LawDigits
Education | Research | Innovation

MODULE 2:

PRINCIPLES OF DATA PROCESSING

Practical Course for Professionals

Created By: **Oladipupo Ige**

www.thelegaldigits@gmail.com

General Learning Objectives

By the end of the course, participants should be able to:

- Explain the meaning of personal data, data processing and data usage.
- Identify the roles and responsibilities of Data Subjects, Data Controllers and Data Processors.
- Describe and apply the principles of fairness, lawfulness, transparency, purpose limitation, data minimisation, accuracy, integrity, confidentiality and storage limitation.
- Distinguish between consent, contractual obligation, legal obligation, public interest, vital interest and legitimate interest.
- Identify technical and organisational measures required under the NDPA and GAID.
- Demonstrate the importance of accountability, transparency and user rights.

COURSE OUTLINE

Module 1 – Introduction to Data Processing

- Overview of data, data processing and data usage
- Key parties in data processing:
- Data Subject (DS)
- Data Controller (DC)
- Data Processor (DP)
- Duty of care owed to the Data Subject

Module 2 – Core Principles of Data Processing

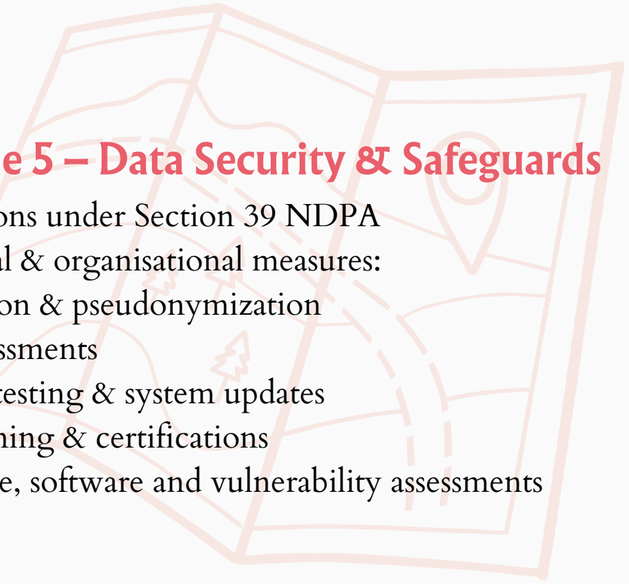
- Lawfulness, Fairness & Transparency
- Definition and operational meaning of Fair processing, Lawful processing, Transparent processing
- Consent, Contractual Obligation, Legal Obligation, Vital Interest, Public Interest, Legitimate Interest

Module 3 – Data Minimization, Accuracy, Confidentiality & Integrity

- Collecting only adequate, relevant and limited data
- Legal requirements under Section 24 NDPA
- Data quality principles: correctness, precision, error prevention
- Linking accuracy to DS rights (rectification, updates)

Module 4 – Purpose Limitation & Storage Limitation

- Processing only for specific, explicit, legitimate purposes
- Information requirements (policies, notices, agreements)
- Retention rules
- Right to erasure and right to be forgotten
- Mandatory erasure under Section 34(2) & GAID Art. 28



Module 5 – Data Security & Safeguards

- Obligations under Section 39 NDPA
- Technical & organisational measures:
- Encryption & pseudonymization
- Risk assessments
- Regular testing & system updates
- Staff training & certifications
- Hardware, software and vulnerability assessments

Module 6 – Conclusion & Next Steps

- Summary of NDPA and GAID compliance expectations
- Future of data processing regulation in Nigeria and globally
- Opportunities in the data governance sector

Principles of Data Processing

Subject to your awareness of the previous module on the necessary definitions of data, data processing and data usage, it is important for you to learn the principles of data processing. In the entire scope of processing, there are three major parties.

1. The Data Subject (DS)
2. The Data Controller (DC)
3. The Data Processor (DP)

For data to be processed ethically and in accordance with the law, the data user and all the parties must understand the necessary principles of processing. These principles include;

i. Lawful, Fairness and Transparency
ii. Data Minimization, Accuracy, Confidentiality & Integrity
iii. Purpose Limitation/Storage Limitation
iv. Data Security and Safeguard

Questions

Who owns your data?

How can you control the use of your data?

What are the uses of your personal data?

What does the law say about data use?

Can you truly control how your data is being used?

Principle 1: Lawful, Fairness & Transparency

Data must be processed in a fair, lawful and transparent manner. See Section 24 NDPA. The questions to be asked in this instance are;

a. When is data processed in a fair manner?
b. When is it processed lawfully?
c. When is it processed transparently?

It is pertinent to state that all DC/DP owe a duty of care to the DS. See Section 24 (3) NDPA.

Fairness has to do with the manner in which the DC collects, uses and retains the data of the subject. The DC must obtain the data legally, use it purposefully and either retain it or erase it when processing is completed or there is no longer any use for the data. This definitely embraces the concepts of purpose limitation, storage limitation and general data use. This includes notifications in terms of processing transparency and putting the necessary systems in place to ensure legitimate data processing activities.

For lawful processing, Section 25 NDPA supported by Art. 16 of the GAID list the lawful basis of data processing. These includes:

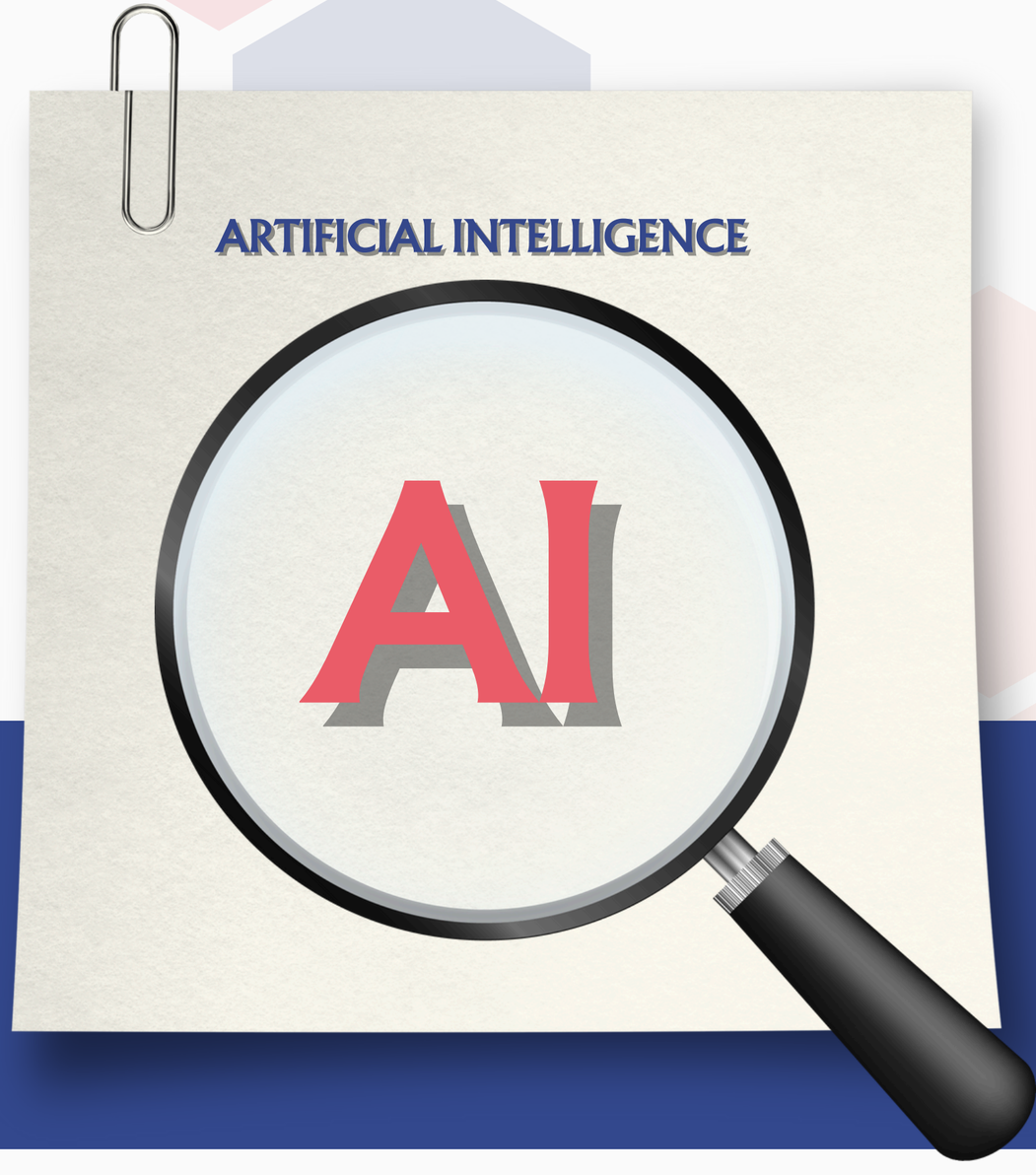
a. Consent
b. Contractual Obligation
c. Legal Obligation
d. Public Interest
e. Vital Interest
f. Legitimate Interest

A. CONSENT:

For a DC to process data lawfully, the consent of the data subject must have given and not withdrawn consent for the specific processing. Under the law, consent is mandatory for;

a. Any direct marketing activity
b. Processing of Sensitive Personal Data
c. Further processing incompatible with the original purposes of processing
d. Processing data of a child
e. Cross-Border Data Transfers
f. Automated Processing

Look at Art 18 GAID.



Advertisements | Promotional Services | Offers | Purchases | New Products

Biometrics | Facial Recognition Systems | Fingerprints

Events | Products Offers | Social Media Posts

Below 18 years | Schools | IDP Camps | Church | Events

Foreign Service Providers

Under the law, the burden of proving consent is on the DC. See Section 26.

Note that silence of inactivity of the DS does not constitute consent. Example: Planet 49 case, Araka v. Ecart, UBA v. Molehin. Also, the DS must be informed of his right to withdraw consent at the time of obtaining the consent as well as other data subject rights.

Consent can be in writing, oral or through electronic means.

Reflections

1. What about writing data in government offices? Is that consent?
2. Can Consent be implied?
3. Is Consent on the internet a farce?

B. CONTRACT:

It is important not to exceed the contractual terms specified for processing. This applies mostly for due diligence and processing agreements. On the part of due diligence at the preliminary stage, data can be processed. However, If contract does not materialize, the DC must erase the data within six (6) months unless a justifiable reason is established. See Art 21.

C. LEGAL OBLIGATION

These involves processing tasks imposed by law e.g order of court, contraption of law, statute or court judgement, tax obligations, legal defense. Myson Nejo case.

Note that government agencies rely on this lawful basis. For example: NIMC, NIBSS, NIS, FRSC etc.

LawDigits
Education | Research | Innovation

LawDigits is a data privacy hub for educational materials, data protection training and consultation. To know more about us, kindly follow us on LinkedIn YouTube

D. VITAL INTEREST

Data can be processed in the vital interest of the DS or an affiliate. In the DS's interest or the interest of a spouse, child, affiliate or even an unknown person. Look at Art 24. This usually applies in life-or-death situations. Instances where vital interest can apply include:

a. Processing health data in Emergencies

b. Disaster Response i.e., Flood, Earthquake, Location Data from telecom providers, Rescue attempts.

c. Humanitarian Crisis or Epidemic i.e., Covid19, Refugees of War, Displaced Persons

d. Imminent threat of danger i.e., swift decision making.

What to consider for vital interest:

a. Strict Necessity
b. Inability to obtain consent
c. Purpose Limitation

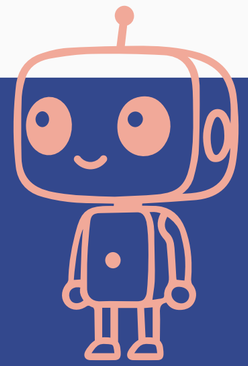
E. PUBLIC INTEREST:

This is similar to legal obligation and vital interest. Issues of public health, census, social programs, danger to public safety, morality, security etc. Advancing matters raised under the Chapter 2 of the Constitution. The processing under this basis should be necessary and proportionate.

F. LEGITIMATE INTERESTS:

This includes support services. For example: Information Sharing, Email Updates, Privacy Policy Updates, Security Safeguards, Data Storage options, Databases, Cloud Storage.

This also applies to innovation and delivery of services such as data training, necessary operations of the company, improvement of user experience and AI testing. For more, observe Art 26.



Question Time

Ever heard of the **"Akara Dilemma?"**

Reflections

1. What happens when there is no lawful basis for processing?
2. How will you know the lawful basis used by the DC?
3. How you protect this right to privacy?

Principle 2: Data Minimisation, Accuracy, Confidentiality & Integrity

Data minimization simply means that a DC must not collect more data than is required for the processing specifically stated. Accumulating unnecessary data can be viewed from two perspectives – Administrative and Regulation.

The Act states that only necessary data should be collected. See Section 24 (1) (c) (d).

The data collected must be adequate, relevant and limited to the minimum necessary for the purposes for which the data was collected. It should be accurate. This relates to the DS right to rectification, right to information and timely updates and confidentiality. For accuracy, the data must be correct, precise and free of errors. It is a matter of data quality.

Principle 3: Purpose Limitation/Storage Limitation

A DC must process data for the specified and explicitly stated purpose. A DC must not overreach. This information must be provided prior to processing, and the DC must stick to it. This can be specified in Privacy Policies, Term of Use or Processing Agreements. This also applies to physical events. Observe Section 24 (1) (b).

Examples include: Multichoice, Fidelity Bank, ClearviewAI etc.

Please note that provision of information must be explicit, clear and in a simple language. Observe Art 27.

For Storage Limitation, a DC must not store or retain data of the DS for more than necessary. According to the law, data should not be retained for longer than necessary to achieve the lawful basis stated during collection. This links to the concepts of data erasure, retention period and the right to be forgotten.

Per Section 34 (2) and Art 28, a DC must erase data without undue delay. Note that the DS can also request for such erasure or even object to processing. Naturally, erasure is advised if the data is inaccurate, outdated, incomplete or misleading. This also applies when the data is no longer needed or there is no other justifiable legal basis for processing.

Ask Questions

EQUIBRIDGE ATTORNEYS

BARRISTERS | CONSULTANTS | SOLICITORS

Hoping to participate in data protection civil class actions or file data privacy claims against your data controller? Reach out to us in **EBA** at **ebafirm@gmail.com**.

To know more about us, visit our website at: **www.ebafirm.com**

Follow us on LinkedIn

Principle 4: Data Security and Safeguards

The law mandates that a DC must implement appropriate technical and organizational measures to ensure security, integrity and confidentiality of data. The DC must protect data from unauthorized or unlawful processing, access, loss, destruction, damage or any form of data breaches. See Section 39.

A DC must take into account the amount of data and the level of sensitivity. Must consider the nature, degree and likelihood of risks that could result from the loss, disclosure or misuse of the personal data, the extent of processing, the data retention period, cost of technical tools relative to the size of the DC or its processor.

The law provides that these security measures may include: Pseudonymization, Encryption, processes to ensure security, periodic assessment of risks to processing systems and services, regular testing and updates. See Section 39 (2).

Other measures include trainings, certifications, software updates, vulnerability testing, database testing, hardware assessments, authentication checks and encryption reviews. For more, see Art 29.

CONCLUSION

Thank you for attending this course. We hope you have received value for your commitment.

For more information, assistance or guide on data protection, cybersecurity or artificial intelligence, kindly reach out to Dipo directly on Linkedin. Please note that we offer legal courses in data protection, consumer protection, cybersecurity and artificial intelligence to companies, government agencies and train professionals.

Course materials will be forwarded to each attendee. Kindly refrain from duplicating, unauthorised sharing or destruction as they remain the intellectual property of LawDigits. To assist us with our work and tell us how we can improve, please contact us.

Special Appreciation

Hoping to be part of more conversations on how to address privacy, technology, cybersecurity issues and the sensitisation of executives and the entire population in Nigeria and beyond.

Thank you for the opportunity.

Most grateful.

DIPO IGE

Managing Partner, **EBA**

Convener, **LawDigits**

Director, Policy & Advocacy **(DPLAN)**