (IDPMs)

Internet of Things (IoTs)

Legitimate Interest Assessment (LIA)

Major Data Processing: -

- Ultra-High Level (UHL)
- Extra-High Level (EHL)
- Ordinary-High Level (OHL)

Monitoring Evaluation and Maintenance (MEM)

National Identification Number (NIN)

Pre-Action Conference (PAC)

Record of Processing Activities (ROPA)

Semi-Annual Data Protection Report (SADPR)

Sensitisation and Training on Privacy (SToP)

Special Rule of Law Indexes (SRLI)

Standard Contractual Clauses (SCC)

Standard Notice to Address Grievance (SNAG)

AUTHORITY: -

PURSUANT TO SECTION 37 OF THE 1999 CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA, SECTIONS 1(A), 6(C), 61 & 62 OF THE NIGERIA DATA PROTECTION ACT 2023 AND ALL OTHER POWERS ENABLING THE COMMISSION IN THAT BEHALF.

PREAMBLE: -

WHEREAS, the implementation of the Nigeria Data Protection Act, 2023 (hereafter referred to as the NDP Act) is designed to among other things, safeguard the right to privacy in accordance with Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (hereafter referred to as the 1999 Constitution), and to foster the trusted use of data in building a sustainable digital economy;

ACKNOWLEDGING the importance of a General Application and Implementation Directive (hereafter referred to as GAID) in providing guidance, particularly in the space of disruptive technologies and shifting paradigms of engagements – involving the processing of personal information – among citizens, organisations, communities, states and countries around the world;

DESIRING that in the vast pressure of changes in technological advancements, there should, nevertheless, be certainty in legal obligations particularly when the rights and freedoms of natural persons may be at risk in the absence of such certainties; and the need to contribute to the evolving jurisprudence of data protection and privacy rights in this regard – particularly the need to advance and never to abridge fundamental rights and freedoms;

MINDFUL of the compelling need to foster a coherent, national adequacy of data protection – which adequacy is a condition precedent to effective data flows for transactions including but not limited to those involving security, economy, migration, finance, international and inter-state trade;

COGNISANT of the function of the Nigeria Data Protection Commission (hereafter referred to as the Commission) under the NDP Act, particularly as Nigeria's independent regulatory authority in superintending over Data Protection and Privacy issues, and supervising data controllers and data processors;

THUS, the Commission hereby issues the Nigeria Data Protection Act General Application and Implementation Directive (GAID).

Article 1: The Objectives and Application

(1) In all processes and transactions relating to the personal data of data subjects in Nigeria, it is a constitutional obligation to carefully consider the material scope and the territorial scope of the NDP Act vis-à-vis its objectives before a decision affecting the fundamental right to privacy is taken.

(2) Section 2(c) of the NDP Act applies to a data controller or data processor not domiciled in Nigeria but processes the personal data of a data subject in Nigeria or targets the personal data of data subjects in Nigeria. A data controller or data processor shall be cognisant of how domiciliation applies in Section 2 of the NDP Act. Sub-Articles 3 and 4 of this Article shall be relied upon for guidance when the right of a data subject and question of domiciliation of the data controller or data processor arises.

(3) In line with the principle of universality of civil liberties, a natural person is entitled to the protection of his or her fundamental rights anywhere in the world. Accordingly, the categories of data subjects listed in Sub-Article 4 shall be entitled to the enjoyment of data subject rights under the NDP Act - subject only to the derogations permitted under the 1999 Constitution and any preemptory norm or international treaty applicable to Nigeria under International Law.

(4) The categories of data subjects to whom Sub-Article 3 relates are:

  (a) A data subject who is within the territory of Nigeria – regardless of nationality and migration status;

  (b) A data subject whose personal data has been transferred to Nigeria;

  (c) A data subject whose personal data is in transit through Nigeria – without more – provided that the obligation of the data controller or data processor responsible for the transmission through Nigeria to another jurisdiction shall be limited to data confidentiality, integrity and availability;

  (d) A Nigerian citizen who is not within Nigeria – taking into account the universal right to privacy under the United Nations Universal Declaration of Human Rights, 1948, as well as the International Covenant on Civil and Political Rights, 1976, provided that:

i. In this circumstance, the Commission may seek mutual legal assistance from the relevant authorities in the country where such citizen is resident in order to safeguard his or her privacy right as may be recognised under International Law; and
ii. The obligation of the data controller or data processor in this circumstance of Article 1(4)(d) shall be limited to the terms of mutual legal assistance and any applicable International Law.

Article 2: Material Context of Data Processing and Priority of the NDP Act

(a) Every person, body or authority owes a duty of care to data subjects, to carefully examine the material context of personal data processing with a view to ascertaining whether the processing required in the said context is consistent with the constitutional right to privacy and the objectives set forth in section 1 of the NDP Act.

(b) The material context referred to in Sub-Article 2(a) which are essentially under the Exclusive Legislative List, 2nd Schedule to the 1999 Constitution and mandates of Federal Executive Bodies may include any of the following items:

(1) Information and data on population for the purpose of facilitating economic and development planning,
(2) Immigration into and emigration from Nigeria,
(3) Implementation of treaties,
(4) Fingerprints identification and criminal records,
(5) Aviation, including airports, safety of aircraft and carriage of passengers and goods by air,
(6) Bankruptcy and insolvency,
(7) Banking, bills of exchange and promissory notes,
(8) Borrowing of moneys within or outside Nigeria for the purposes of the Federation or of any State,
(9) Census, including the establishment and maintenance of machinery for continuous and universal registration of births and deaths throughout Nigeria,
(10) Citizenship, naturalisation and aliens,
(11) Control of capital issues,
(12) Copyright,

(13) Creation of States,
(14) Currency, coinage and legal tender,
(15) Customs and excise duties,
(16) Defence,
(17) Deportation of persons who are not citizens of Nigeria,
(18) Designation of securities in which trust funds may be invested,
(19) Election to the offices of President and Vice-President or Governor and Deputy Governor and any other office to which a person may be elected,
(20) Education,
(21) Evidence,
(22) Exchange control,
(23) Export duties,
(24) External affairs,
(25) Extradition,
(26) Health,
(27) Incorporation, regulation and winding up of bodies corporate,
(28) Insurance,
(29) Labour, including trade unions, industrial relations, conditions,
(30) Safety and welfare of labour, industrial disputes,
(31) Legal proceedings between Governments of States or between the Government of the Federation and Government of any State or any other authority or person,
(32) Maritime,
(33) Taxation,
(34) Trade and commerce, and in particular trade and commerce between Nigeria and other countries including import of commodities into and export of commodities from Nigeria, trade and commerce between the States,
(35) Weights and measures,
(36) Wireless, broadcasting and television other than broadcasting and television provided by the Government of a State, allocation of wave-lengths for wireless, broadcasting and television transmission, and
(37) The establishment and regulation of authorities for the Federation or any part thereof to promote and enforce the observance of the Fundamental Objectives

and Directive Principles of State Policy under the 1999 Constitution of the Federal Republic of Nigeria.

(c) The implication of the itemisation in Sub-Article 2(b) above is that personal data is fundamental to the performance of transnational and inherent functions of the Federal Government of Nigeria as well as to trade and commerce – by persons or entities – which transcend subnational levels; the Act, therefore, applies as a common statutory authority for the protection of privacy of data subjects in the Federal Republic of Nigeria; and

(d) Data controllers and data processors shall take into consideration the material character of data – particularly its value, volume, variety, velocity and veracity – as it flows within and beyond the Nigerian territory and put in place appropriate technical and organisational measures to mitigate associated risks.

Article 3: Statutory Remedy in Respect of Double or Multiple Regulatory Framework on Data Protection

(1) In order to guarantee certainty, harmony and efficacy on the regulation of:

a) Informational self-determination (fundamental right to privacy);
b) Data sovereignty (the inherent right of an independent country to govern data processing pertaining to persons in her territory);
c) National and cross-border data flows; and
d) Treaty obligations (particularly in the material context highlighted in Article 2(b) of this GAID),

it is imperative to uphold the provision of section 63 of the NDP Act in all proceedings and transactions pertaining to the processing of personal data. For ease of reference Section 63 of the NDP Act provides: "*Where the provisions of any other law or enactment, in so far as they provide or relate directly or indirectly to the processing of personal data, are inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail.*"

(2) In the event of a conflict between the NDP Act and this GAID, the NDP Act shall prevail.

(3) Upon the issuance of the GAID, the Commission shall cease to apply the Nigeria Data Protection Regulation (NDPR) 2019 as a legal instrument for regulating data privacy and protection. In line with Section 64 of the NDP Act relating to transitional

provisions, this measure shall not affect anything done under the NDPR prior to the issuance of this GAID.

Article 4: Cooperation between the Commission and a Public Authority

(1) Section 5(h) of the NDP Act mandates the Commission to collaborate with public authorities among others in order to achieve the objectives set forth in the NDP Act.
(2) Without prejudice to the provisions of Section 63 of the NDP Act, the Commission shall cooperate with relevant public authorities in the development of sub-national or sectoral guidelines on data protection.
(3) The Commission shall conduct periodic reviews of sub-national or sectoral guidelines to determine whether such guidelines or instruments comply with the NDP Act, taking into account the provisions of Articles 1 & 2, of this GAID.
(4) Where the Commission determines that a guideline by a public authority relating to the processing of personal data negates the objectives of the NDP Act, it shall communicate its decisions to the public authority and it may in addition, request joint reviews with a view to developing a harmonious sub-national or sectoral guideline.
(5) The Commission shall take proactive steps in collaborating with public authorities and relevant institutions for the purposes of setting up Data Privacy Service Units, Legal Clinics for Data Privacy, Centres of Excellence or similar forums at sub-national, sectoral and organisational levels.
(6) In line with section 33 of the NDP Act, the Commission may engage a person who may be referred to as a Fellow, Associate, Trainee, Champion or a Data Protection Compliance Organisation to participate in a Forum referred to in Sub-Article 5 of this Article.

Article 5: Evaluation of Exemptions to the NDP Act

(1) A data controller, a data processor or an individual who relies on or intends to rely on any exemption pursuant to Section 3 of the NDP Act, shall abide by other provisions which are not exempted by the NDP Act.
(2) A data processing activity which falls within the exemptions under Section 3 of the NDP Act is at the minimum, bound by the following provisions of the NDP Act:
    a) S. 24 – Principles of personal data processing
    b) S. 25 – Lawful basis of personal data processing

c) S. 32 - Designation of Data Protection Officers
d) S. 40 – Personal data breaches notification
e) Part VI - Data subjects' rights

(3) Exemptions under the NDP Act apply to the obligations under Chapter V of the NDP Act apart from the sections mentioned in Sub-Article 2 of this Article. Thus, the Commission shall hold a data controller or data processor accountable for the infraction of any other provision of the NDP Act not covered by the exemption.

(4) In exercise of its power under the NDP Act, and in carrying out an assessment of data processing activities exempted under Section 3 of the NDP Act, the Commission shall take into consideration:
a) The degree of derogation permitted under the 1999 Constitution;
b) The lawful basis relied upon by the data controllers or data processors involved;
c) The impact on data subjects;
d) The degree of compliance with the principles of data protection;
e) Proportionality and necessity of the data processing in relation to the impact on privacy of the affected data subject.
f) The opportunity given to a data subject to lodge a complaint with the Commission.

Article 6: Data Processing by Individuals for Household or Personal Purposes

(1) In line with the provision of Section 3(1) of the NDP Act, an individual who processes data solely for personal or household purposes shall respect the privacy of a data subject and shall be held accountable for the conduct which puts the privacy of a data subject at risk.

(2) The conduct referred to in Sub-Article 1 of this Article which may put another person at risk includes the following:
a) Permission granted to data controllers or data processors to access contacts on phones through the use of software or digital applications;
b) Sharing or transferring personal data to any person or platform for any reason;
c) Lack of duty of care in handling any device which stores personal data;
d) Verbal or written disclosure of personal data; and
e) Unauthorised access to personal data of any person.

Article 7: General NDP Act Compliance Measures by Data Controllers and Data Processors

In order to comply with the provisions of the NDP Act, a data controller or data processor is, among others, expected to:

a) Register with the Commission as a data controller or data processor of major importance as the Commission may determine in accordance with the NDP Act.
b) Conduct a NDP Act compliance audit within Fifteen (15) months of commencement of business and thereafter on an annual basis;
c) In the case of data controllers and data processors of major importance (Ultra High Level and Extra-High Level as defined in Article 8 of this NDP Act-GAID), file NDP Act Compliance Audit Returns (CAR) with the Commission not later than the 31st of March of each year;
d) Identify all its obligations under the NDP Act and prepare schedules of compliance;
e) Prepare and keep semi-annual data protection reports which shall be a detailed analysis of data processing within six (6) months;
f) Prepare and follow Schedules on Monitoring Evaluation and Maintenance of Data Security System in order to guarantee data confidentiality, integrity and availability;
g) Prepare and follow schedules on organisation-wide, internal sensitisation and training on data privacy and protection in order to foster a culture of compliance with the NDP Act and best practices;
h) Identify all obligations relating to data controllers or data processors under the NDP Act and prepare schedules of compliance;
i) In the case of a data controller or data processor of major importance, designate a Data Protection Officer (DPO). Associate DPOs/Privacy Champions may be designated to support the DPO where the data controller or the data processor carries out data processing or interfaces with data subjects on multiple platforms and places;
j) Develop or review its organisational privacy policies, the privacy policy shall be in compliance with the NDP Act;
k) Publish its organisational privacy policies on its platforms with a view to sensitising data subjects on data processing activities as well as rights and duties in connection therewith;

l) Provide privacy and cookie notices at the homepage of its website. The cookie notice should give a data subject the opportunity to decline or accept the notice; A cookie notice must be displayed in such a way that it significantly obstructs the middle, the left or the right side of the home page of a website. Displaying a cookie notice at the bottom of a webpage where it may be ignored or be unnoticed by a data subject is tantamount to lack of transparency in data processing.

m) Ensure that the privacy policy and notice is transparent and appropriately provided on platforms/places where data processing is taking place; and without prejudice to the NDP Act, it shall also take into account specific directions on privacy by relevant Application Hosting Platforms through which a data subject may access its services;

n) Develop and circulate an internal data protection strategy or policy and basic privacy checklist to help members of staff and other relevant persons (such as vendors, agents and contractors) understand the organisation's direction in connection with the processing of personal data and outline the steps they are to take to ensure the organisation's direction is maintained;

o) Conduct a Data Privacy Impact Assessment (DPIA) when required under the NDP Act, or when directed by the Commission;

p) Notify the Commission of personal data breaches within seventy-two (72) hours of becoming aware of the breach;

q) Notify a data subject immediately after becoming aware of a personal data breach that may pose high risk to his or her privacy;

r) Update agreements with third party processors to ensure compliance with the NDP Act;

s) Design systems and processes to make data requests and access seamless for data subjects;

t) Design systems and processes to enable data subjects to easily correct or update their personal data;

u) Design systems and processes to enable data subjects easily transfer data to another platform or person (natural or artificial);

v) At least within the six (6) months of commencement of business and then, at the minimum, on an annual basis, train its personnel on data protection law and practices; and

w) Clearly explain the complaints process to data subjects including the right to lodge a complaint with the Commission.

Article 8: Designation of Data Controllers and Data Processors of Major Importance

(1) Section 65 of the NDP Act provides, *"data controller or data processor of major importance"* means a data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate.

(2) "Operating in Nigeria" as stated in section 65 includes a data controller or a data processor who targets a data subject in Nigeria. Such data controller or processor may not be domiciled in or resident in Nigeria. This is taking into consideration the provision of section 2(2)(a) of the NDP Act on the Application of the Act as well as sections 24(3) and 44 on the need to hold accountable data controllers and processors whose processing activities significantly impact the economy, society or security of Nigeria.

(3) In carrying out an objective assessment of what is of value or significance to *the economy, society or security of Nigeria,* the Commission shall take into consideration all relevant factors – including but not limited to the following:

a) The risks that the data processing by a data controller or a data processor poses to a data subject if such data controller or data processor is not under the obligation imposed by the NDP Act on a data controller or a data processor of major importance as contemplated by section 29(1)(a) of the NDP Act;
b) The implication for data sovereignty where data controllers or data processors may advertently or inadvertently transfer data outside Nigeria's jurisdiction to the detriment of the economy, society or security of Nigeria;
c) The sensitivity of the personal data involved;
d) Data driven financial assets entrusted by data subjects in the care of the data controller or data processor;
e) Reliance on third party servers or cloud computing services for the purpose of substantial processing of personal data;

f) Substantial involvement in cross-border data flows;
g) Use of filing systems and automation of data processing;
h) Number of data subjects involved; and
i) The need for international standard certifications for people, processes and technologies involved in data confidentiality, integrity and availability.

(4) In order to ensure proportionality of obligations in relation to various levels of major data processing, the Commission classifies data controllers and data processors into 3 (three) levels or categories of major data processing, namely:
   (a) Ultra-High Level (UHL)
   (b) Extra-High Level (EHL)
   (c) Ordinary-High Level (OHL)

(5) For direction on the classes of UHL, EHL and OHL and fees payable, the Guidance Notice issued by the Commission and reproduced in this GAID as Schedule 7, shall be relied upon until such a time that the Commission amends or replaces the said Guidance Notice.

Article 9: Registration as a Data Controller or Data Processor of Major Importance

(1) A data controller or a data processor of major importance as designated by the Commission shall register with the Commission in accordance with the Guidance Notice issued by the Commission and reproduced in this GAID as Schedule 7.

(2) A data controller or a data processor in the category of UHL or EHL shall register once and shall only be required to file CAR annually.

(3) A data controller or a data processor in the category of OHL shall renew its registration with the Commission on an annual basis and it shall not be required to file annual CAR when it renews its registration annually.

(4) A data controller or data processor of major importance shall notify the Commission of any significant change to the information submitted in its most recent registration submission within sixty (60) days after such change by providing any information required by the Commission through any electronic submission system provided by the Commission, or in the absence of which by email to an address provided by the Commission for such purpose.

(5) If a data controller or data processor no longer qualifies as a data controller or data processor of major importance, they may request removal from the register by

providing the information required by the Commission through any electronic submission system provided by the Commission, or in the absence of which by email to an address that the Commission shall publish on its website.

(6) Notwithstanding its removal from the register, a former data controller or data processor of major importance shall remain responsible for payment of any outstanding fees from the then-current and any prior annual registration periods.

(7) The Commission shall publish on its website the register of data controllers and data processors of major importance that have duly registered with it and shall update the register at least once annually.

Article 10: Filing of NDP Act Compliance Audit Returns with the Commission

(1) A data controller or a data processor shall carry out periodic compliance audit of its data processing activities with a view to mitigating the risk of data breaches through appropriate technical and organisational measures.

(2) In order to carry out an audit, a data controller or a data processor shall adopt a risk-based approach as may be associated with people, processes and technologies involved in its data processing value chain.

(3) A data controller or a data processor shall develop or adopt privacy audit controls in line with global best practices. Each model of audit may comprise of a series of techniques ranging from simple to complex and technical to organisational.

(4) A data controller or data processor shall identify each point of risk and determine the techniques and frequency of audit to be carried out on each point of risk subject to any directive by the Commission.

(5) Where personal data may be accessed from an online device of a data controller or data processor, such personal data is vulnerable to data security breach by means of cyber technology. The audit of such online device shall be as frequently as possible.

(6) A data controller or data processor of major importance shall file CAR on an annual basis. The CAR shall be based on the template provided in Schedule 2 to this GAID or as may be prescribed by the Commission.,

(7) In the case of a data controller or a data processor of major importance that was established before the 12th day of June, 2023, it shall file its CAR not later than 31st of March each year.

(8) In the case of a data controller or data processor of major importance established after the 12th day of June 2023, it shall file CAR not later than fifteen (15) months after its establishment and shall subsequently file its CAR annually.

(9) Where a data controller or data processor fails to file its CAR as and when due, it shall pay, in addition to the stipulated filing fee, an administrative penalty, which shall be 50% of the stipulated CAR filing fee.

(10) Except as otherwise determined by the Commission, CAR filing fees for UHL and EHL shall be as provided for in Schedule 10 of GAID.

(11) Where a CAR has been filed, the Commission may where necessary, direct that additional information be provided by a data controller or a data processor of major importance or by any person connected to the data processing under audit.

(12) The annual filing of CAR as prescribed in Sub-Article 8 of this Article shall be carried out through an automated platform or portal provided by the Commission.

(13) The Commission may issue a Compliance Audit Returns Certificate to a data controller or a data processor upon filing CAR.

(14) Except as otherwise approved by the Commission, a data controller or a data processor within the categories of UHL and EHL shall file CAR through a Data Protection Compliance Organisation (DPCO) licensed by the Commission in line with Section 33 of the NDP Act.

Article 11: Designation of a Data Protection Officer

(1) Section 32 of the NDP Act mandates the designation of a DPO, accordingly, the DPO may be a member of staff of the data controller or data processor, or fulfil the tasks on the basis of a service contract.

(2) The data controller or the data processor shall publish the contact details of the DPO and communicate the same to the Commission in the prescribed form.

Article 12: Position of the Data Protection Officer

(1) A data controller or a data processor shall actively engage its DPO in all issues which relate to the processing of personal data**.**

(2) The data controller or data processor shall give appropriate support to the DPO in performing the data protection responsibilities as prescribed by the NDP Act or by

the Commission. Accordingly, the data controller or data processor shall put in place the necessary organisational measures, namely:

a) Provide necessary resources to the DPO to carry out data protection tasks;
b) Ensure access to personal data processing activities and processing operations; and
c) Make adequate provision for continuous training for the DPO.

(3) The data controller or data processor shall ensure that the DPO does not carry out his or her task under duress, coercion, covert or overt influence.
(4) He or she shall not be dismissed or penalised by the data controller or the data processor for performing his or her tasks.
(5) The DPO shall directly report to the management level of the controller or the processor.
(6) Data subjects may contact the DPO with regard to all issues relating to the processing of their personal data and to the exercise of their rights under the NDP Act.
(7) The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with relevant legislation.
(8) The DPO may fulfil other tasks and duties. The data controller or data processor shall ensure that any such tasks and duties do not result in a conflict of interest.

Article 13: Submission of Internal Semi-Annual Data Protection Report by a Data Protection Officer

(1) A data controller or a data processor shall ensure that a semi-annual data protection report is compiled by its DPO and submitted to its management.
(2) The report shall be submitted to an officer of the data controller or data processor who is authorised to receive a Record of Processing Activities (RoPA).
(3) The report shall be acknowledged by the receiving officer and shall form part of the ROPA by the data controller or data processor.
(4) The report shall be verified by a DPCO during the NDP Act compliance audit.
(5) The report to be submitted by the DPO shall among others, contain the compliance status of the data controller or data processor under the NDP Act – particularly taking into account:

(a) Assessment of privacy notices – taking the requirements of the NDP Act into account.
(b) Types of data being processed by the data controller or data processor.

(c) Principles of data protection as applicable to the processing activities of the data controller or data processor.
(d) Lawful bases of data processing as applicable to the processing activities of the data controller or data processor.
(e) The need for DPIA where it is applicable to the processing activities of the data controller or data processor.
(f) Legitimate Interest Assessment (LIA) as applicable to the processing activities of the data controller or data processor.
(g) Ease of data subjects in exercising their rights.
(h) Data subjects' complaints and remediation (if any).
(i) Notices issued by the Commission (if any).
(j) Guidance sought from the DPCO, if any.
(k) Assessment of data security.
(l) Legal grounds for cross-border data transfer.
(m) Breach notification to the Commission and to data subjects.

Article 14: Credential Assessment of a Data Protection Officer

(1) The Commission shall create a database of Certified DPOs who are designated by data controllers and data processors in furtherance of Section 32 of the NDP Act.
(2) The Commission shall carry out Annual Credential Assessment (ACA) of DPOs in order to ensure that each DPO maintains the level of professionalism required to carry out his or her responsibilities towards safeguarding the rights and interests of data subjects as required under the NDP Act, relevant case laws and any regulatory instrument issued by the Commission.
(3) The assessment of a DPO shall be based on the metrics provided in Schedule 3 of this GAID.
(4) A DPO shall be guided by the provisions of the NDP Act, this GAID, the Code of Conduct for Data Protection Compliance Organisations (DPCOs) and any other relevant instrument issued by the Commission. Similarly, directives, codes or guidance relating to professionalism and ethics issued by any professional body to which a DPO belongs shall also be taken into account.
(5) The certification of a DPO shall be verified by the Commission as part of the CAR or registration prescribed by the NDP Act.

(6) The Commission may award verification scores or decline verification where the evidence submitted by a DPO as proof of Continuous Professional Development is unverifiable or wholly lacks credibility.
(7) The DPO credential assessment may be verified by the Commission upon the payment of the appropriate fees.
(8) The verification of certification under Sub-Article 5 of this Article shall be a medium through which the Commission may determine if the person designated as a DPO is a fit and proper person to carry out the duties contemplated by section 32 of the NDP Act and in particular his or her proficiency in safeguarding the rights of data subjects at organisational level.

Article 15: Principles of Personal Data Protection

(1) The entire principles of data protection are obligatory in any form of data processing. The principles under section 24 of the NDP Act are:
   a) Fairness, lawfulness and transparency of data processing,
   b) Purpose limitation,
   c) Data minimisation and ethics,
   d) Storage limitation,
   e) Data accuracy,
   f) Data confidentiality, integrity and availability,
   g) Accountability, and
   h) Duty of care.
(2) The scope of the foregoing principles is more particularly described in Schedule 1 of this GAID.

Article 16: Lawful Bases of Data Processing

(1) In line with Section 25 of the NDP Act, it is important for a data controller to carefully assess the lawful bases of data processing before embarking on same.
(2) Subject to the provisions of the NDP Act and any regulatory instruments issued by the Commission, a data controller shall carefully consider and choose the appropriate lawful bases of data processing in order to process personal data. The lawful bases are:
   a) Consent

b) Contractual Obligation
c) Legal Obligation
d) Vital Interest
e) Public Interest
f) Legitimate Interest.

(3) As the party who determines the purpose of data processing, the data controller is ultimately responsible for determining the lawful bases of data processing.

Article 17: Reliance on Consent

(1) Considering that data privacy is a fundamental right to informational self-determination, it is prudent for a data controller to prioritise the interest of the data subject which may be effectively addressed through his or her informed consent.

(2) Where reliance on consent may effectively defeat the rule of law, another lawful basis may be considered.

(3) In any complaint to the Commission as to whether consent was not obtained before data processing, and the Commission is to make a determination whether reliance on consent would effectively defeat the rule of law, the Commission shall take into account:

a) The clear and present risk to fundamental rights and freedoms of the data subject and third parties;
b) The security implication;
c) Public welfare;
d) The need for efficacy in the administration of justice - taking into account the need to;
    i. Uphold equality before the law,
    ii. Submit to the neutrality and impartiality of courts of competent jurisdiction;
e) Sustainable development;
f) Prior relationship between the data controller and the data subject; and
g) Proportionality and necessity of the scope of the processing.

(4) The items listed in sub (3) above are hereafter referred to collectively as Special Rule of Law Indexes (SRLI).

(5) Reliance on any lawful bases of data processing which is not consent and not supported by any SRLI shall be strictly scrutinised during NDP Act compliance

audits and in any proceeding where the conduct of a data controller or processor is called into question.

(6) Whenever a data controller relies on consent, it shall keep a proper record that guarantees accountability in respect of the consent.

(7) In determining whether a data controller is accountable in the mode of obtaining consent, the data controller shall:

a) Provide appropriate information to the data subject such that the data subject, on the basis of the information, may make an informed decision;
b) Make the process of withdrawal of consent as easy as giving consent; and
c) Ensure that refusal of consent is not detrimental to the rights and interests of the data subject.

(8) Nothing in this GAID shall prevent a data subject from giving a constructive or an implied consent to data processing in the following circumstances:

a) A data subject's acts of participation in a public event and the images taken in that event may be used for a report of that event – provided that such images shall not be used for profit or commerce-oriented advertisement without the express consent of the data subject. A data controller in this circumstance shall ensure that images captured do not portray data subjects in a bad light. In addition to other measures of duty of care, a data controller may put participants on notice that images captured may be used for reporting, journalistic or other purposes permitted by the NDP Act.
b) Subject to the NDP Act and Article 18 of this GAID, a data subject's act of closing a privacy notice displayed on the centre of a webpage and which notice significantly obstructs the viewing of the webpage – provided that the data collected in such circumstances is limited to processing of personal data which is necessary to basic functionality of the website. Basic functionality means such functions that permit the website to respond to and analyse the interactions of the data subject with the website.

(9) At all times where consent is required, a data subject shall be provided with a clear and explicit option to accept or to decline.

Article 18: Data Processing Which Requires Consent

(1) Without prejudice to the provisions of the NDP Act and in addition to other circumstances in which consent may be required under this GAID or by operation of law, consent is required:
   a) For any direct marketing activity;
   b) For the processing of sensitive personal data;
   c) For further processing that is incompatible with the original purpose of processing;
   d) For the processing of the personal data of a child;
   e) Before personal data may be transferred to a country in respect of which the Commission has not made an adequacy decision; and
   f) Before the data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject.

(2) A CAR shall state whether or not the data controller or the data processor relies on consent to carry out data processing in any of the activities itemised in Sub-Article 1 of this Article.

Article 19: Consent to Cookies and other Tracking Tools

(1) Operation of cookies and other tracking tools shall comply with the principles of data protection under section 24 of the NDP Act.
(2) Except as otherwise provided by this GAID, the use of cookies on a website or other digital platforms requires consent.
(3) The consent shall be freely given, informed and specific.
(4) A Data Controller/Data Processor should display a cookie banner in a manner that is conspicuous and obvious to a user or site visitor.
(5) Necessary cookies which do not process sensitive data, financial data or any data stored privately by a data subject does not need the ticking of a box or similar methods;
(6) In this article "necessary cookies" means cookies that enable core functionality such as security, network stability management, and accessibility. All other forms of cookies require a specific selection of "yes or no" (alternatively: "accept" or "reject") options presented to the data subject.

(7) In deploying cookies, website owners are required to:
   a) Make cookies notice banner or display conspicuous. Accordingly, a data subject shall not be required to scroll to any part of a website before seeing the cookie banner. Similarly, every tracking tool shall be made known to the data subject at the section of the web page which appears first;
   b) Make cookie information clear and easy to understand;
   c) Notify users of the presence and purpose of the cookies;
   d) Identify the organisation responsible for the use of the cookies; and
   e) Provide information on how to withdraw consent from the use of the cookies.

(8) The Commission shall treat any personal data tracking tool which performs functions that are similar to cookies as bound by the rules that apply to the use of cookies – taking into account the legal ground that where the same facts exist the same rules shall apply.

Article 20: Lawfulness of Purpose, Reliance on Consent, and Other Lawful Bases

(1) In addition to other obligations under the NDP Act and this GAID, every data processing shall only proceed from purposes that are:
   i. Lawful under the NDP Act,
   ii. Not in violation of other legislation for the time being in force in Nigeria, and
   iii. Not in violation of preemptory norms of general International Law.

(2) No consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violations and criminal acts.

Article 21: Reliance on Contract

(1) At the preliminary stage of a contract with a data subject, a data controller or data processor may carry out data processing on the data subject for the purpose of due diligence.

(2) Where the contract did not materialise, any personal data collected relating to the data subject shall be destroyed within six (6) months unless there is a justifiable ground to archive the data for the purposes of any future legal claim.

(3) A contract with a data subject involving data processing shall make provision for termination of the contract prior to the tenure of the contract.

(4) Pursuant to Section 46 of the 1999 Constitution and Section 34(1)(a)(vi) of the NDP Act, a specific term of a contract on personal data processing that ousts or purports to oust the adjudicatory jurisdiction of Nigerian courts or the executive jurisdiction of the Commission shall be treated as void.

(5) Without prejudice to Sub-Article 4 of this Article, and the inherent powers of a court of competent jurisdiction, a contract on personal data processing between a data controller or a data processor and a data subject may make provision for Alternative Dispute Resolution (ADR) mechanisms.

Article 22: Reliance on Legal Obligation

(1) A legal obligation means any one of the following:
   a) a specific duty imposed by law;
   b) an order of a court of competent jurisdiction; or
   c) a responsibility incidental to an obligation imposed by law to carry out an act which requires the processing of personal data.

(2) Where a legal obligation derogates from the general safeguards of the NDP Act, it shall be treated as a derogation from the right to privacy as enshrined under Section 37 of the 1999 Constitution, and accordingly, Section 45 of the 1999 Constitution applies.

(3) In line with Section 45 of the 1999 Constitution, data processing shall only take place in such circumstances of derogation as stipulated in Sub-Article (2) of this Article if the enabling law for the said legal obligation is reasonably justifiable in a democratic society and:
   i. it is in the interest of defence, public safety, public order, public morality or public health; or
   ii. for the purpose of protecting the rights and freedom of other persons; accordingly, account shall be taken of practices in a democratic society where the rule of law is firmly entrenched.

(4) Data processing under legal obligation shall be strictly limited to the minimum requirement under a law in line with Sub-Article (3) above and shall not be used for a voyage of discovery into the privacy of a data subject or in circumstances of establishing a speculative claim.

(5) In any circumstance where a legal obligation for data processing is to be imposed on a data controller or data processor, account shall be taken of any less intrusive method of processing proposed by anyone of the following persons:
   a) The affected data subject;
   b) The Commission;
   c) The concerned data controller or data processor;
   d) A non-governmental organisation in the field of human rights advocacy; and
   e) The media.

(6) Without prejudice to the NDP Act, a data controller or data processor who is in possession of the personal data of a data subject may rely on the written opinion of its DPO in order to satisfy itself with:
   a) The legal competence of the authority demanding the processing of personal data under a legal obligation;
   b) The measures provided for the protection of personal data in accordance with the principles of data protection set forth in Section 24 of the NDP Act;
   c) The scope of the processing as contained in a competent order, warrant or administrative directive;
   d) Access of the data subject to applicable data subjects' rights in accordance with Part VI of the NDP Act; and
   e) The enforceability of data subjects' right against unfair data processing – taking into account the principles of necessity and proportionality.

(7) Whenever a data controller or a data processor is dissatisfied with an administrative order, warrant or directive regarding the processing of personal data, he or she may seek guidance from the Commission in line with Section 3(4) of the NDP Act and shall take the safeguards mandated under this Article into account.

(8) Whenever a data controller or a data processor or the affected data subject is dissatisfied with a judicial order regarding the processing of personal data, he or she may approach a court of competent jurisdiction to seek a variation or the setting aside of the order in accordance with binding judicial precedents.

Article 23: Evaluation of Lawful Bases of Data Processing

(1) In all adjudicatory or administrative proceedings pertaining to personal data processing, it shall be essential to the character of a democratic society to meticulously evaluate:

(a) The necessity of processing of personal data – taking into consideration the risks and the alternatives forgone;
(b) The duty of care and the standard of care employed to mitigate unnecessary, disproportionate risks of data processing;
(c) The functional opportunity of redress accessible to an aggrieved person in accordance with Part 10 of the NDP Act and the Fundamental Rights Enforcement Procedure Rules for the time being in force;
(d) The proportionality of the processing of personal data – taking into account:
    i. the scope of measures adopted or intended to be adopted for the processing of personal data in relation to the
    ii. the legitimate aim pursued. Duty of care shall be exercised in favour of the data subject and or other data subjects whose fundamental rights and freedoms that may be affected. It is obligatory to avoid the setting of precedents which are prejudicial to fundamental rights and freedoms. It is prudent and obligatory to avoid any data processing that may undermine the adequacy of data protection which exists within the Federal Republic of Nigeria.

(2) Nothing in the NDP Act, this GAID, any legislation, or any legal instrument shall be deemed as authorising any form of data processing without compliance with Sections 37 and 45 of the 1999 Constitution of the Federal Republic of Nigeria. For ease of reference, the sections provide:

> *Section 37 CFRN 1999: The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.*
>
> *Section 45(1) CFRN 1999: Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom or other persons.*

Article 24: Reliance on Vital Interest

(1) A data controller may rely on vital interest as a lawful basis for the processing of personal data, particularly when circumstances do not permit the data subject to give consent to the processing.

(2) The vital interest referred to in Sub-Article (1) of this Article may be that of the data subject or of a third party and it shall meet the conditions stipulated below:

a) The processing is necessary for the preservation or protection of life or livelihood and failure or refusal to act may be harmful to the data subject or a third party;

b) There is a legitimate expectation based on relationship or connection, operation of law, convention or prevailing norms that personal data should be processed in such circumstances of vital interest; and

c) The data controller or data processor may be called into question as being negligent, unprofessional or reckless for failing to carry out the data processing in such adverse circumstance in which a vital interest is in jeopardy.

(3) The method of processing employed for the purposes of vital interest shall be necessary and proportionate.

(4) The data controller shall give an account of its processing to the affected data subject, his or her representative in interest, or to a competent authority upon request.

Article 25: Reliance on Public Interest

(1) Public interest may be relied upon as a lawful basis of data processing in circumstances where there is:

(a) a public health or humanitarian emergency; or

(b) there is a clear and present danger to public safety; or

(c) there is a need to address dire cases of destitution or deprivation for the benefit of the data subject – in furtherance of the Fundamental Objectives and Directive Principles of State Policy or Sustainable Development Goals.

(2) In addition to other obligations that may be imposed under the NDP Act, in any regulatory instrument issued by the Commission and any other legislation, a data controller shall take into account the safeguards in the provisions of Article 23 of this GAID when carrying out data processing on the ground of public interest.

(3) The method of processing employed for the purposes of public interest shall be necessary and proportionate.
(4) Article 23 of this GAID regarding the evaluation of legal obligation shall also apply to the evaluation of public interest when it is relied upon as a lawful basis of data processing.

Article 26: Reliance on Legitimate Interest

(1) A data controller shall cautiously consider reliance on legitimate interest as a lawful basis for data processing and shall be required in a compliance audit to show the basis of its preference. A template of a Legitimate Interest Assessment is in Schedule 8.
(2) Section 25 (2) of the NDP Act makes compatibility with contract, vital interest, legal obligation or public interest, a basis for reliance on legitimate interest. Accordingly, it shall be mandatory for a data controller under the circumstances to:
    a) Carry out Legitimate Interest Assessment (as prescribed in Schedule 8) before embarking on data processing;
    b) Prioritise privacy by design and by default – taking into consideration the suitability of anonymisation or pseudonymisation;
    c) Identify and document the lawful basis of processing which is compatible with the legitimate interest pursued;
    d) Identify and eliminate data processing that may overreach the fundamental rights and freedoms of data subjects – particularly such processing that may lead to behavioural monitoring or profiling, or lead to targeted advertisement by third parties or partners;
    e) Identify and eliminate data processing that may lead to a breach of data confidentiality, integrity and availability – taking into account vulnerable data subjects;
    f) Provide transparent information to data subjects in accordance with Section 27 of the NDP Act;
    g) Provide for prompt remediation of data subjects' rights; and
    h) Prioritise data ethics and utmost duty of care.

Article 27: Consideration Regarding Information to Data Subjects

(1) Provision of information to a data subject shall be in accordance with Section 27 of the NDP Act. The information shall be clear and shall take into consideration vulnerable data subjects.

(2) In circumstances of exclusive physical events, interviews or interactions where a data controller or data processor may not be able to provide data subjects with a privacy policy or if provided, the class of data subjects may not be able to understand the privacy policy without the aid of an interpreter, the data controller or data processor shall provide the information in the form that the data subject can understand.

(3) The information to be provided by the data controller or data processor includes but is not limited to the following:

a) The name of the data controller or data processor,
b) Lawful basis of data processing,
c) Types of personal data to be collected,
d) The purpose of the processing,
e) The means of processing,
f) Access to personal data by authorised third parties,
g) Purpose of access by third parties,
h) Data subjects' rights,
i) Access to prompt internal remediation through contact to be supplied by the data controller or data processor, and
j) Right to lodge a complaint with the Nigeria Data Protection Commission.

(4) Information to data subjects does not constitute a request for consent. Consent shall be specifically requested and obtained when it is required by law and on the ground that the information which may guide the data subject in making an informed decision has been duly provided prior to the processing of personal data**.**

Article 28: Data Privacy Impact Assessment

(1) A Data Privacy Impact Assessment (DPIA) is mandated under Section 28 of the NDP Act when data processing may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes.

(2) Introduction of new technologies or new processing techniques or directives mandating processing of personal data on a large scale requires a DPIA on the following grounds:

(a) Unintended, adverse consequences to the lives and livelihoods of data subjects may result from the data processing;

(b) Such adverse consequences are threats to fundamental rights and freedoms as well as to the Fundamental Objectives and Directive Principles of State Policy – which Policy forms the basis of sustainable development, security and economic programmes of government; and

(c) In circumstances where data processing measures constitute a derogation from Section 37 of the 1999 Constitution, they shall comply with the safeguards under Section 45 of the 1999 Constitution. In this regard, the need to fulfil the conditions of necessity and proportionality and other safeguards stipulated under Article 23 of this GAID is obligatory.

(3) A DPIA is mandatory and shall be filed with the Commission in any of the following circumstances:

a. Evaluation or scoring (profiling);
b. Automated decision-making with legal or similar significant effects;
c. Systematic monitoring;
d. When sensitive or highly personal data is involved;
e. When personal data processing relates to vulnerable data subjects;
f. When considering the deployment of innovative processes or applications, of new technological or organisational solutions which may pose a significant risk to the privacy of data subjects;
g. Development of software for the purposes of enabling communication with data subjects;
h. Financial services involving the processing of personal data through digital devices;
i. Health care services;
j. E-Commerce services;
k. Deployment of surveillance cameras in places that may be accessed by members of the public;
l. Development and implementation of any legal instrument or policy which requires the processing of personal data of members of the general public;

m. Educational services involving processing of various records relating to students or pupils;
n. Hospitality services; and
o. Cross-border data transfer.

(4) A DPIA shall be vetted by a certified DPO duly accredited by the Commission.

(5) The outcome of a DPIA conducted by a data controller or a data processor shall be part of the NDP Act CAR to be filed with the Commission.

(6) Failure, refusal or negligence in the conduct of a DPIA may, among other enforcement provisions under PART X of NDP Act, result in a restriction on all platforms where data subjects may have contact with a data controller or a data processor for the purpose of carrying out any transaction in which personal data is required.

(7) In carrying out a DPIA, a data controller or a data processor shall, in addition to the NDP Act, be guided by the provisions in this GAID.

(8) In addition to the circumstances in Article 28 (3), a data controller or a data processor who deploys software for processing of sensitive personal data, among other datasets shall carry out a DPIA and submit same to the Commission within four (4) months after the issuance of this GAID.

(9) Whenever required, a DPIA shall be carried out and submitted to the Commission before the commencement of data processing.

(10) In any event, where data processing commenced before the coming into force of the NDP Act and this GAID, a DPIA shall be carried out within six (6) months of the issuance of this GAID.

(11) A DPIA which indicates that data processing may be carried out shall in addition to the contents prescribed under Section 28(4) of the NDP Act, contain measures which guarantee privacy by design and by default – and shall particularly take into account the following principles:

(a) The need to be proactive and not reactive, preventive and not remedial;
(b) Mitigation of risks through privacy as the default;
(c) Prevention of risks through privacy by design practices;
(d) Full functionality – positive-sum, not zero-sum (such that no functionality is compromised because of another functionality);
(e) End-to-end security – full lifecycle protection;
(f) Visibility and transparency; and

(g) Respect for user privacy.

(12) The DPIA submitted to the Commission shall be signed by a duly certified DPO who is accredited by the Commission.

(13) The DPIA shall be in accordance with Schedule 4 of the GAID.

Article 29: Monitoring, Evaluation and Maintenance of Data Security System

(1) A data controller or data processor shall have schedules for monitoring, evaluation and maintenance of data security systems.

(2) The schedules shall take into account people, processes and technologies involved in data security and each shall contain applicable technical and organisational measures including but not limited to:

(a) Training;
(b) Certifications;
(c) Updates of software;
(d) Vulnerability tests of databases;
(e) Assessment of hardware for repairs or replacements;
(f) Authentication checks;
(g) Encryption reviews; and
(h) Quality Assurance on products and services being used for data confidentiality, integrity and availability.

(3) A data controller or data processor shall assign relevant officers to carry out the tasks under the schedule and stipulate time to take appropriate technical and organisational measures under the schedule.

(4) The schedule shall be vetted and certified by a duly certified information security officer.

(5) Notwithstanding the schedule, a data controller or data processor shall carry out monitoring, evaluation and maintenance of data security systems as frequently as possible, taking into account the risks of data processing.

Article 30: Schedule for Internal Sensitisation and Training on Privacy

(1) A data controller or a data processor shall prepare and implement an organisational schedule for internal sensitisation and training on privacy.

(2) The schedule shall contain a mode of evaluating the level of compliance with the NDP Act, this GAID and other regulatory instruments issued by the Commission.
(3) In respect of people, a data controller or data processor may adopt the use of meetings, questionnaires and interviews.
(4) The schedule shall be used to identify:
    (a) Data processing practices to stop,
    (b) Data processing practices to start, and
    (c) Data processing practices to continue.
(5) A data controller or a data processor shall publish the schedule on appropriate communication mediums where employees and other relevant workers, agents, and contractors, who are engaged in relevant activities may see it.
(6) A data controller or data processor shall:
    (a) Review its data processing platforms,
    (b) Assign relevant officers to carry out the tasks under the schedule, and
    (c) Stipulate time to implement appropriate technical and organisational measures.
(7) In order to enable persons engaged in data processing to understand their duties and responsibilities, a data controller or data processor shall develop a basic privacy checklist as a guide.
(8) A data controller or data processor shall develop and implement a written policy for routine checks on compliance practices which may be carried out without notice to employees. This policy may be part of a larger data governance policy of the data controller or data processor.

Article 31: Deployment of a Data Processing Software by a Data Controller or Data Processor

(1) A data controller or a data processor who (whether for itself or for other persons) deploys or intends to deploy data processing software for the purposes of tracking a data subject or enabling a communication link with a data subject and processing his or her personal data, is under an obligation to abide by the provisions of the NDP Act.
(2) For the purposes of complying with this GAID and in addition to other obligations imposed on a data controller or a data processor, it is mandatory for the data controller or data processor in the circumstances referred to in Article 31 (1) to:
    a) Carry out a DPIA before the deployment of the software;

b) Ensure that the software is designed in accordance with the principles of privacy by design and by default;
c) Without prejudice to any contrary provisions of the NDP Act or regulatory instruments issued thereunder, ensure that the software follows data security guidelines or instructions provided in the stores where the software may be downloaded;
d) Provide data privacy policy within the software;
e) Provide a privacy statement to data subjects (prospective users) prior to installation – expressly indicating the following:
    i. The types of personal data to be processed (types to be supplied by the data controller or data processor);
    ii. The lawful purpose for processing the personal data (lawful purpose to be supplied by the data controller or data processor);
    iii. The personal data to be processed without prejudice to data subjects' right to privacy;
    iv. No personal data will be processed unless such personal data is crucial to the lawful purposes being pursued through the use of the software;
    v. Technical and organisational measures are implemented as part of privacy by design and by default (types of technical measures such as encryption should be specifically indicated);
    vi. A DPIA has been conducted and the result indicates that the use of the software is unlikely to compromise data privacy and protection;
    vii. Prompt technical support on data privacy and protection is accessible via the software (link shall be supplied by the data controller);
    viii. Self-service measures which may disable, uninstall or restrict the software is available (link shall be supplied by the data controller);
    ix. Redress of grievances, right to complain to a data protection authority - (link should be provided by the developer comprising a list of countries and their data protection authorities respectively).
f) The required information in the privacy statement before the installation of the software shall be provided by a data controller or a data processor (as applicable) within six (6) months of the issuance of this GAID; provided that where the software is already in use by the data subjects prior to the issuance

of this GAID, an update shall be carried out within six (6) months in order to bring the software into compliance with the NDP Act and this GAID.

(3) Examples of software referred to in this GAID are:

(a) Operating System
(b) Mobile Applications
(c) Device Driver
(d) Firmware
(e) Programming Language Translator
(f) Utilities

Article 32: Measures Against Privacy Breach Abetment

(1) A data controller or data processor shall put in place, appropriate technical and organisational measures to prevent the use of its platform, facility, network or howsoever called, from being used to breach the privacy of a data subject.

(2) When the Commission notifies a data controller or data processor that its platform, facility, network or howsoever called is being used by any person to commit an offence under the NDP Act or to carry out a breach of privacy, the data controller or data processor shall immediately restrict such person on its platform, facility or network, pending the outcome of an investigation by the Commission.

(3) In determining if a breach of privacy has occurred, the Commission shall only rely on credible documentary or electronic records.

(4) Where a data controller or data processor fails, refuses or neglects to carry out the directives of the Commission to prevent further breach of privacy, the data controller or data processor shall be deemed as abetting a breach of privacy and shall be accountable for violation of the NDP Act as if it directly committed a breach of data privacy.

Article 33: Data Breach Notification

(1) The NDP Act under Section 40(2) provides that "a data controller *shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the Commission of the breach and, where feasible, describe the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned."*

(2) A breach is likely to result in a high risk to the rights and freedoms of individuals if, considering the nature of the breach, the personal data involved as well as the probability of accessing other personal data of the data subject through the breach, the data subject may become a victim of fraud, identity theft or exposure of sensitive personal data.

(3) In line with Section 40(2) of the NDP Act, a data controller shall notify affected data subjects immediately after becoming aware of the breach in order to ensure that data subjects are not unlawfully targeted as a result of the breach. This is in furtherance of the principle of duty of care and accountability.

(4) Notwithstanding the time provided for the notification of a data breach, a data controller or data processor shall exercise a duty of care by providing immediate information on data breach to all relevant authorities including the Commission, if such immediate information may help in containing imminent data breaches on a national scale or when containment measures may be necessary at national, sectoral or at an individual level or where it may affect members of the general public.

(5) The content of a data breach notification to the Commission shall include the following among others:

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 unauthorised access or disclosure;
f) A description of steps the organisation 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 unauthorised access or disclosure; and
h) The name and contact information of a person who can answer on behalf of the organisation, the Commission's questions regarding the loss of unauthorised access or disclosure of personal data.

Article 34: Data Processing Agreement

(1) In line with Section 29(2) of the NDP Act, a data processor is expected to rely on a Data Processing Agreement (DPA) with the data controller in order to carry out data processing on behalf of the data controller.

(2) In addition to other relevant terms and conditions as may be prescribed by law, a DPA shall include the following:

a) Obligations of the data controller and data processor under Section 29 of the NDP Act;
b) Name of parties;
c) Addresses of parties;
d) Recitals containing reference to any Principal Agreement or Service Level Agreement;
e) Purpose of data processing;
f) Location of data processing (taking into account the provisions of the NDP Act on cross-border data transfer);
g) Scope of the processing;
h) Lawful bases of data processing;
i) Responsibilities of parties under the DPA;
j) Technical and Organisational Measures for data protection (if highly technical or scientific, it should be expressly outlined in a schedule to the DPA);
k) The outcome of a DPIA where relevant;
l) Potential risks;
m) NDP Act compliance (evidence of registration with the Commission should be ascertained);
n) Confidentiality;
o) Tenure;
p) Specific Restrictions;
q) Indemnity;
r) Insurance;
s) Force Majeure; and
t) Dispute Resolution.

(3) A party to any DPA other than an individual data subject, shall take reasonable measures to ensure that the other party is compliant under the NDP Act, accountable

to the Commission or, in the case of a foreign party, to a competent regulatory authority outside Nigeria; accordingly, every data controller or data processor shall be accountable for the actions or inactions of third parties it engages or permits to carry out data processing.

(4) Where a party to an agreement operates as a sole proprietorship, an individual agent or a self-employed worker, by reason of which he or she may not be organised to fulfil the obligations of corporate entities, such a person or individual shall for the purposes of his or her engagement in high-risk data processing, be required to be trained in data protection and privacy. Evidence of training and registration as a data processor of major importance shall be relied upon as a rebuttable proof of compliance with the NDP Act.

Article 35: Benchmarking with Interoperable Data Privacy Measures

(1) A data controller or data processor shall be cognisant of the need to advance data protection and privacy rights and the measures meticulously designed for this purpose in the globally interconnected and constantly evolving data protection ecosystem.

(2) In the event that a data controller or data processor is to take a decision on an applicable technical and organisational measure for safeguarding data privacy rights, it is legally imperative to take into account the provisions of the extant Fundamental Rights Enforcement Procedure Rules in Nigeria on the importance of municipal, regional and international bill of rights.

(3) In furtherance of Article 36 (1), (2), a data controller or data processor may, subject to the approval of the Commission, benchmark its data processing with Interoperable Data Privacy Measures (IDPMs) in circumstances where a specific directive is required by the Commission under the NDP Act.

(4) Where a data controller or data processor intends to benchmark with an IDPM which expressly requires directives of the Commission under the NDP Act, it shall seek the approval of the Commission through an application stating the following:

a) The name and address of the data controller or data processor,
b) The nature of business,
c) The purpose and lawful bases of data processing,
d) The nature of data processing in which an IDPM is required,
e) The author and the jurisdiction of the IDPM being proposed for approval,
f) The benefit of the IDPM in data processing value chain,

g) The benefit of the IDPM to the ecosystem,
h) Three (3) use cases of the IDPM,
i) Any disadvantage of the IDPM, and
j) The name and contact details of its certified DPO.

(5) In furtherance of Sections 5(i) and 62(a)(ii) of the NDP Act, the Commission may within thirty (30) days, issue an approval for the benchmarking of data processing with an IDPM if it is satisfied that the use of such IDPM is without prejudice to the provisions of the NDP Act.

(6) For the purposes of Article 35 (1) – (5), IDPM means best practice templates which are not limited by jurisdictional procedures and are particularly in furtherance of the globally interoperable principles of data protection as stipulated in Section 24 of the NDP Act. Accordingly, instances where IDPM may be used include but are not limited to:

a) Anonymisation,
b) Automated Decision Making,
c) Child Online Protection,
d) Data Portability,
e) Data Subjects' Access Request,
f) Data Privacy Impact Assessment,
g) Deployment of Artificial Intelligence,
h) Encryption,
i) Forensic Data Security Audit,
j) Legitimate Interest Assessment,
k) Pseudonymisation, and
l) Record of Processing Activities.

(7) Without prejudice to the provisions of the NDP Act and any regulatory instrument issued by the Commission, a DPO is required to consider suitable IDPMs which may be used by a data controller or a data processor as part of global best practices in data processing. Accordingly, it is appropriate for a DPO to proactively review IDPMs prior to when the need for them arises. The Commission shall continuously provide guidance on IDPMs.

Article 36: Exercise of Right to Rectification

(1) The right to data rectification is essential to the operation of the principle of data accuracy under the NDP Act.
(2) A data controller or processor shall ensure that the platforms through which it processes personal data also provides an effective opportunity for data rectification.
(3) Data rectification may not depend on the provision of an affidavit or a publication in a newspaper provided that the rectification is to bring the data into alignment with the personal data relating to the data subject's National Identification Number (NIN).
(4) Where data rectification is for the purpose of correcting an error made by a data controller or a data processor in inputting the personal data of a data subject, the data subject shall not be required to pay in order to correct an error which is not his or her fault. Accordingly, it is important to ensure that a data subject is provided with manifestly ample opportunity to verify his or her data before such data is submitted in a permanent format.
(5) Whenever there is a dispute as to whether a data subject was provided with manifestly ample opportunity to verify his or her personal data before being submitted in a permanent format, the data controller or data processor shall provide the evidence of the manifestly ample opportunity. Accordingly, data processing platforms together with the technical and organisational measures for their operations shall be designed in a way that may allow a data controller or data processor to audit any source of error.

Article 37: Exercise of Right to Data Portability

(1) A data subject has a right to data portability.
(2) The right to data portability shall apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It may not apply where processing is based on a legal ground other than consent or contract.
(3) The right to data portability may not apply against a data controller or data processor in the performance of its public duties; unless there is a compelling legitimate interest or right of a data subject that may be abridged by reason of denying the data subject's right of data portability.

(4) Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with the NDP Act or any regulatory instrument issued by the Commission.
(5) The right to data portability shall not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as prescribed under the NDP Act.
(6) Nothing in this Article shall imply the erasure of personal data concerning the data subject which has been provided by him or her for the performance of a contract to the extent that and for as long as are necessary for the performance of that contract.

Article 38: Exercise of Right to be Forgotten

(1) A data subject has the right to have his or her personal data erased if:
   a) The personal data is no longer necessary for the purpose a data controller or data processor originally collected or processed it.
   b) A data controller or data processor is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws his or her consent.
   c) A data controller or data processor is relying on legitimate interest as its justification for processing an individual's data, of which, the individual objects to this processing, and there is no overriding legal ground for the organisation to continue with the processing.
   d) A data controller or data processor is processing personal data for direct marketing purposes and the individual objects to this processing.
   e) A data controller or data processor processed an individual's personal data unlawfully.
   f) A data controller or data processor must erase personal data in order to comply with a legal ruling or obligation.
(2) However, an organisation's interest in processing the personal data may override a data subject's right to be forgotten if:
   a) The data is being used to exercise the right of freedom of expression and information subject to the limit of derogation permitted under Section 45 of the 1999 Constitution and other safeguards of the NDP Act.
   b) The data processing is necessary:

i. to comply with a legal ruling or obligation.
ii. to perform a task that is being carried out in the public's interest or when exercising an organisation's official authority.
iii. for public health purposes and to serve the public interest.
iv. to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.

c) The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely impair or halt progress towards achieving the goal of the processing.
d) The data is being used for the establishment of a legal defence or in the exercise of other legal claims.

(3) Without prejudice to the provisions of the NDP Act, where a data controller or data processor has made personal data public or has shared data with third parties, the data controller is under obligation to ensure the erasure of such personal data by the third parties at the request of the data subject or in compliance with the directives of the Commission in that regard.
(4) This right may not apply where there is a public interest pursued by disclosure of the data to the general public – provided that the burden of proving the existence of a public interest shall be on the data controller who intends to keep the personal data public.

Article 39: Exercise of Right to Lodge a Complaint with the Commission

(1) The right to lodge a complaint with the Commission shall be deemed as a threshold right of redress in furtherance of the right to privacy under Section 37 of the 1999 Constitution and Section 46 of the NDP Act.
(2) Every regulation, policy, framework, or legal instrument which pertains to the processing of personal data shall in addition to all applicable data subject rights and safeguards contain a clause on the right to lodge a complaint with the Nigeria Data Protection Commission.
(3) The Commission shall set up an electronic platform through which a data subject may lodge his or her complaint with the Commission and it shall acknowledge the receipt of the complaint within seven (7) days, provided that the Commission shall continue

to receive complaints by any reasonable means through which it may be contacted by a complainant (including but not limited to hard copies at its known offices and emails).

(4) Upon the receipt of a complaint in line with Section 46 of the NDP Act, the Commission shall carry out a preliminary evaluation of the complaint – taking into account:
   a) The applicability of the NDP Act to the complaint;
   b) The urgency of the complaint and any urgent relief contained therein;
   c) The impact of the allegations on the complainant or on a third party on whose behalf the complaint is being lodged with the Commission; and
   d) The temporary remedy that may be provided pending the outcome of an investigation into the complaint.

(5) Where the Commission is convinced through a preliminary evaluation that there is a violation of the NDP Act, it shall open a case file for the complaint.

(6) Upon the opening of a case file, the Commission shall immediately serve the affected data controller or data processor (hereafter referred to as the respondent) a notice of investigation.

(7) The notice of investigation may require the respondent to provide, where applicable:
   a) The information itemised under this Sub-Article.
   b) The list of third-party data processors, agents or contractors engaged by the respondents for data processing together with data processing agreements and evidence of compliance with the NDP Act;
   c) Foreign countries to which the respondent transfers personal data together with the legal basis relied upon for the transfer;
   d) DPIA for technologies and methodologies relied on for personal data processing; and
   e) Name and official contact details of the respondent's DPO.

(8) The respondent shall, except as otherwise specified by the Commission, reply the Commission within twenty-one (21) days.

(9) If the Commission deems it appropriate, it shall invite the respondent to a Pre-Action Conference (PAC) in order to examine the facts and the available evidence provided by the parties or obtained by the Commission through investigation.

(10) A PAC may take place as frequently as necessary in respect of a complaint or an investigation carried out by the Commission pursuant to Section 46(3) of the NDP Act.

(11) In line with the power vested in the Commission under Section 6(e) of the NDP Act, the Commission may direct a data controller or data processor to attend a PAC with any relevant person who is legally compellable or competent to give evidence and who may provide relevant information in determining an issue relating to violation of the NDP Act.

(12) Where the Commission has determined that a violation of the NDP Act has taken place, it shall direct appropriate remedial action to be taken by the respondent as prescribed by the NDP Act. The Commission shall communicate its decision to the complainant and to the affected parties within seven (7) days.

(13) Nothing in this GAID shall prevent the Commission from issuing a temporary order on such terms and conditions as it deems fit in the interest of protecting the privacy right of a data subject – particularly when the violation of a data privacy right may not be remedied properly through compensation**.**

Article 40: Data Subject's Standard Notice to Address Grievance

(1) In line with the power vested in the Commission to, among others, make regulations for the protection of personal data and data subjects under section 61(1)-(2)(b) of the NDP Act, the Commission may promote the use of Data Subject's Standard Notice to Address Grievance (SNAG) as provided under Schedule 9 of this GAID.

(2) An aggrieved data subject may issue a SNAG to a data controller or a data processor where the data subject reasonably believes that the data controller or data processor violated his or her right to data privacy.

(3) SNAG shall not be regarded as a condition precedent for lodging a direct complaint with the Commission or for instituting an action, rather it shall be regarded as a standardised template for demanding internal remediation in an organisation which may be acting in violation of a data subject's privacy.

(4) SNAG may be served directly by a data subject or by a person acting under his or her authority or by a civil society organisation acting in the public interest.

(5) The Commission may create an electronic platform through which it may track SNAGs.

(6) Upon receipt of a SNAG, a data controller or a data processor shall communicate its decision on the SNAG to the Commission through the designated electronic platform.

(7) The Commission may take executive notice of SNAGs and institute direct investigation into the service of a SNAG on a data controller or a data processor particularly when such SNAG appears to be unresolved.
(8) A SNAG may be served on a data controller or a data processor via its physical address, telephone messaging medium, e-mail address, courier service or other reasonable means of correspondence.

Article 41: Data Ethics, Privacy and Dignity of the Human Person

(1) A data controller or a data processor shall prioritise the principles of data ethics which offer additional safeguards to the privacy and dignity of the human person.
(2) To fortify the principles of the sanctity of personal information and the preservation of human dignity, both data controllers and data processors must steadfastly adhere to the tenets of data ethics.
(3) Data ethics, as enshrined in this Article, serves as an indispensable guide, elevating the standards of safeguarding individuals' privacy and upholding their inherent dignity. This entails a commitment to transparency, fairness, and responsible data management practices.
(4) Transparency forms the bedrock of ethical data handling. Data controllers and processors must furnish individuals with clear and comprehensible information regarding the collection, processing, and storage of their data. This ensures that individuals are well-informed, empowering them to make informed decisions about their personal information.
(5) Fairness in data processing underscores the commitment to impartiality and equity. Discrimination based on gender, ethnicity, religion, physical ability or any other characteristic is strictly prohibited. Every individual is entitled to equal protection, fostering an inclusive digital landscape.
(6) Responsible data management involves the implementation of robust security measures to protect against unauthorised access, breaches, or any form of misuse. It requires the continuous evaluation and enhancement of data protection protocols to adapt to evolving technological landscapes.
(7) Emphasising the dignity of the human person, data controllers and processors must acknowledge the intrinsic value of every individual's data. The extraction, processing, or utilisation of data must not compromise the autonomy, freedom, or integrity of any person.

(8) Any data collection or processing that may result in harm, discrimination, or violation of individual rights is strictly prohibited. Safeguards should be in place to prevent the creation of profiles or the application of algorithms that could lead to prejudiced outcomes.

(9) In cases where data is shared with third parties, explicit consent must be obtained from the data subject. The purpose, scope, and duration of such data sharing must be clearly communicated, and individuals should retain the right to revoke consent at any time.

(10) Continuous education and awareness programs should be implemented to keep individuals informed about their digital rights, empowering them to exercise control over their personal data.

(11) The principles outlined in this article reflect a commitment to building a digital ecosystem that respects the fundamental rights of individuals. By prioritising data ethics, we aim to create a responsible and trustworthy digital environment that values and protects the privacy and dignity of every human person.

Article 42: Application of Global Best Practice on Data Ethics

The global best practice on the principles of data ethics to which a data controller or a data processor may be audited are:

(1) *Organisational Policy on Ownership of Data* – taking the following into consideration:

(a) Personal data, to all intents and purposes, belong to the natural person to whom it relates. Accordingly, it shall be construed as unethical to process data in a manner that the owner may object, taking into account, law, culture and faith.

(b) Where there are ethical concerns on individual's expectations on the use of his or her data, it is appropriate to anonymise the data and to only process it within the confines of the laws to which the individual is subject.

(c) Where there are proceeds from the lawful use of other people's property – in this case, personal data - it is to be considered ethical for the user to create ample opportunity for them to benefit from the proceeds through corporate social responsibility or other similar measures.

(2) *Demonstrable Transparency and Accountability* – taking the following into consideration:

(a) Processing of data shall not only be transparent; it shall also be seen to be transparent through accountability.
(b) The ethical standard particularly where the data controller is relying on consent, contract, vital interest, or legitimate interest, is to disclose all information upon which a data subject may make an informed decision.
(c) Information that is expected to be disclosed includes, the information required by the NDP Act to be disclosed generally to the data subjects and the following:
    i. Expected outcomes of the purpose of processing for the data controller and those with whom the data may be shared;
    ii. Capabilities of the technology used for processing – particularly, the use of algorithms for profiling, the risks involved, mitigation of risks, and
    iii. Effective channel for redressing grievances.
(d) A data controller or data processor who neglects to be demonstrably transparent may be acting in violation of the principle of transparency under the NDP Act. Thus, taking into account the ownership of data, the requirement for duty of care, and the liability of the controller or processor, may include a breach of trust.
(e) Designation of a DPO (and providing him or her with full support to carry out data protection tasks) as well as filing of NDP Act CAR with the Commission are part of the ways of demonstrating transparency and accountability.

(3) *Informational Autonomy or Informational Self-Determination* – taking the following into consideration:
(a) A data controller or data processor shall respect the informational autonomy of a data subject by making sure that his or her data are not carelessly, recklessly or negligently shared, even when consent has been obtained.
(b) Where sharing of information may lead to prejudice or abuses, efforts shall be made by the data controller or data processor to mitigate these risks.
(c) Processing to portray, project or propagate indecent acts shall be regarded as a violation of the principle of fairness under the NDP Act – initial consent of the data subject notwithstanding.

(4) *Fairness of Intention* – taking the following into consideration:
(a) A data controller or data processor shall take the lawfulness of the purpose of processing into account when processing personal data. The notion that what is not prohibited is permitted does not apply in data processing ethics.

(b) A data controller or data processor shall ensure that its intention is clear and understandable to the data subject – particularly in the context of consent, contract and legitimate interest.

(5) *Assessment of Outcomes* – taking the following into consideration:

(a) A data controller or data processor shall put in place adequate technical and organisational measures for the assessment and appreciation of data processing outcomes.

(b) The measures may involve the use of sandboxes and simulations particularly where there is a likely or probable outcome of harm or injury to a data subject.

(c) An outcome that is adversely different from the original expectation of the processing, shall be treated as a disparate outcome which may upon investigation by the Commission, result in a liability for the violation of the principle of duty of care under the NDP Act.

(d) A data controller or data processor shall take into consideration the interlinked character of human rights and their attribute of inalienability – subject to lawful derogations – when carrying out an assessment of outcomes.

(e) A data controller or data processor is expected to rely on a DPIA in order to assess the outcomes of a proposed data processing activity. Thus, while undertaking a DPIA, further analysis of potential disparate impact is required in order to achieve appropriate standards of data ethics in data processing.

(f) Assessment of Outcomes in this Article means a systematic analysis of the effect or result of data processing particularly on the enjoyment of other fundamental rights and freedoms.

Article 43: Emerging Technologies

(1) A data controller or a data processor who deploys or intends to deploy Emerging Technologies (ETs) such as Artificial Intelligence, Internet of Things and Blockchain for the purposes of processing personal data shall take into consideration:

(a) The provisions of the NDP Act,

(b) Public Policy, and

(c) This GAID, and other regulatory instruments issued by the Commission in order to safeguard the privacy of data subjects.

(2) A data controller or a data processor who deploys or intends to deploy ETs for the purposes of processing personal data is expected to set forth technical and

organisational parameters for the processing in order to design its ET tools in accordance with the threshold of data processing permitted by law – particularly taking into account the:

a) Right of a data subject not to be subject to a decision solely based on automated processes or algorithms;
b) Right to be forgotten – and the possibility of using synthetic data or tokenisation of personal data which may not be amenable to this right;
c) Safeguards for the processing of sensitive personal data;
d) Safeguards for child rights and other vulnerable groups;
e) Regulation of cross-border data flows; and
f) Privacy by design and by default.

(3) The technical and organisational parameters are to be documented and filed with the Commission as part of NDP Act CAR.

(4) A data controller or data processor under the circumstances contemplated by this Article shall:

(a) Carry out a DPIA - particularly taking into account:
   i. Assessment of disparate outcomes of data processing.
   ii. Data Subjects' Vulnerability Indexes (DSVI) as stated in Schedule 6 and the DPIA shall be filed with the Commission as part of NDP Act CAR.

(b) Determine the suitability of:
   i. Data anonymisation upon collection either directly from data subjects or from any legitimate source.
   ii. Testing the ETs in low-risk environments where public interest may be served for a reasonable period and where significant outcomes of their use may be observed.

(c) Determine whether there are disparate outcomes and the possibility of effectively addressing the disparate outcomes.

(d) Retool and return (repeatedly as occasions may warrant) to the controlled environment to re-test the ETs tools until satisfactory outcomes are achieved or a determination may be made to wholly discard the ETs tools on the ground of unmitigable risk to privacy.

(e) Where a determination has been made that the ETs are safe for use, a data controller shall put in place a mechanism for continuous monitoring and evaluation in all circumstances where they may be deployed.

(5) In this Article, the "suitability" or the "possibility" of a safeguard or an act implies an obligation on the part of a data controller or a data processor to take reasonable technical and organisational measures in guaranteeing fair and accountable use of data – taking into consideration data ethics and regulatory audits.

Article 44: Parameters for Assessing Privacy and Public Interest in Emerging Technologies

(1) In line with Section 5(b) of the NDP Act, the Commission shall foster the development of personal data protection technologies, in accordance with recognised international best practices and applicable international law; accordingly, the Commission shall accord priority to ETs which strengthen data privacy.

(2) In furtherance of Section 1(h) of the NDP Act towards strengthening the legal foundations of the national digital economy and guaranteeing the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data, the Commission shall take into account the utilitarian value of ETs in achieving sustainable development through lawful processing of personal data.

(3) A data controller or data processor who intends to process personal data in the circumstances contemplated by Article 44 (2), may benchmark with global consensus on ETs such as the United Nations Resolution on Artificial Intelligence. Accordingly, data controllers and data processors shall, among other self-correcting measures, refrain from or cease the use of ET systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights.

Article 45: Cross-Border Data Transfer

(1) Part VIII of the NDP Act provides for cross-border data transfer. By virtue of Section 63 of the NDP Act, the provisions of Part VIII of the NDP Act shall be the overarching, governing provision in all matters pertaining to cross-border transfer of personal data from Nigeria.

(2) Pending the issuance of any regulatory instrument by the Commission on cross-border data transfer, the explanatory note in Schedule 5 of this GAID shall be used for the evaluation of countries for the purposes of determining their level of adequacy and for other grounds of cross-border data transfer recognised under the NDP Act.

(3) In respect of safeguards for data subjects' rights in a country, the Commission shall take into account the enforcement of fundamental rights in general and the decisions of courts which seek to advance fundamental freedoms in such jurisdictions being considered for adequacy decisions.

Article 46: Capacity Building in Data Protection and Continuous Professional Development Credits

(1) Capacity building is mandatory as an organisational measure of data privacy and protection.

(2) In furtherance of Section 5(e)-(f) of the NDP Act and taking into account the high technical skill required, the Commission shall foster capacity building and professional development in data protection and privacy.

(3) All employees and other persons who are engaged by the data controller or data processor shall be trained and sensitised periodically on emerging developments in data processing and to such an extent that is reasonably relevant to their job descriptions respectively.

(4) The Commission may develop a mechanism in place for the training, and the award of certifications on Data Privacy and Protection.

Article 47: Jurisdiction of Court and Access to Justice

(1) Without prejudice to binding precedents of courts, a data subject has a right to seek redress of the violation of his or her data privacy rights – in line with Section 46 of the 1999 Constitution.

(2) Access to justice for the purposes of national adequacy of data protection includes proximity and access to courts of justice particularly in the context of civil liberties and fundamental freedoms. Accordingly, regardless of the parties involved and the material context of data processing, a data subject may seek redress for the violation of his or her right to privacy at the closest Federal or State High Court in line with settled precedents of the Supreme Court of Nigeria and extant Fundamental Rights Enforcement Procedure Rules.

Article 48: Evidence of Compliance with the NDP Act

(1) Evidence by a data controller or a data processor relating to compliance with the NDP Act or any regulatory instrument issued by the Commission shall be evaluated in the context they directly relate to.

(2) Compliance in relation to registration, filing of annual CAR, submission of DPIA or cross-border transfer instruments approved by the Commission shows commitment to accountability and prima facie good faith in data processing. It does not replace the need to provide concrete evidence in defence of any complaint of violation relating to other provisions of the NDP Act.

(3) The Commission, in furtherance of Section 48(6)(f) of the NDP Act shall take compliance in terms of accountability as a partial fulfillment of cooperation.

Article 49: Consideration of Time-Bound and Non-Time-Bound Obligations

(1) The need to safeguard the rights and freedoms of a data subject as guaranteed under Section 37 by the 1999 Constitution shall be the overriding consideration in considering whether a data controller or a data processor has fulfilled any obligation within a stipulated time or within a reasonable or an appropriate time.

(2) Where the NDP Act or any regulatory instrument issued thereunder does not make an obligation to be timebound, it is expected that such obligation shall be discharged timeously taking into account the urgency of such obligation to the realisation of the rights and interests of the data subjects that are immediately connected to them, and, also, taking into account that if such obligation is not performed within a definite time frame which may be provided by the data subject, the rights and interests of the data subject may likely be abridged or defeated.

(3) In circumstances requiring storage limitation, where no timebound obligation has been provided by law, the storage time for the purpose of data processing shall lapse not later than six (6) calendar months when the original purpose of the processing has been accomplished.

(4) Notwithstanding Article 49(3) and subject to the principles of data protection under section 24 of the NDP Act, a data controller may store personal data with appropriate technical and organisational measures for the purposes of defence of a legal claim or due diligence.

Article 50: Supplementary Regulations, Directives and Schedules

(1) The Commission may at any time issue supplementary regulations and directives for the purposes of amending this GAID; accordingly, a data controller or a data processor shall comply with the provisions of the supplementary instrument as may be issued by the Commission.
(2) Where necessary, the Commission may issue directives or guidance which may be annexed as schedules to this GAID.
(3) In the event of a conflict between this GAID and a supplementary regulation or directive issued by the Commission, the provisions of the supplementary regulation or directive shall prevail.

Article 51: Review of Administrative and Financial Obligations under Special Grounds

(1) The Commission may use its discretion to review any administrative or financial obligation under this GAID or which falls within the discretion of the Commission if such obligations cannot be fulfilled, taking into account any one of the following grounds:
    (a) Bankruptcy of the affected data controller or data processor;
    (b) Legal encumbrances brought about by judicial proceedings;
    (c) Dire humanitarian conditions; and
    (d) Necessities of implementing fiscal or developmental policy, and on the ground that if such necessities are not considered, they may be defeated by the obligations.
(2) A data controller or a data processor or an intervener who seeks a review under this Article shall specifically demonstrate how any ground for review stated in Article 51(1) applies to a data controller or a data processor or to an intervener.
(3) Application for a review under this Article shall be made in writing to the National Commissioner and Chief Executive Officer of the Commission and it shall be supported by a verifying affidavit stating, among others:
    (a) The name of the affected data controller or data processor or intervener;
    (b) The contact address;
    (c) The designated DPO and his or her contact;

(d) The nature and scope of data processing;
(e) A summary of facts in proof of the ground or grounds relied upon; and
(f) A declaration of commitment to the principles of data protection and safeguards for the rights and freedoms of data subjects.

(4) The Commission shall within forty-five (45) days upon the receipt of the application, verify the claims of the applicant stating whether or not the application is meritorious or request for further information and further and better affidavit where the circumstances warrant.

(5) Nothing in this GAID shall result in the grant of a waiver to the detriment of the rights and interests of a data subject.

Article 52: Definitions

"appreciation of outcomes" means a systematic analysis of the effect or result of data processing.

"basic privacy checklist" means a simple list of steps a worker should take when dealing with personal data.

"*data protection officer*" is an expert in data protection law and practices. He or she ensures, in an independent manner, that an organisation complies with the laws relating to processing individual's personal data.

"*data subject access request*" is a request directed to the organisation by a data subject, granting the data subject right to access information about personal data the organisation is processing.

"disparate outcome or disparate impact" means an adverse effect of carrying out an appropriate task. The task becomes inappropriate and unlawful if it could result in a disparate outcome.

"*domiciliation*" means the state of living or permanently residing in a place. Domiciliation of a data controller or data processor outside Nigeria does not mean an exemption from the obligations imposed by the NDP Act or any regulatory instruments issued under the NDP Act. The major point is in data processing; if the data subject is in Nigeria, then the NDP Act protects him or her.

"duly certified" means certified by an institution that is accredited or approved by a competent authority in data privacy protection or in educational services.

"infraction" means any degree of violation of the law or a regulatory instrument.

"*interface with*" means communication with a data subject involving the processing of personal data.

"*interoperable data privacy measures*" are essentially tools and approaches that ensure different data protection laws and frameworks work together seamlessly.
"lodge a complaint" means to report a wrongful or perceived wrongful act.
"may" when used in the context of an obligation in this GAID, indicates that there exist accountability safeguards for regulatory actions for data controllers or data processors to take into consideration. It does not imply that the obligation is merely advisory.
"platform of data processing" means any medium through which a data controller or a data processor handles personal data.
"r*ecord of processing activities*" means a record of data processing activities under a data controller's responsibility, including all categories of processing activities.
"regulatory instruments" mean laws, regulations, directives, codes, guidelines and guidance notices and certifications.
"*relevant authority*" means a data protection authority or a competent authority having jurisdiction over the subject matter of the data processing activity.
"sandbox" means a controlled environment where an initiative or technology may be tested before being deployed in a targeted or intended environment.
"sub-national or sectoral framework" is any regulatory instrument issued for the purposes of operating within a state, local government area or a sector of the economy.
"sustainable development" means a type of development that promotes resilience and inclusiveness such as the Fundamental Objectives and Directive Principles of State Policy and United Nations Sustainable Development Goals.

SCHEDULES TO
NIGERIA DATA PROTECTION ACT-GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE, 2023

- Schedule 1 - Principles of Data Protection
- Schedule 2 - NDP Act Compliance Audit Returns
- Schedule 3 – Data Protection Officer Assessment
- Schedule 4 - Data Privacy Impact Assessment
- Schedule 5 - Guidance on Cross-Border Data Transfer
- Schedule 6 - Data Subject's Vulnerability Indexes
- Schedule 7 - Guidance Notice on Registration of Data Controllers and Processors of Major Importance
- Schedule 8 - Legitimate Interest Assessment Template
- Schedule 9 - Data Subject's Standard Notice to Address Grievance
- Schedule 10 - NDP Act Compliance Audit Returns Filing Fee

SCHEDULE 1
PRINCIPLES OF DATA PROTECTION

Explanatory Note: *Principles of data protection constitute the foundational safeguards of data privacy and protection frameworks. The degree of reliance on the principles in any form of data processing is to be regarded as the measure of respect a data controller or a data processor has for the data subject concerned. The degree of reliance may be examined through the specific outline of technical and organizational measures a data controller or a data processor takes or intends to take to implement the principles of data protection.*

A data controller or data processor shall prioritise "privacy by design and by default" in order to guarantee compliance with the principles of personal data protection. This means that at the outset of devising technical and organizational measures, the focus should be on the responsibility of the data controller or data processor to minimise the risk factors that may exist as a result of engagement with data subjects (for data processing) or unauthorised access, loss or damage of personal data and maximise the controls for the security and privacy of the collected data.

1. *24(1)(a) of the NDP Act: A data controller or data processor shall ensure that personal data is -*

   processed in "a fair, lawful and transparent manner."

   i. "Fair" means the data processing is free from prejudice and exploitation and it is generally consistent with civil liberties in a democratic society.

   ii. "Lawful" means the data processing is founded on at least one of the legal grounds of data processing recognized under Section 25 of the NDP Act and it does not violate any law or principle of law in Nigeria. Nigerian Court precedents on human rights enforcement which respects advancement of fundamental freedoms in other jurisdictions shall be favourably considered for the purposes of evaluating the lawfulness of data processing.

   iii. "Transparent" means due disclosure of all material facts that may help a data subject and the Commission to take informed decisions. Even where consent or contract is not the lawful bases relied upon for data processing, disclosure of material facts for the purposes of regulatory oversight is paramount. A Record of Processing Activities (ROPA) shall in addition to other informational documents required by the NDP Act disclose the material facts referred to in this paragraph. See Sections 27 and 34 of the NDP Act on the information to be provided to a data subject.

2. *24(1)(b) of the NDP Act: A data controller or data processor shall ensure that personal data is -*

   "collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with this purpose;"

i. "Specified" purpose means the declared and exact intention of a data controller or data processor. This is the responsibility of the concerned data controller or data processor.
ii. "Explicit" purpose means the words used to describe the purpose are free from ambiguity. Where practicable, appropriate, images otherwise known as "infographics" or audiovisuals may be used to illustrate the purpose of the data processing. The simplicity and clarity of language is essential to "explicit purpose". Account must be taken of the class of data subjects targeted in the data processing. See Section 27(3) of the NDP Act.
iii. "Legitimate" purpose means a bona fide intention of data processing. A purpose shall not be regarded as legitimate if it overrides the rights and interests of a data subject and it has no basis in law or public policy.
iv. "Compatible further processing" means any form of processing which essentially fosters the realisation of the original purpose or constitutes an innovative progression of the original purpose. Further processing shall not be regarded as compatible if it overrides the rights and interests of a data subject and it has no basis in law or public policy.
v. Processing or further processing of personal data which enables a data processing platform to monitor a data subject's behaviour for the purpose of systematic matching of such behaviour with advertisements or contents without the explicit and voluntary consent of the data subject as prescribed under Section 26 of the NDP Act shall not be deemed as compliant with the principle of "*specified, explicit, and legitimate purposes."*

3. *Section 24(1)(c) of the NDP Act: A data controller or data processor shall ensure that personal data is – "Adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;"*
    i. "Adequate" means appropriate quantity and quality of personal data.
    ii. "Relevant" means materially useful and indispensable in the fulfilment of the specified, explicit, and legitimate purposes.
    iii. "Minimum necessary" means the least possible data which is essential to the fulfilment of the specified, explicit, and legitimate purposes should be collected.
4. *Section 24(1)(d) of the NDP Act*: *A data controller or data processor shall ensure that personal data is –* "*retained for not longer than it is necessary to achieve the lawful bases for which the personal data was collected or further processed;"*
    i. "Retained" is a form of data processing which means keeping personal data for specified, explicit, and legitimate purposes.
    ii. Once the specified, explicit, and legitimate purposes have been achieved or no longer pursued, the legitimate grounds for retaining the data ceases to exist.

iii. A data controller or a data processor must have a clear data retention – otherwise called data storage – policy.
iv. Without prejudice to the priority of the NDP Act as stipulated under Section 63, the retention policy should be consistent with relevant laws.
v. Whenever it is essential to retain data solely for record purposes, a data controller or data processor should determine the minimum data that is relevant and necessary for the record purposes.
vi. Any residue of data that is not needed should be properly destroyed or irreversibly de-identified.
vii. A data controller or data processor is under obligation to communicate its data retention policy to data subjects. The information to data subject in respect of data retention must clearly indicate the implication for Data Subject's Access Request (DSAR).

5. *Section 24(1)(e) of the NDP Act*: *A data controller or data processor shall ensure that personal data is - "accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed;"*
    i. "accurate" means the data being processed or intended for processing is free from foreseeable errors. The data controller or data processor must therefore put in place appropriate technical and organisational measure to ensure data accuracy. The data controller or the data processor shall put in place a functional and efficient system of data rectification for the benefit of data subjects. This also presupposes existence of an opportunity for the data subject to review his or her data with the data controller or data processor.
    ii. "complete" means wholeness of personal data in relation to the specified, explicit, and legitimate purposes of data processing.
    iii. "not misleading" means the personal data collected and its processing are trustworthy representation of the personal data, the processing, the data subject and all material facts.
    iv. "up to date" means that personal data is contemporary in relation to the data subject and the data processing. The data controller or the data processor shall put in place an efficient system of data for periodic review of personal data to ensure its currency or contemporaneity.
6. *Section 24(1)(f) of the NDP Act*: *A data controller or data processor shall ensure that personal data is – "processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach."*
    i. Data controllers and data processors must carefully access the risks to personal data and data subjects in accordance with the provisions of Section 39 of the NDP Act.

ii. Appropriate technical and organisational measures must be taken to address identified risks.

iii. Data controllers and data processors of major importance must determine its security measures vis-à-vis the outcomes of Data Privacy Impact Assessment (DPIA). See Section 28 of the NDP Act and Schedule 4 of this GAID.

iv. In all circumstances of data processing, security risk assessment shall be carried out with reasonable consideration for Volatility, Uncertainty, Complexity and Ambiguity (VUCA) of both internal and external environment where the data processing is taking place or intended to take place. This environment includes but is not limited to foreign jurisdictions targeted for cross-border data flows.

v. A data controller or data processor shall take reasonable measures to mitigate risks to the Volume, Value, Veracity, Velocity and Variety of data.

7. *Section 24(2) of the NDP Act: A data controller and data processor shall use appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.*

a) "Appropriate" means reasonable measures taking into consideration all material privacy factors including but not limited to the data privacy rights, Data Subject's Vulnerability Index (DSVI) in accordance with Schedule 6 of this GAID, foreseeable threats, technology, data sensitivity and resources.

b) "Technical" (otherwise referred to as technological whenever the context permits) means the technology and expertise required in ensuring data protection.

c) "Organisational" means operational rules, regulations, codes, ethics standards, controls or procedures laid down by a data controller or data processor. Effectual and periodic training and sensitisation on data privacy is a pivotal part of organisational measure.

d) "Confidentiality" means secrecy and exclusionary nature of personal data. A data controller or data processor must ensure that personal data is appropriately categorised in order to put requisite access control measures in place.

e) "Integrity" means defined properties of personal data free from any form of unauthorised variation. Where variation of a non-personal data may lead to unauthorised variation of personal data, the non-personal data shall be considered as an intrinsic part of the personal data. Such non-personal data must be properly accounted for and secured.

f) "Availability" means personal data in a useable or processable state. In relation to the data subject, a data controller or data processor shall put in place appropriate technical and organisational measures to ensure that personal data is available for specified, explicit and legitimate purposes. In addition, it should be available for the purposes of data subject access request and data portability.

8. *Section 24(3) of the NDP Act: Notwithstanding anything to the contrary in this NDP Act or any other law, a data controller or data processor owes a duty of care, in respect of personal data processing, and shall demonstrate accountability, in respect of the principles contained in this NDP Act.*
    a) "Duty of care" means the responsibility of a data controller or data processor to carry out data processing professionally and ethically with a view to preventing avoidable harm or injury to the data-subject.
    b) To demonstrate duty of care, a data controller or data processor is under obligation to align its data processing activities with the reasonably high standard of care. This may be evaluated based on industry standard and contemporary best practice.
    c) "Contemporary best practice", "best practice", "good practice" "global best practice" or however called when used in relation to standard of compliance or performance of a duty, means the process or technology employed for carrying out a task is current, tested and trusted.
    d) Inference as to the currency or trustworthiness should be drawn from verifiable used cases and credible expert reviews.
    e) Where available, reputable certifications or codes of conduct may be relied upon as a ground of inference as to the standard of care provided by a data controller or data processor.
    f) "Accountability" means being:
        i. transparent;
        ii. meticulous in keeping record of processing activities;
        iii. promptly responsive to complaints and requests;
        iv. promptly responsive to regulatory procedures and directives; and
        v. committed to the principles of data protection.

SCHEDULE 2
NDP ACT COMPLIANCE AUDIT RETURNS (CAR)
Pursuant to Section 6(d) of NDP Act, 2023.

Name of Organisation					
Address					
Phone			**Email**		
DPO's Name			**Email**		
DPCO's Name			**Email**		
Sector					
Estimated Number of Data Subjects					
PART 1: PEOPLE AND PROCESS (GOVERNANCE)					
S/N	**AUDIT PARAMETERS**	**NDP Act/ GAID**	**TYPES OF ANSWERS**		
			YES	**NO**	**FACTS**
1(A)					
1.	Is the organisation currently registered with the NDPC for data processing?	S.44-45 Art. 9			Provide Registration number.
2.	Is there a designated Data Protection Officer (DPO) for the organisation?	S.32 Art. 11			
3.	Is the DPO a member of staff or a consultant?	S.32			
4.	Is the DPO trained in data privacy and protection?	S.32 Art. 12(2)(c)			
5.	Is the DPO certified by duly accredited certification body for data protection?	S.32 Art 14			Provide Accreditation number.
6.	Is the DPO participating in Continuous Professional Development training?	S.32 Art. 12			
7.	Did the DPO obtain the required Continuous	S.32			Provide Continuous Professional Development Credit.

	Professional Development Credit within 12 months?	Art. 14(8)					
8.	Does the organisation have a schedule for capacity building on data protection for all employees and persons engaged to work on their premises or engage with their data subjects?	S.24 (2)(3) Art. 30					
9.	Does the organisation carry out the training as provided in the schedule?	S.24 (2)(3) Art. 30					
10.	Does the organisation have a Basic Privacy Checklist (BPC) of "Dos and Don'ts" on data privacy provided for all persons working for or with the organisation as prescribed under Article 31(7) of the NDP Act-GAID?	S.24 (2)(3) Art.30 (7)					
11.	Is the Basic Privacy Checklist part of the annexure to the organisation's NDP Act CAR as prescribed under the NDP Act GAID?	S.24 (2)(3) S.39 S.6(e) Art. 30(7)					
12.	Please select from the list **"types of answers"** column, the type of facts that describe the organisation's data protection practices.	S.24			a.	The organisation has a written schedule it follows for the general review of all of its data processing platforms and practices.	
					b.	Only a certain category of data processing in the organisation has a schedule; and the	

						organisation follows this schedule.	
					c.	Procedures in the organisation ensure that data subject's rights are safeguarded in line with the NDP Act.	
					d.	At least one procedure in the organisation may not safeguard data subject's rights	
					e.	The organisation has a procedure for ensuring that it obtains informed consent of the data subject in line with the NDP Act.	
					f.	The process for obtaining informed consent needs more improvement.	
					g.	In the event of offering services to children and persons without legal capacity, appropriate safeguards have been put in place to obtain approval from concerned parents or guardians. Other measures required ethically and legally are implemented.	
					h.	In the event of offering services to children and persons without legal capacity, there is little or no evidence that appropriate safeguards have been put in place to obtain approval from concerned parents or guardians. Other measures required ethically and legally are yet to be implemented or are still being developed.	
					i.	The organisation has a written policy for routine checks on compliance practices which may be carried out without notice to employees.	
					j.	The organisation does not have a written policy for routine checks on compliance practices	

						which may be carried out without notice to employees.	
					k.	The organisation carries out routine checks on compliance practices which may be carried out without notice to employees.	
					l.	The organization relies on data pseudonymisation, anonymisation and encryption methods to reduce exposure of personal data.	
					m.	The organisation has no implemented data pseudonymisation, anonymisation or encryption methods to reduce exposure of personal data.	
					n.	The organisation checks for data protection compliance when procuring new software for data collection purposes.	
1(B)	**PRINCIPLES OF DATA PROTECTION** Please select from the list **"types of answers"** column, the type of facts that describe the organisation's alignment with the principles of data protection.	S.24				By its written policy and in actual practice as **observed** during an audit of all its data processing platforms and practices, data processing in the organisation follows the principles of data protection **on the ground that:**	
					a.	Data processing in the organisation is fair, lawful and transparent.	
					b.	It specifically makes sure that the processing does not override the interests of the data subjects.	
					c.	It is not in violation of any law or public policy in Nigeria; it is reasonable, based on mode of communication and direct engagement (in major indigenous languages and in info-graphics) to state that the data subject is **fully aware** of at	

						least some of the major data processing in the organisation.	
					d.	Data subjects are aware of at least some of the major data processing activities in the organisation.	
					e.	The processing in **all** circumstances is limited to the purpose for which the personal data was/will be collected. Specific and observable efforts have been made to ensure that the data being processed is minimal, adequate and relevant to what is actually needed.	
					f.	Specific and observable efforts have been made to ensure that personal data is not stored longer than the period of usefulness in relation to its lawful purpose and it is appropriately deleted or irreversibly de-identified to guarantee the privacy of the data subject to whom it relates.	
					g.	Specific and observable efforts have been made to ensure that some personal data for research purposes have been irreversibly de-identified to guarantee the privacy of the data subject to whom it relates.	
					h.	Specific and observable efforts have been made to ensure that personal data is accurate, complete, not misleading and, complaints of inaccuracies (if any) are in practice resolved within 21 days or before such complaints become a source of frustration to data subjects (whichever is conducive to the circumstances of an affected data subject).	

					i.	Specific and observable efforts have been made to ensure that the Confidentiality, Integrity and Availability of personal data is not compromised.	
1(C)	**LAWFUL BASES FOR PROCESSING** Please select from the list **"types of answers"** column, the type of facts that describe your organisation's lawful bases.	S. 25			a.	Consent	
					b.	Legal Obligation	
					c.	Contract	
					d.	Vital Interest	
					e.	Public Interest	
					f.	Legitimate Interest	
	Please select from the list **"types of answers"** column, the type of facts that describe the organisation's lawful bases.	S. 25			a.	Consent	
					b.	Legal Obligation	
					c.	Contract	
					d.	Vital Interest	
					e.	Public Interest	
					f.	Legitimate Interest	
1(D)	**PROFILING AND MARKETING** Please select from the list **"types of answers"** column, the type of facts that describe the organisation's lawful bases.	S. 25			a.	Consent	
					b.	Legal Obligation	
					c.	Contract	
					d.	Vital Interest	
					e.	Public Interest	
					f.	Legitimate Interest	
PART 2: TECHNOLOGY (DATA SECURITY CONTROLS AND STANDARDS)							
2(A)	**DATA PROCESSING AND ACCESS CONTROLS** Please select from the list **"types of answers"** column, the type of facts that describe the organisation's access control measures.	Ss.24 & 39			a.	The organisation has a central database (or server) for personal data.	
					b.	The organisation does not have a central database (or server) for personal data.	
					c.	The organisation has other files or registers for personal data outside the database (or server).	
					d.	The organisation does not have other files or register(s) outside	

						the central database (or server) for personal data.	
					e.	Only authorised personnel can access the physical space provided for the central database (or server).	
					f.	Members of staff generally do have access to the physical location of the database (or server).	
					g.	The physical location of the database (or server) is specially secured apart from the general security.	
					h.	Members of staff may access the database (or server) even when they are not specifically authorised.	
					i.	Only authorised personnel can access other files or registers containing personal data.	
					j.	Other personnel could access other files or registers containing personal information without being specifically authorised.	
					k.	Every file or register - in every location of the organisation - containing personal data are kept in a confidential form and place not accessible to unauthorised persons.	
					l.	Some files or registers containing personal data are not kept in a confidential form and place and are accessible to unauthorised persons.	
					m.	A data subject who inputs his or her personal data on a register or file may see the personal data of other data subjects.	
					n.	Reasonable measures have been taken to ensure that a data subject who inputs his or her personal data on a register or	

						file cannot see the personal data of other data subjects.	
					o.	Digital devices such as computers used for data processing have access controls.	
					p.	At least one of the digital devices used for data processing does not have access control.	
2(B)	**DATA ACCESS CONTROL** Please select from the list **"types of answers"** column, the type of facts that describe the organisation's practices in respect of data access control in order to guarantee data Confidentiality, Integrity and Availability within the organisation.	S.39 Art.30			a.	User Specific or Personalised Password	
					b.	2 factor Authentication	
					c.	Multi-factor Authentication	
					d.	Encryption of data at rest	
					e.	Encryption of data in transit	
					f.	Anti- Ransomware	
					g.	Anti-Spyware	
					h.	Anti-Malware	
					i.	Locational Security	
2(C)	**DATA ACCESS CONTROL AND BUSINESS CONTINUITY** Please select from the list **"types of answers"** column, the type of facts that describe the organisation's practices in respect of data access control in order to guarantee data Confidentiality, Integrity and Availability within the organisation.	S.39 Art.30			a.	All the access controls **are adequate** in relation to risks of breaches.	
					b.	**At least one** of the controls may not be very strong or adequate in relation to risk of breaches.	
					c.	The organisation has a schedule for Monitoring, Evaluation and Maintenance (MEM) of its data security system	
					d.	The Schedule for MEM data security was vetted by a certified data security expert in accordance with NDP ACT GAID.	
					e.	The organisation does not have a schedule for MEM of its data security system vetted by a duly certified data security expert.	
					f.	The organisation has a disaster recovery plan.	

					g.	The organisation does not have a disaster recovery plan.	
					h.	The disaster recovery plan is **POOR** because some crucial data may not be recovered.	
					i.	The disaster recovery plan is **FAIR** because crucial data will be recovered but it may take a long time.	
					j.	The disaster recovery plan is **GOOD** because **ALL DATA** will be recovered but it may take a long time.	
					k.	The disaster recovery plan is **EXCELLENT because ALL DATA** will be recovered **ALMOST IMMEDIATELY –** with the least possible latency.	
2(D)	**DATA SECURITY** Please select from the list **"types of answers" column**, the type of facts that describe the organisation's practices in respect of data security to guarantee data Confidentiality Integrity and Availability.	S.39			a.	**Poor** – on the ground that critical security measures are non-existent or not up to date.	
					b.	**Average** – the level of data security measure in place may offer basic protection to sensitive and non-sensitive personal data, importantly, the possibility of a breach which may create harm or compromise the privacy to data subjects is low.	
					c.	**Above Average** – critical security measures are in place but may be vulnerable because some controls that are crucial for the security of sensitive personal data or financial data are not in place or not adequate.	
					d.	**Close to Industry Grade** – Critical security measures and controls are in place but falls below recognised global standards or more specifically, they do not follow any one of the following standards:	
					i.	ISO 27000 series.	

					ii.	National Institute of Standards and Technology Special Publications (NIST SP) 800-*series*.	
					iii.	NIST Cyber Security Framework CSF.	
					iv.	Center for Internet Security (CIS) Critical Security Controls.	
					v.	COBIT.	
					vi.	Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).	
					e.	Industry Grade – adequate technical and organisational measures are in place managed by qualified experts who are certified in accordance with recognised global standards. More specifically, the organisation implements the following standards:	
					i.	ISO 27000 series.	
					ii.	National Institute of Standards and Technology Special Publications (NIST SP) 800-*series*.	
					iii.	NIST Cyber Security Framework CSF.	
					iv.	Center for Internet Security (CIS) Critical Security Controls.	
					v.	COBIT.	
					vi.	Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).	
					vii	The Organisation is also on the National Data Protection Adequacy Programme Whitelist.	

PART 3: ACCOUNTABILITY AND BASIC RISK EVALUATION						
3(A) 1.	**DATA PRIVACY IMPACT ASSESSMENT** At the commencement of operation as an organisation or in the course of operation, did the organisation ever carry out a Data Privacy Impact Assessment (DPIA)?	S.28 Art.29	Yes	No		
2.	Did the organisation deploy a new technology or introduce new measures of data processing within the last year?	S.28 Art.29	Yes	No		
3.	Did the organisation take into consideration the NDP Act in the specification, design and testing of the new technology?	S.28 Art.29	Yes	No		
4.	From the list in "**types of answers"** column, choose the type of facts that describe the organisation's consideration on DPIA.	S.28 Art.29			a.	The organisation is not processing sensitive personal data.
					b.	The organisation processes or intends to process sensitive personal data.
					c.	At least some of data subjects being targeted by the data processing fall within the risk factors under the Data Subjects' Vulnerability Index.
					d.	Data subjects being targeted by the data processing do not fall within the risk factors under the Data Subjects' Vulnerability Index.
					e.	New technology or procedures have been deployed that may significantly impact the privacy of data subjects.
					f.	No new technology or procedures have been deployed that may

						significantly impact the privacy of data subjects.
3(B)	**LEGITIMATE INTEREST ASSESSMENT** Does the organisation rely on legitimate interest to process personal data?	S.25 (1)(b) (v)	Yes	No		
1.	Does the organisation carry out legitimate interest assessment?		Yes	No		
2.	Please select from the list **"types of answers"** column, the type of facts that describe the organisation's practices in respect of legitimate interest.				a	The organisation relies on legitimate interest to foster some of its business interests and this business interests are not, in some cases, connected to security of lives and crime prevention, sustainability of Health, Safety and Environment.
					b	Legitimate interest is only relied upon as a lawful basis when the rights of data subjects are considered and it is EVIDENT that the legitimate interest does not override the rights of the data subject.
					c	Legitimate interest is relied upon only in circumstances that are necessary and relevant to the fulfilment of data processing which already has another lawful basis. E.g. in circumstances of security of lives and crime prevention, sustainability of Health, Safety and Environment.
3(C) 1.	**ACCOUNTABILITY AND RECORD OF PROCESSING ACTIVITIES** Does the DPO prepare Semi-Annual Data	Art. 13	Yes	No		

	Protection Report (SAPR) as provided for under the NDP ACT GAID?						
2.	Please select from the list **"types of answers"** column, the type of facts that describe the organisation's practices in respect of accountability and record of processing activities.	Art. 13			a.	The (SAPR) is an accurate, evidence-based assessment of the organisation's data security based on Art.14 of the GAID.	
					b.	The organisation processed personal data of at least ---------- ---------- data subjects in the last 3 months.	
					c.	The organisation has lawful basis recognized by the NDP Act to process personal data.	
					d.	In instances where the organisation is not sure of its lawful basis, it sought guidance from a DPCO or the NDPC.	
					e.	The DPCO provided guidance on the appropriate lawful basis.	
					f.	The DPCO DID NOT provide guidance on the appropriate lawful basis.	
					g.	The organisation complies with the Nigeria Data Protection Act, and other regulatory instruments issued by NDPC.	
					h.	There are ---------- ---------- complaints by data subjects (or Not Applicable).	
					i.	---------- complaints are under investigation (or Not Applicable).	
					j.	---------- complaints are resolved within ---------- ----------days (or Not Applicable).	
					k.	---------- compliance notices were issued by the NDPC to the organization (or Not Applicable).	
					l.	---------- of the compliance notices have been	

						resolved within ----------days. (or Not Applicable).	
					m.	---------- of Data Subject's Access Requests (DSAR) were received by the organisation. (or Not Applicable).	
					n.	---------- of DSAR are receiving attention? (or Not Applicable).	
					o.	---------- of DSAR were resolved with Data Subjects within ---------- days (or Not Applicable).	
					p.	There are ---------- number of breaches (or Not Applicable).	
					q.	Breach notification was sent to the NDPC within 72 hours. (or Not Applicable).	
					r.	Breach notification was sent to the data subjects immediately. (or Not Applicable).	
3.	Does the DPO submit their report directly to the management at least once in six (6) months?	Art.13 (2)	Yes	No			
4.	Is the report submitted by the DPO acknowledged as provided under NDP ACT-GAID?	Art.13 (3)	Yes	No			
5.	Is the acknowledgement of report submission verified by a Data Protection Compliance Organisation as provided under NDP ACT -GAID?	Art.13 (4)	Yes	No			

PART 4: CROSS-BORDER DATA TRANSFER							
1.	Does the organisation engage in cross-border data transfer?	Ss.41-43	Yes	No			
2.	In the list of "Types of Answers," pick the type of personal data the organisations transfer outside Nigeria.			a.	Sensitive Personal Data.		
				b.	None Sensitive Personal Data.		
3.	Please select from the list **"types of answers"** column, the legal grounds upon which the organisation conducts cross-border data transfer (if any).				a.	Adequacy decision of the Commission in respect of the destination of the personal data.	
					b.	Cross-border transfer instrument approved by the Commission.	
					c.	Fiduciary or Jural grounds in anyone of the applicable circumstances below:	
					i.	Data subject has provided and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections.	
					ii.	Transfer is necessary for the performance of a contract to which a data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract.	
					iii.	Transfer is for the sole benefit of a data subject and — it is not reasonably practicable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such consent, the data subject would likely give it.	
					iv.	Transfer is necessary for important reasons of public interest.	

					v.	Transfer is necessary for the establishment, exercise, or defense of legal claims.	
					vi.	Transfer is necessary to protect the vital interests of a data subject or of other persons, where a data subject is physically or legally incapable of giving consent.	
4.	Are cross-border data transfers documented and assessed for compliance?	YES/NO					
5.	Which countries are these transfers made to?					Select Countries.	
PART 5: DATA PROCESSORS							
1.	Does your organisation use data processors in carrying out its activities?	S.29	Yes	No		(If yes, questions in this section pop up; if no, skip to the next section).	
2.	Is there a written contract between your organisation and the processors?	S.29 (2)	Yes	No			
3.	Please select from the list **"types of answers"** column, choose the type of facts that describe your organisations due diligence in engaging data processors.					The organisation:	
					a.	Implements Data Processing Agreement.	
					b.	Monitors ongoing compliance.	
					c.	Confirms the Processor is duly registered with NDPC as a data controller or processor of major importance.	
					d.	Obtains evidence of Certifications or Standards.	
					e.	Secures methods of storage or transfer of data.	
					f.	Ensures Involvement of Processor in the DPIA process.	
					g.	Implements Clear Incident Response protocols.	

						Confirms compliance of sub-processor (where applicable) with obtaining proof of compliance from the processor regarding the sub-processor.	
4.	Please select from the list **"types of answers"** column, choose the type of facts that describe your organisations due diligence after termination of data processing agreement					The organisation ensures:	
					a.	Data deletion (with confirmation of deletion).	
					b.	Data Return.	
					c.	Anonymisation of data.	
					d.	Audit records (assessed by your organisation.	
					e.	Revocation of access to systems and data.	

SCHEDULE 3
DATA PROTECTION OFFICER ASSESSMENT

SN	METRIC	MARKS
1	Confirmation that the issuing body is an educational body approved or accredited by a competent regulator of educational services.	15
2	Confirmation that the training leading to the award of the certificate is up to 40 hours.	15
3	Confirmation that an examination was conducted as a condition precedent to the award of the certificate.	20
4	Confirmation that the DPO is enrolled on the database of the Commission.	10
5	Cumulative Score for Continuous Professional Development (CPD) Yearly (At least active participation in 4 different progammes recognised by the Commission).	40
	TOTAL	100

SCHEDULE 4
DATA PRIVACY IMPACT ASSESSMENT TEMPLATE

S/N	GENERAL BACKGROUND	
	WHAT TO NOTE	MATERIAL INFORMATION
	Highlight the central work of the organisation, for processing of personal data and the major reasons for carrying out a DPIA.	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. if lack of material information on purpose limitation should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	NATURE OF ENVISAGED (OR ONGOING) PROCESSING:	
	Will data be processed automatically (e.g. by software) or manually (e.g. by people)?	
	What specific areas or types of data will be processed (e.g. customer data, employee data)?	
	Who will this data be about (e.g. all customers, specific employee groups)?	
	Is there a risk of the processing exceeding this intended scope?	
	Will any third-party companies be involved in processing the data?	
	Will this processing involve sending data to other countries (cross-border transfers)?	
	If data is transferred, what legal justification exists (e.g. contractual safeguard)?	
	Considering the processing method and data types, what are the potential risks to data subjects (e.g. unauthorised access, discrimination)?	
	What specific types of data will be processed (e.g., names, email addresses, financial data)?	
	How many people will be affected by this data	

	processing (estimated number)?	
	You can reference similar situations if there are no existing numbers.	
	ASSESSMENT	
	State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to10) in relation to what is reasonably required. E.g. lack of material information on purpose limitation should make the processing score low on the scale of 1 to 10. E.g. lack of information on the capabilities or the processing medium in terms of collection of data, storage, access to data points or personal data files should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	THE LAWFUL BASIS AND CONTEXT OF PROCESSING	
	WHAT TO NOTE	MATERIAL INFORMATION
	State the lawful basis for processing personal data such as consent, legal obligation, vital interest, legitimate interest and public interest. Give reasons for choosing your lawful basis for the processing. **Additional information as to any prior relationship with the data subject will be helpful. Describe the class of data subjects targeted by the processing.**	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. lack of clear lawful basis and description of data subjects should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	NECESSITY AND PROPORTIONALITY:	
	WHAT TO NOTE	MATERIAL INFORMATION
	Explain why the chosen processing method is essential for achieving the legal reason you have for using the data.	
	Briefly explain how it directly helps you achieve your goal.	
	Describe how you will keep data secure and respect people's privacy while processing it.	
	Mention practices common in democratic societies for data protection.	
	Briefly state if you considered alternative methods.	
	Explain why these other methods would not be effective in achieving your legal purpose.	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. lack of clear lawful basis and description of data subjects should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	CONSULTATION OF STAKEHOLDERS:	
	WHAT TO NOTE	**MATERIAL INFORMATION**
	Who are the stakeholders? The data subjects, Nigeria Data Protection Commission and the internal managers of the data processing (e.g. the Management level decision makers, Chief Information Security Officers, Data Protection Officers and users of the data processing medium). **You may rely on surveys, carry out assessment, review instructions from Original Equipment Manufacturers and where necessary interact with them. Seek information on what can make the medium function optimally or malfunction. Seek information as to data Confidentiality, Integrity and Availability.**	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. lack of rigorous consultation on the Confidentiality, Integrity and Availability of data should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	IDENTIFIED/POTENTIAL VULNERABILITIES	
	WHAT TO NOTE	**MATERIAL INFORMATION**
	Account for every possible risk including but not limited to possible inadvertence on the part of data subjects. State the risks to Data Confidentiality, Integrity and Availability. **State the Data Subjects' Vulnerability Indexes (DSVI) under the NDP ACT-GAID that may apply in the processing.** Examine efficiency or promptness in remediation process for data subjects and disaster recovery. Efficiency may be measured by the time it takes a complaint to be resolved, the satisfaction of the data subject and usefulness of the resolution taking into consideration the urgency of the complaint at the material time. Examine the technical capacity of persons involved in data processing - whether they are conversant with technical and organisational measures for data protection that are relevant to the level of their involvement. E.g. data rectification or data subject access request towards: admission into university, travelling, seeking medical service or preventing fraud or alleviating deprivation should be addressed urgently. A resolution which fails to	

	address the urgency in cases such as the above lacks merit.	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. Deficiency in the principles of data privacy and protection or lack of prompt remediation of data subjects' complaints or resilient disaster recovery plan should be treated as high vulnerability. This should make the processing score very low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	
		Choose the fact that approximates to your assessment of risk **NOTE:** *Under NDP Act-GAID Ultimate or decisive credential means any information such as a password or a token. Once provided, it completes a transaction such as opening an email account, access to bank account or access to secure records.*
	Degree of Risk and Potential Harm to Data Subjects - taking into consideration the protocols to be followed in the processing.	**REMOTE** – because personally identifiable information is: lawfully in the public domain/it is limited to nominal contact information (name, phone number and email address)/contains no sensitive personal data/ adequate measures have been put in place to guarantee its Confidentiality, Integrity and Availability and it contains no decisive or ultimate credential for authenticating valuable transactions. Mark here if this is your choice ☐
		Give succinct and cogent reasons for your choice:

		POSSIBLE - it contains decisive or ultimate credential for authenticating valuable transactions. PII may be accessed through extra-ordinary measures. Extra-Ordinary measures are measures that are beyond the state of the art or contained in directives given under public interest to address a clear and present danger or measures given under vital interest of a data subject or a third party. Mark here if this is your choice: ☐
		Give succinct and cogent reasons
		PROBABLE - because it involves covert or over access to personally identifiable information. May or may not contain decisive or ultimate credential for authenticating valuable transactions. PII may be accessed through simple or complex measures. Simple or complex measures are measures that are available through existing software or through directives that are issued under a routine legal obligation. Mark here if this is your choice: ☐
		Give succinct and cogent reasons for your choice:
	Severity of harm	Choose the fact that approximates to your assessment of harm to data subjects.
		MARGINAL OR LOW – because the data processing does not involve sensitive personal data. The processing may not create any avenue through which the data subject may lose his or her life or livelihoods. Mark here if this is your choice: ☐
		Give succinct and cogent reasons for your choice:

		SIGNIFICANT OR MODERATE – because the data processing involves sensitive personal data or the processing may create avenue through which the data subject may lose some marginal fraction of his or her valuables. Mark here if this is your choice: ☐
		Give succinct and cogent reasons for your choice:
		GRAVE OR EXTREME OR ENORMOUS - because the data processing involves sensitive personal data, ultimate or decisive credentials. The processing may create an avenue through which the data subject may lose her life, all or substantial part of his or her livelihood. Mark here if this is your choice: ☐
		Give succinct and cogent reasons for your choice:

POTENTIAL DISPARATE OUTCOMES:	
WHAT TO NOTE	MATERIAL INFORMATION
Consider how data processing might intersect with other rights, particularly the right to human dignity. How can you mitigate risks to these rights? **For example, a survey of disadvantaged group for a good cause (e.g. free healthcare) could still lead to further stigmatisation if the data is handled by people with little sympathy or data security is not adequate.** **Cameras used for security can also limit people's privacy, for example, the use of CCTV. These are deployed for security; however, this may infringe on the right to privacy or inhibit freedom of expression.**	
ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. if lack of material information on the intersection of the processing with other fundamental rights and freedoms that are closely associated with the processing should make the processing score low in this particular metric on the scale of 1 to 10.	
RATIO (If applicable)	

S/N	CROSS-BORDER DATA TRANSFER	
	WHAT TO NOTE	**MATERIAL INFORMATION**
	Will Data Be Transferred Outside Nigeria?	
	If yes, specify the countries where the data may be transferred.	
	Indicate the legal justification for transferring data under Sections 41-42 of the NDP Act (e.g. consent, adequacy decisions by the NDPC).	
	If transferring to a country in respect of which the Commission has not made an adequacy decision. Briefly describe the legal and technical safeguards in place to protect human rights in those countries, considering relevant international instruments like the United Nations Universal Declaration of Human Rights and relevant international covenants.	
	Mention if non-citizens have the same data protection rights as citizens in those countries.	
	Indicate if there are documented instances of systemic discrimination against vulnerable groups.	

	Additional Applicable Laws List any other relevant data protection laws or regulations that apply to the transfer, such as the ECOWAS Supplementary Act, African Union Convention, or the GDPR (if applicable).	
	Data Subject Grievance Redress Describe the specific mechanisms for data subjects to address any grievances related to data transfer (e.g. complaints, procedures).	
	Data Sovereignty Considerations Explain the effectiveness of data sovereignty principles (keeping data within Nigeria) in this specific case. Consider if the data processing is for public service or inherently governmental function. State if (i) The processing may adversely impact national norms/initiatives on: Unity, Faith, Peace and Progress (ii) Loss of access to sovereign or public data for public good may undermine performance of government functions that are data driven. E.g. for security, economic and democratic development (iii) Data subjects may not be able to obtain immediate and effective remedy for violation of their data subjects rights in	

	jurisdictions where their data may be processed. For guidance on public good and national norms see Fundamental Objectives and Directive Principles of State Policy, Chapter II of the Constitution of the Federal Republic of Nigeria, 1999.	
	Data Security Risks Assess any potential risks of data breaches in the transfer jurisdictions, considering actions by state or non-state actors.	
	ASSESSMENT State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required. E.g. lack of material information on the enjoyment of fundamental freedoms in line with international bill of rights should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	

S/N	GENERAL EVALUATION OF THE INTERPLAY OF DATA PROCESSING, PRINCIPLES OF DATA PROTECTION AND DATA SUBJECTS' RIGHTS	
	WHAT TO NOTE	**MATERIAL INFORMATION**
	Itemise the principles of data protection and data subjects' rights. State succinctly the operation of each of the principles and rights in the data processing under assessment. E.g. **The need for Lawfulness, Fairness and Transparency in data processing**: *There is a clear legal ground identified in the processing, the data subjects are not prejudiced and the material information relating to processing are given before, during and after processing to data subjects. Where a procedure of data processing does not mandate the giving of information to data subjects for overriding security reasons or in other circumstances where lawful derogation is permitted, the processing is still subject to statutory guidance or review by NDPC or to judicial proceedings*. It is important to state whether or not the data controller or data processor is accountable to NDPC by way of registration and by filing annual NDP Act Compliance Audit Returns.	
	ASSESSMENT	

	State in the column below whether or not the information available is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required, e.g. lack of material information on how **EACH** of the principles and rights operates within the context of the processing should make the processing score low in this particular metric on the scale of 1 to 10.
	RATIO (If applicable)

S/N	RECOMMENDATIONS FOR MITIGATION OF IDENTIFIED RISKS	
	WHAT TO NOTE	**MATERIAL INFORMATION**
	Risks **List all the potential problems identified during the DPIA related to data privacy (e.g. data breaches, unauthorised access.**	
	Mitigating Risks (Minimum Necessary) **For each risk, explain the simplest and most effective technical and organisational method you will take to reduce the risk (e.g. strong passwords, access controls)**	
	Insurance and Liability **While insurance might help with some issues, it does not replace your responsibility for protecting data.**	
	Commitment to Fixing Problems **If the measures in point 2, do not completely eliminate the risk, explain how you will address any problems that can still occur (e.g., containment measures, indemnity notifying affected individuals).**	
	Sandboxes (Optional) **Evaluate if using a "sandbox" (a simulated environment) to test the data processing activity**	

	before full implementation would be beneficial.	
	ASSESSMENT State in the column below whether or not the information available in all the steps above is adequate. Provide succinct and cogent reasons for your assessment. Provide ratio (on the scale of 1 to 10) in relation to what is reasonably required, e.g. if lack of material information on purpose limitation should make the processing score low in this particular metric on the scale of 1 to 10.	
	RATIO (If applicable)	
	FINAL ASSESSMENT: Select the facts that best align with your assessment	
	GO AHEAD: Data Processing may be carried out because the risk is remote and the recommendations are adequate in addressing the risks in the unlikely event of their occurrence. This assessment particularly takes into account the concrete evidence of necessity and proportionality of the processing, the high degree of enjoyment of data subject rights, data subjects may reasonably expect that their personal data may be processed under the lawful basis recognised by the NDP Act. Mark here if this is your choice: ☐	
	MODIFY DATA PROCESSING: Data Processing may be carried out subject to fundamental modifications as recommended in the DPIA. This assessment particularly takes into account the concrete evidence of necessity and proportionality of the processing and the high degree of enjoyment of data subject rights. Any derogation falls within the scope permitted under the 1999 Constitution of the Federal Republic of Nigeria or there are no derogations because the data subjects may reasonably expect that their personal data may be processed under the lawful basis recognised by the NDP Act. Mark here if this is your choice: ☐	
	STOP DATA PROCESSING: Data Processing should be stopped on the ground that the general nature of the processing appears to be unnecessary and disproportionate. The derogations may fall outside the scope permitted under 1999 Constitution of the Federal Republic of Nigeria. This assessment also takes into consideration other less intrusive methods of data processing, inherent risks and disparate outcomes of the processing. Mark here if this is your choice: ☐	
	FREQUENCY OF REVIEW: State how frequently the DPIA should be reviewed and give succinct and cogent reasons for your choice.	

	Monthly----------	☐
	Bi-Monthly----------	☐
	Quarterly----------	☐
	2 Times in a Year----------	☐
	Annually----------	☐
	Once in 2 Years----------	☐
	Once in the lifecycle of the Data Processing----------	☐
	GIVE COGENT AND SUCCINCT REASONS FOR YOUR CHOICE	

SCHEDULE 5
GUIDANCE ON CROSS-BORDER DATA TRANSFER

1. There are various grounds for data transfer, namely:
    a) Adequacy Decision by the Commission;
    b) Cross-Border Data Transfer Instrument (CBDTI) approved by the Commission; and
    c) Other lawful bases.
2. The Commission may adjudge a country as affording adequate data protection based on the following conditions:
    a) Availability of enforceable data subject rights, the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law; (S.42(2)(a) of the NDP Act). This means*:*
        i. The data subjects' rights in the jurisdiction to be considered as affording adequate data protection are recognised in a legislation or a subsidiary legislation.
        ii. Data subjects in the said jurisdiction are not under any barrier whether economic, social or political in enforcing their rights in a forum duly constituted or recognised in law, and are reasonably accessible to data subjects without undue constraints.
        iii. The judicial or administrative platform or forum for redress operates in accordance with principles of impartiality, equality, independence and respect for human rights.
    b) Existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection. (S.42(2)(a) of the NDP Act). This means the Commission may enter into an agreement with the Data Protection Authority of the jurisdiction for the purposes of Mutual Legal Assistance on:
        i. Investigation of data breaches.
        ii. Enforcement of cross-border decision.
        iii. Intergovernmental information sharing.
    c) *Access of a public authority to personal data; (S.42(2)(c) of the NDP Act). This means: Scrutiny of mode of access by public authority to personal data where this is a derogation from privacy right and taking into account*:
        i. The degree of derogation or margin of appreciation permitted by law;
        ii. The necessity of the access to personal data;
        iii. The proportionality of the method employed for data processing;
        iv. The frequency of access to personal data; and
        v. The opportunity of redress by an aggrieved person and the safeguards for fair hearing.

d) *Existence of an effective data protection law. (S.42(2)(d) of the NDP Act).* This means an Act of Parliament:
   i. Which is in force, and
   ii. It is not subject to any overriding law,
   iii. Not likely to be repealed by an Administrative Act or amended to suit light and transient causes, and
   iv. Amenable to only laws which seek the protection of larger freedoms as recognised by the Universal Declaration of Human Rights, 1948 and relevant customary principles of international law.

e) *Existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers. (S.42(2)(e) of the NDP Act).* This means*:*
   i. An executive body established by the instrumentality of the Sovereign Authority within a sovereign nation – taking into account the efficacy of enforcement of executive decisions in the sovereign nation without any need for a higher power except the courts. In this regard, sub-national authorities do not enjoy independent sovereign powers that may enable them to effectively determine safeguards for data flows across borders. Accordingly, sub-national authorities shall not be considered by the Commission as bodies that are legally empowered to act independently in order to guarantee national adequacy of data protection.
   ii. An administrative body under an establishment of a sovereign authority may be considered as an independent authority for the purpose Section 42(2)(a) of the NDP Act provided that its decisions on the enforcement of data subject rights are subject to appeal or adjudicatory reviews by courts of competent jurisdiction only.

f) *International commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.* (Section 42(2)(f) of the NDP Act). This means the Commission shall consider the international commitments which:
   i. May impact data flows within and across borders – taking into account the possibility of data flows to countries without adequate data protection safeguards;
   ii. Impact the enforcement of data subjects' rights; and
   iii. Generally, impact the efficacy of bilateral agreement with the country being considered for adequacy decision.

3. The Commission may approve CBDTI for a data controller or data processor or a group of data controller and processors in the absence of an adequacy decision. These instruments may be referred to as:
   a) codes of conduct,
   b) certifications,
   c) binding corporate rules, or
   d) standard contractual clauses.

4. The objective of the CBDTI is to ensure:
   a) Proper monitoring of data flows and accountability between or among the parties concerned;
   b) Access to remedy on the part of the data subjects concerned; and
   c) Data Sovereignty.

5. The Commission may consider the outcome of NDP Act Compliance in Audit carried out by a DPCO in respect of a data controller or a data processor seeking approval of a CBDTI before granting approval of same. Similarly, evidence of adherence to global best practice or reputable standards by the data controller or processor shall also be taken into account.

6. (a) The NDP Act recognises special circumstances which may necessitate cross-border data transfer without adequacy decision or approved CBDTI. These special circumstances are covered by Jural or Fiduciary Obligations.
   (b) A data transfer may be referred to as jural when it is founded on a compelling legal right or duty of the data controller or data processor.
   (c) A compelling legal right is different from a business interest. Profit and personal business/organisational development considerations do not fall within this category of a compelling legal right or duty.
   (d) Other lawful bases recognised under the NDP Act are: -
      i. Defence or establishment of a legal claim;
      ii. Vital Interest of another data subject where the data subject is physically or legally impossible to give consent; and
      iii. Public interest.
      iv. The data subject concerned has given and has not withdrawn consent.
      v. The risks must be properly communicated and there must be a clear indication that the data subject understands the risks involved.
      vi. There is a contract involving the data subject as a party.
      vii. If the contract is under negotiation, an agreement in principle will suffice. This agreement in principle may be by series of affirmative actions from which a reasonable inference of constructive consent may be drawn. The amount of data must also be limited to that which is necessary for identification purposes in the envisaged contract.
      viii. The purpose of the transfer is for the sole benefit of the data subject. An inference will be drawn from prior relationship between the data subject and the data controller or data processor. It must be that the data subject would have given consent. The prudential safeguards are that:
         1. The organisation itself is known for carrying out charitable acts for the benefit of others.
         2. The benefits are vital to the welfare of the data subject.

SCHEDULE 6
DATA SUBJECT's VULNERABILITY INDEXES (DSVI)

i. A data controller or data processor shall take into consideration data subject's vulnerability index with a view to developing and implementing adequate technical and organisational measures.

ii. A data subject's vulnerability index is a risk factor which may be peculiar to a data subject, a group or a class of data subject, which, if not particularly considered, may lead to unfair processing or a breach of duty of care in data processing.

iii. The DSVI to be considered by a data controller or a data processor before and during data processing include, but are not limited to the following:

(a) Age – being too old or being a minor.
(b) Health.
(c) Financial Difficulty.
(d) Physical disability.
(e) Lack of:
  i. capacity to exercise freewill;
  ii. education;
  iii. digital literacy; and
  iv. access to online data security support services.

SCHEDULE 7

GUIDANCE NOTICE

REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS OF MAJOR IMPORTANCE AND ALL MATTERS CONNECTED THEREWITH

NDPC/HQ/GN/VOL.03/B/24

(Pursuant to Sections 5d, 6(c), 44, 45 and 65 of the Nigeria Data Protection Act, 2003)

WHEREAS, personal data of citizens and persons (hereafter referred to as data subjects) in Nigeria are being processed by various organisations or persons for myriads of reasons within and outside Nigeria;

AND WHEREAS it is important for the privacy and security of data subjects to ensure that their personal data are processed only by genuine persons or organisations and ONLY for genuine reasons recognised by law;

CONSIDERING that the Nigeria Data Protection Act, 2023 (hereafter referred to as the Act) under section 5(d) empowers the Nigeria Data Protection Commission (hereafter referred to as the Commission) to designate data controllers and data processors of major importance who are to register with the Commission;

NOTING that section 65 of the Act defines a data controller and a data processor of major importance as an entity which *is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate;*

FURTHER CONSIDERING the prior notice and sensitisation programmes in which the Commission specifically referred to data controllers and processors of major importance under section 5(d) of the Act as the only eligible organisations for registration**;**

THUS, in line with its mandate to, among others, designate data controllers and data processors with "*particular value or significance to the economy, society or security of Nigeria"* the Commission hereby issues this Guidance Notice on the Registration of Data Controllers and Processors of Major Importance:

1. Designation of Data Controllers and Data Processors of Major Importance

(1) A data controller or data processor shall be deemed to have ***"particular value or significance to the economy, society or security of Nigeria"*** and hence designated *to* be of major importance if it keeps or has access to a filing system (whether analogue or digital) for the processing of personal data; and:

(a) Processes the personal data of more than Two-Hundred (200) data subjects in six (6) months; or

(b) Carries out commercial Information Communication Technology (ICT) services on any digital device which has storage capacity for personal data and belongs to another individual; or

(c) Processes personal data as an organisation or a service provider in anyone of the following sectors:
   i. Aviation;
   ii. Communication;
   iii. Education;
   iv. Electric Power; and
   v. Export and Import;
   vi. Financial;
   vii. Health;
   viii. Hospitality.
   ix. Insurance;
   x. Oil and Gas;
   xi. Tourism;
   xii. E-Commerce
   xiii. Public Service

(2) This designation does not include the processing of personal data that is specifically excluded by Section 3 of the NDP Act - such as data processing solely for personal or household purposes.

2. Classification of Data Controllers and Data Processors of Major Importance

(1) The Commission classifies data controllers and data processors into three (3) levels or categories of major data processing, namely:

(a) Ultra-High (UHL).
(b) Extra-High Level (EHL).
(c) Ordinary-High Level (OHL).

(2) Ultra-High Level (UHL) shall be a category of data controllers and data processors of major importance that are, among other obligations, generally expected to **abide by global and highest attainable standards** of data protection - taking into account the following factors:

(a) The sensitivity of personal data in their care;
(b) Data-driven financial assets entrusted in their care by data subjects;
(c) Reliance on third-party servers or cloud computing services for the purpose of substantial processing of personal data;
(d) Substantial involvement in cross-border data flows;
(e) Processing the personal data of over Five-Thousand (5,000) data subjects through the means of technology under its technical control or through a service contract;
(f) The need for international standard certifications for people, processes and technologies involved in data confidentiality, integrity and availability; and

Provided always that any four (4) of the foregoing factors in this sub-paragraph 2(2) shall suffice for the purposes of categorisation.

(3) Extra-High Level (EHL) shall be a category of data controllers and data processors of major importance that are, among other obligations, generally expected to abide by **global best practices** of data protection taking into account:

(a) The sensitivity of personal data in their care;
(b) Data-driven financial assets entrusted in their care by data subjects;

(c) Functions as an establishment of government;
(d) Reliance on third-party servers or cloud computing services for the purpose of substantial processing of personal data;
(e) Substantial involvement in cross-border data flows;
(f) Processing the personal data of over One-Thousand (1,000) data subjects through the means of technology under their technical control or through a service contract;
(g) The need for reputable and standardised certifications for people, process and technologies involved in data confidentiality, integrity and availability; and

Provided that any four (4) of the foregoing factors in this sub-paragraph 2(3) shall suffice for the purposes of categorisation.

(4) Ordinary-High Level (MDP-OHL) shall be a category of data controllers and data processors of major importance that are, among other obligations, generally expected to abide **by global best practices** of data protection taking into account:
(a) The sensitivity of data assets in their care;
(b) Inherent vulnerability of data subjects they typically engage with;
(c) High risk to the privacy of data subjects if such personal data are processed by the data controller or data processor in a systematic or automated manner;
(d) Processing the personal data of over Two-Hundred (200) data subjects through the means of technology under their technical control or through a service contract;
(e) The need for adequate technical and organisational measures for data protection;
(f) The need for reputable and standardised certifications for people, processes and technologies involved in data confidentiality, integrity and availability; and

Provided that any four (4) of the foregoing factors in this sub-paragraph 2(4) shall suffice for the purposes of categorisation.

3. Specific Types of Data Controllers and Data Processors and their Fees

(1) The Commission specifies the types of data controllers and data processors of major importance under the classes referred to in paragraph two (2) of this Guidance Notice as follows:

(a) **Ultra-High Level (UHL)** – the amount payable is ₦250,000. These are:
i. Commercial banks operating at national or regional level;
ii. Telecommunication companies;
iii. Insurance companies;
iv. Multinational companies;
v. Electricity distribution companies;
vi. Oil and Gas companies;
vii. Public social media App developers and proprietors;
viii. Public e-mail App developers and proprietors;
ix. Communication devices manufacturers;
x. Payment gateway service providers; and
xi. Fintechs.

(b) Apart from those mentioned in sub-paragraph 3(1)(a) above, organisations that process personal data of over Five-Thousand (5,000) data subjects in six (6) months are also in in the category of Ultra-High Level (UHL).

(c) **Extra-High Level (EHL)** – the amount payable is ₦100,000. These are:

i. Ministries, Departments and Agencies (MDAs) of government;
ii. Micro Finance Banks;
iii. Higher Institutions;
iv. Hospitals providing tertiary or secondary medical services; and
v. Mortgage Banks.

(d) Apart from those mentioned in sub-paragraph 3(1)(e) above, organisations that process personal data of over One-Thousand (1,000) data subjects but less than Five-Thousand (5,000) within six (6) months are also in the category of Major Data Processing-Extra High Level (MDP-EHL).

(e) **Ordinary High Level (OHL)** – the amount payable is ₦10,000. These are:

i. Primary and Secondary Schools;
ii. Corporate Training Service Providers;
iii. Primary Health Centres;
iv. Independent Medical Laboratories;
v. Hotels and Guest Houses with less than fifty (50) suites; and
vi. Processors who process sensitive personal of more than Two-Hundred (200) data subjects for commercial purposes.

(f) Apart from those mentioned in sub-paragraph 3(1)(g) above, organisations that process personal data of over Two-Hundred (200) data subjects but less than One-Thousand (1000) within six (6) months are also in the category of Major Data Processing-Ordinary High Level (MDP-OHL).

4. Data Controllers that are Not of Major Importance

a) Traders or artisans who do not transmit personal data as a trade or business object to other data controllers or processors that may process the transmitted personal data for their business goals.
b) Traders with less than fifteen (15) employees, or Artisans who do not keep any specific filing system of personal data relating to their customers except routine phone contacts files, receipts data, contact addresses and electronic mail addresses.
c) A Community of Friends, Professionals or People of Common Interest who interact on Social Media Platforms.

5. Statutory Obligations on Data Controllers and Data Processors of Major Importance

Section 29(1)(a) of the Act provides that: *where a data controller engages the services of a data processor, or a data processor engages the services of another data processor,* ***the data controller or data processor engaging another shall ensure that the engaged data processor complies with the principles and obligations set out in this Act as applicable to the data controller.*** Accordingly, it is prudent and mandatory for a data controller to ensure that those they engage as processors comply with the obligations that are applicable to the data controller.

6. Exemption of Establishments or Organisations that are Data Controllers and Data Processors of Major Importance

In line with section 44(6) of the NDP Act, the Commission exempts the following categories of data controllers of major importance from registration:

a) Community-Based Associations;
b) Faith-Based Organisations;
c) Foreign Embassies and High Commissions;

d) Judicial establishments or bodies carrying out adjudicatory functions; and
e) Multigovernmental Organisations.

7. Data Processing Fees

(1) Section 6(b) of the Act provides that ***the Commission shall have powers to prescribe fees payable by data controllers and data processors in accordance with data processing activities.*** Accordingly, a data controller of major importance in the category of MDP-UHL shall on pay Five-Thousand-naira (~~₦~~5, 000) as data processing activities fee for each processor it engages for data processing activities within a period of twelve (12) months.

(2) Where a data controller transfers the data processing activity of its data processor to another data processor it shall not be required to pay data processing fee for the new processor within twelve (12) calendar months.

(3) Where a data controller pays for the renewal of registration of its data processors that are in the category of OHL, the data controller shall not be required to pay data processing fee for the same data processor.

Dated this 19th day of December, 2024.

SCHEDULE 8
LEGITIMATE INTEREST ASSESSMENT TEMPLATE

This legitimate interest assessment (LIA) template is designed to help you to decide whether or not the legitimate interest basis relied upon in Section 25 of the NDP Act is likely to apply to your data processing.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?
- Will the processing involve the personal data of a child in anyway?
- Do you have an effective means of carrying out age verification?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA **"what to note sections"** in Schedule 4 of the GAID. If you answer yes to any of the questions on what to note, then you need to conduct a DPIA instead to assess risks in more detail.

Nature of the Personal Data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative? • Do you have any evidence about expectations, for example from market research, focus groups or other forms of consultation?

- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interest basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by	
Date	

What is next

a. Keep a record of this LIA, and keep it under review.

b. Do a DPIA if necessary.

c. Include details of your purposes and lawful bases for processing in your privacy information, including an outline of your legitimate interests.

SECTION 37 OF THE 1999 CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA

SCHEDULE 9
NIGERIA DATA PROTECTION ACT, 2023, GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (NDP ACT - GAID)

(ARTICLE 40)

DATA SUBJECT'S STANDARD NOTICE TO ADDRESS GRIEVANCE (SNAG)

NAME OF DATA SUBJECT (COMPLAINANT)----------
PHONE NUMBER----------
EMAIL ADDRESS ----------
OFFICIAL CONTACT ADDRESS (OPTIONAL) ----------

NAME OF RESPONDENT (Data controller, data processor or a person)----------
---
PHONE NUMBER----------
EMAIL ADDRESS ----------
OFFICIAL CONTACT ADDRESS ----------

NATURE OF VIOLATION (MARK APPROPRIATE BOX) "Personal Data" means PD.

Unauthorised Access to PD	Unauthorised Use of PD	Loss of Record	Intrusive Use of CCTV
Inaccurate Personal Data	Identity Theft	Excessive Processing of PD	Lack of Privacy Policy
Lack of Information/transparency on PD Processing	Processing Denial of Access to PD		
Unsolicited Messages	Breach of Child's Privacy	Preselected Cookies Apart from Necessary Cookies	
Unlawful Automated Processing of PD	Unauthorised Disclosure of PD	Others	

Nature of PD **Sensitive** PD | NON-Sensitive PD

Specify the types of data

Give particulars of violation: When did it happen? Where? Who is involved (if any) How?

Have you suffered any loss? Yes | No

What is the nature of the loss? Financial | Reputational | Health Related | Education Related | Job-Related | Property/Valuable | Family Related | Others

Describe the nature of the loss (if any)

State your demand

Specify time within which the demand is to be carried out

----------days. Between----------20------ AND ----------20----

TAKE NOTICE that the within named data controller/processor/person is under an obligation to protect the privacy rights of data subjects in line with section 37 of the 1999 Constitution and the Nigeria Data Protection Act, 2023. You are to immediately address the complaint herein stated and take a decision on the complaint as specified in this complaint or within 30 days – whichever is earlier.

FURTHER TAKE NOTICE that the Nigeria Data Protection Commission has been notified of this compliant and it is tracked with reference number----------. You may be required to give account of your data processing activities in accordance with the provisions of the NDP Act. Failure to act on this complaint may result in legal liability for you or your organization.

Signature----------Date----------Name----------

OFFICIAL

STATUS REPORT: RESOLVED | UNRESOVED | ONGOING

REMARKS:

SCHEDULE 10

NDP ACT COMPLIANCE AUDIT RETURNS FILING FEE

SN	DCPMI	Tier	Fee (₦)
1.	Ultra-High Level – UHL	A – 50,000 data subjects and above.	1,000,000
		B – 25,000-49,999 data subjects.	750,000
		C – below 25,000 data subjects.	500,000
2.	Extra-High Level – EHL	A – 10,000 data subjects and above.	250,000
		B – 5,000-2,500 data subjects.	200,000
		C – below 2,500 data subjects.	100,000

Issued under my hand this 20th ----------Day of March, 2025



DR. VINCENT O. OLATUNJI, CDPO CPPPS, FIIM
(National Commissioner/CEO)