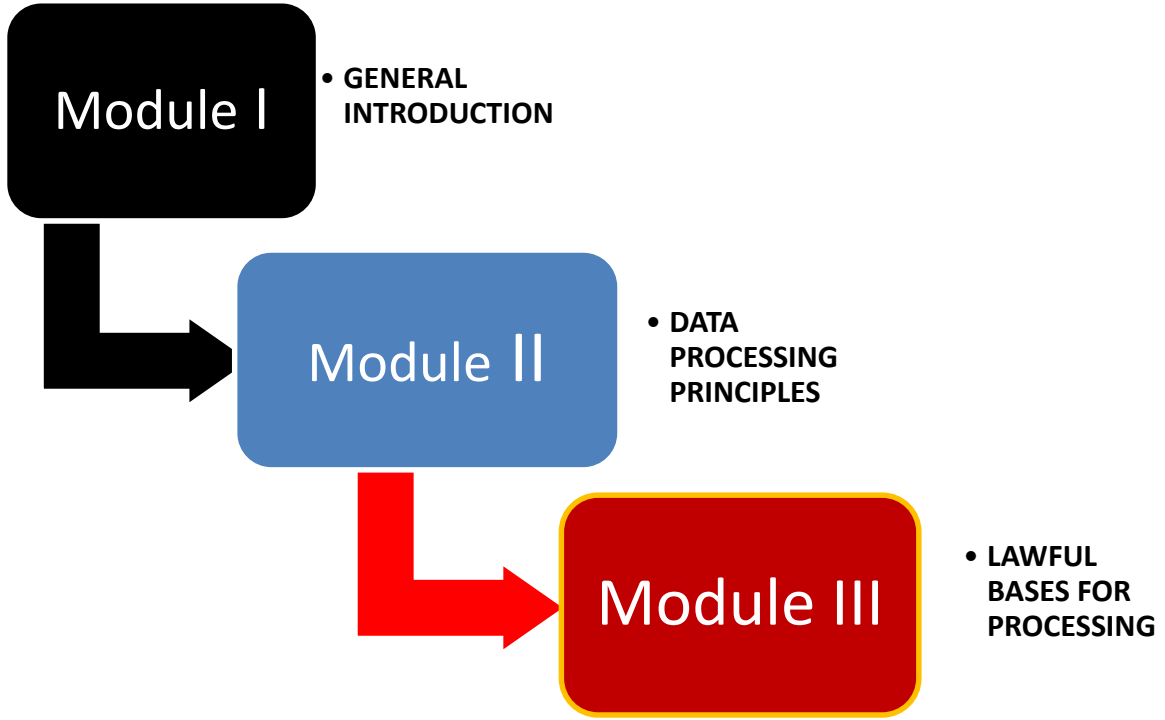
CYBER SECURITY AWARENESS TRAINING

AGENDA


Module I
• GENERAL INTRODUCTION
Module II
• DATA PROCESSING PRINCIPLES
Module III
• LAWFUL BASES FOR PROCESSING

MODULE 1

GENERAL INTRODUCTION


WHO HAS
ACCESS
TO YOUR DATA?

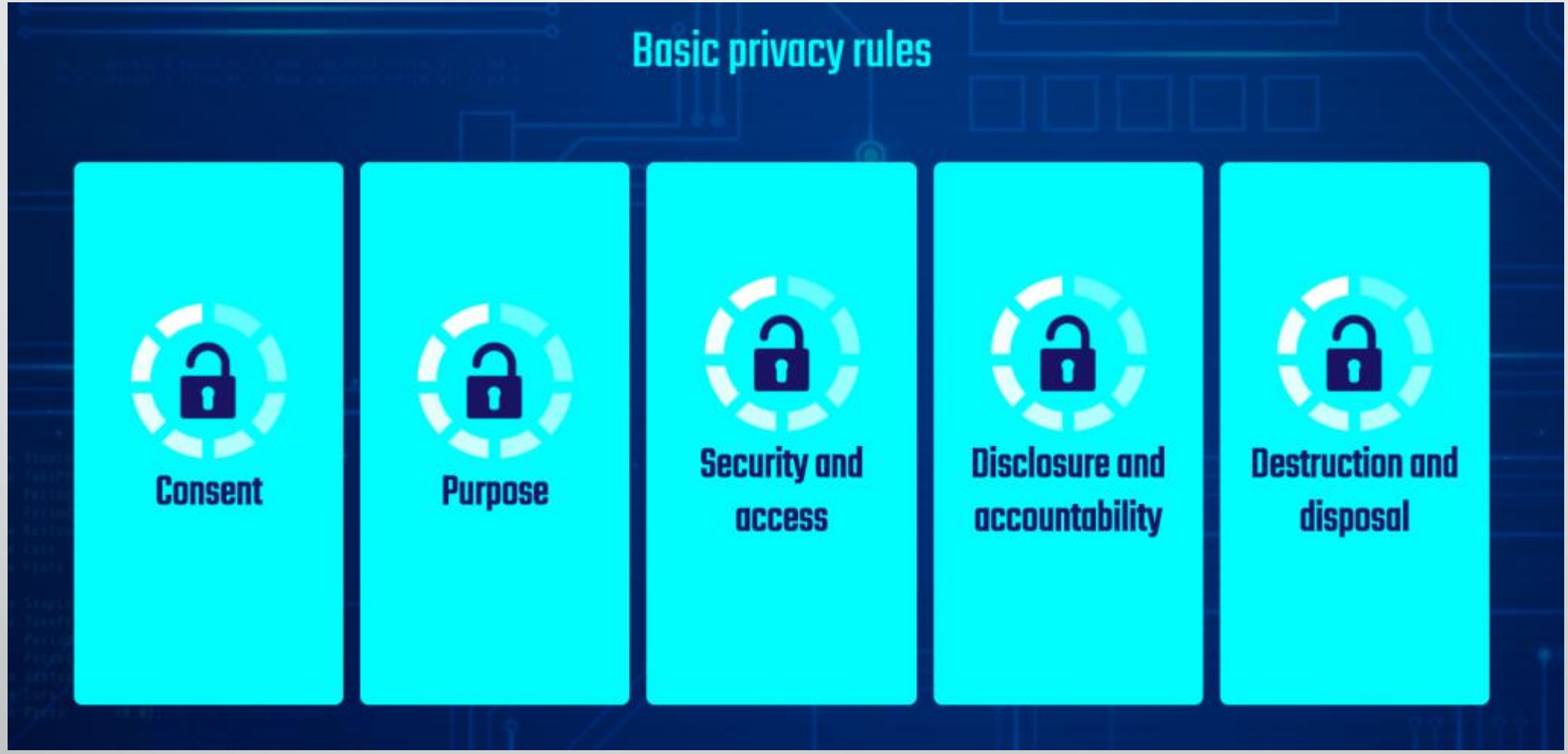
Why NDPR

New challenges are emerging in the form of new technologies, business models, services and business are increasingly relying on data analytics, tracking, profiling, and artificial intelligence.

Personal data v Business data

S/N	Personal Data	Business Data
1.	Identifies living individuals in Nigeria or Nigerians abroad	Identifies businesses/Companies or their operations in Nigeria
2.	Protected under the NDPR and other ancillary legislations	Protected under the Copyright Act, Patents and Design Act, Trademarks Act, etc.
3.	BVN/NIN, Phone number, location, health records, email address etc. of individuals	Statistics, Account books, Physical assets, trade secrets/ intellectual property
4.	Comes with Data Subjects rights and additional obligations to protect and not to collect and/or use same for other undisclosed reasons.	Mostly comes with confidentiality obligations devoid of extensive data subject's rights.

Basic Privacy Rules for Data Collection



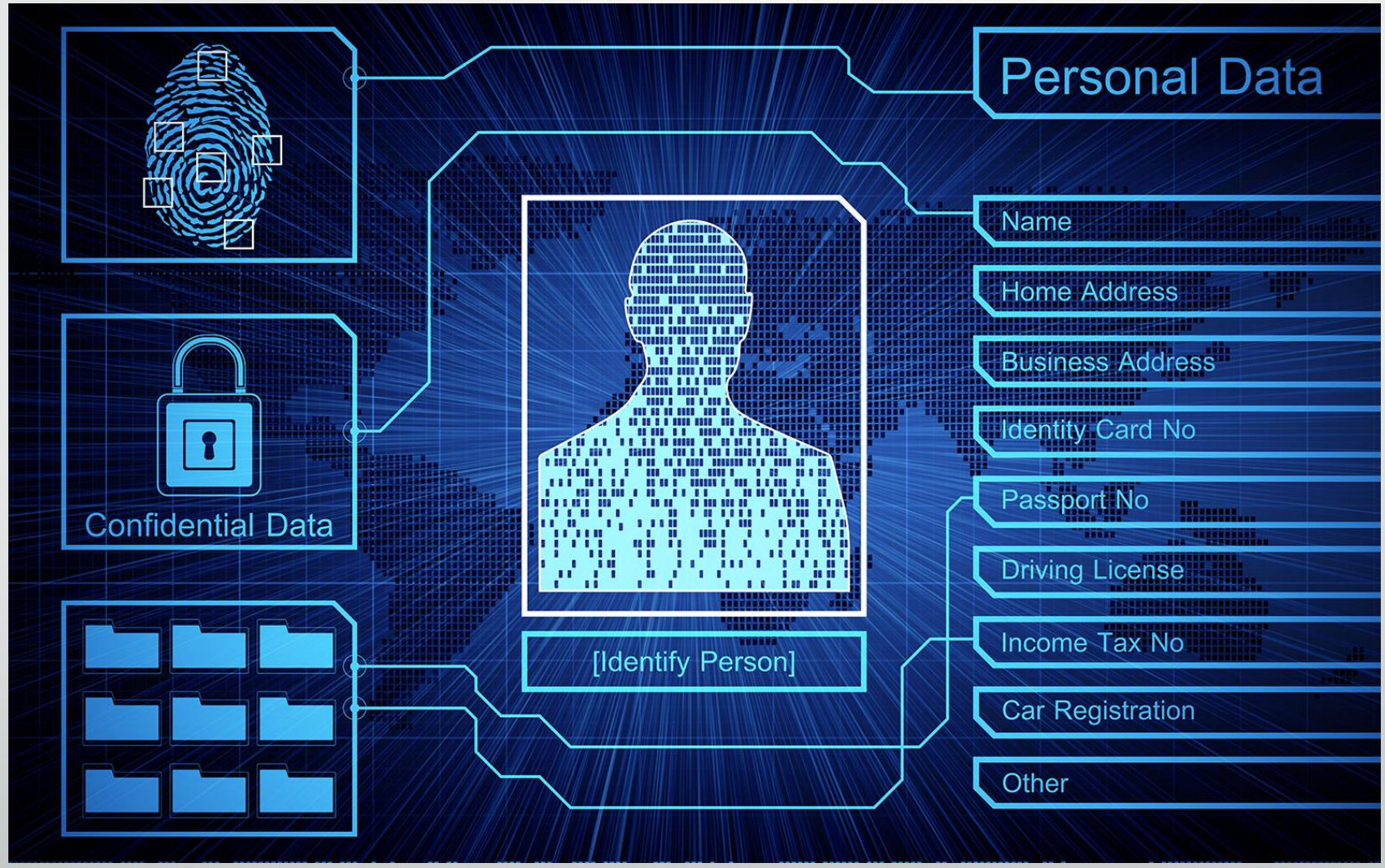
How will the training benefit You and Central Bank of Nigeria?

- You and CBN will be equipped with the knowledge necessary to ensure compliance with the NDPR.
- You and CBN will be able to demonstrate compliance with the NDPR by providing evidence of training.
- CBN may avoid hefty fine by the Regulator in the event of a data breach.

How will the training benefit You and Central Bank of Nigeria?

- The training will help you and CBN towards the prevention of data loss and data misuse.
- You and CBN will be able to build a data protection compliance regime in your business operations from ground up.
- You will be able to identify breaches and red flag situation as soon as possible.
- You will be empowered with reporting anything that you feel compromises data protection compliance, privacy, security of customers and employees of the organisation.

Personally Identifiable Information (PII)



General Introduction to the Concept of Right to Privacy.

The Right to Privacy (4 Harvard L.R. 193 (**Dec. 15, 1890**)) is a law review article written by **Samuel Warren and Louis Brandeis,** and published in the 1890 Harvard Law Review. It is "one of the most influential essays in the history of American law and is widely regarded as the first publication advocating a right to privacy, articulating that primarily that natural persons have a **"right to be let alone.**

The article is attributed to a specific incident to an intrusion by journalists on a society wedding, but in truth it was inspired by more general coverage of intimate personal lives in society columns of newspapers.

General Introduction to the Concept of Data Protection and Privacy.

- **The Universal Declaration of Human Rights, [1948]** an international document adopted by the **United Nations in Article 12 states that**: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

- **The International Covenant on Civil and Political Rights[1966]** [ICCPR] a multilateral treaty adopted by the United Nations affirms in Article 17 that: **1.No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.**

General Introduction to the Concept of Data Protection and Privacy contd.

- **Section 37 of the 1999 Constitution - Right to privacy is one of the fundamental human rights entrenched in the Nigerian Constitution.** It provides that: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."
- **Child Rights Act 2003** – reiterates the constitutional right to privacy as it relates to children subject to parents or guardian rights to exercise supervision and control.
- **Consumer Code of Practice Regulations 2007** issued by Nigeria Communications Commission requires all licensees to protect consumer information against improper or accidental disclosure.
- **Cybercrime Act 2015** – it requires financial institutions to retain and protect data of its customers and criminalises the interception of electronic communication.


Privacy is a Human Right

Development of Data Protection in Nigeria

- New challenges are emerging in the form of new technologies, business models, services, and systems increasingly rely on analytics, tracking, profiling, and artificial intelligence.

- The spaces and environments we inhabit and pass through generate and collect data from human behaviour.

- The devices we wear and carry with us, install in our homes, our channels of communications, sensors in our transport and our streets all continue to generate more and more data footprints. Personal data footprints are now significant and hardly erased.

- It became imperative that privacy rights of natural persons are better protected through a “one stop” legislation which takes into consideration the various emerging issues including developments in Information Technology.

Introduction to the Nigeria Data Protection Regulation (NDPR)

- The Nigerian Data Protection Regulation (NDPR) was released in January 2019 on the protection of natural persons with regards to the processing of personal data and the free movement of such data.

- The NDPR was issued by the National Information Technology Development Agency (NITDA) as a subsidiary legislation to the NITDA Act. The NDPR came into effect on January 25, 2019 with NITDA as the regulatory authority under the Regulation.

Introduction to the Nigeria Data Protection Regulation (NDPR)
Objectives of NDPR contd.

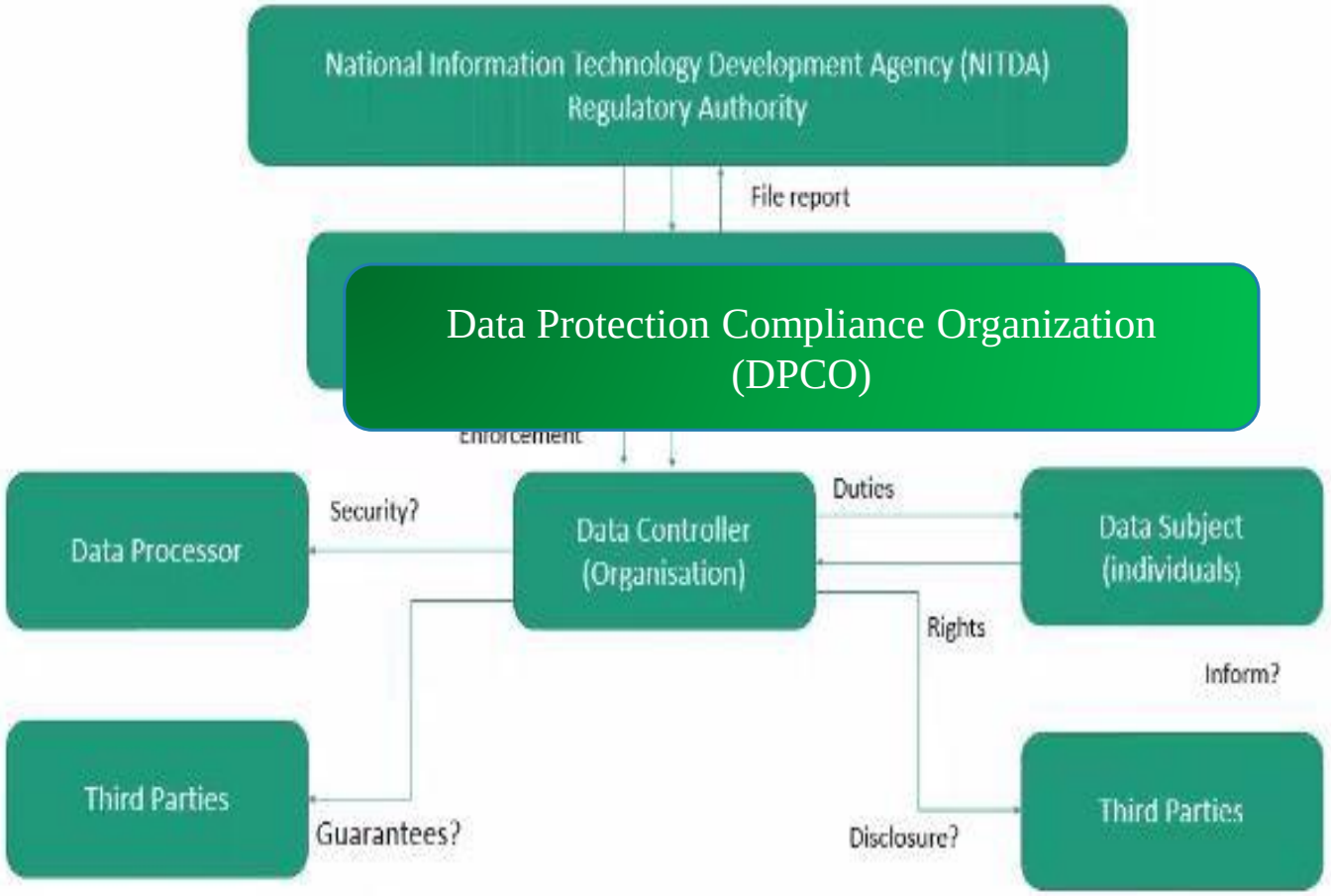
- To safeguard the rights of natural persons to data privacy;
- To foster safe conduct for transactions involving the exchange of personal data;
- To prevent UNLAWFUL manipulation of personal data; and
- To ensure that Nigerian businesses remain competitive in international trade through the safe guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

Introduction to the Nigeria Data Protection Regulation (NDPR) contd.

Scope of the NDPR

- The NDPR will apply to organizations present in Nigeria and processing personal data in the course of the ordinary operations of such an establishment.
- The NDPR applies to all transactions intended for the processing of personal data of natural persons residing in Nigeria or Nigerian citizens residing in foreign jurisdictions.
- Based on the NDPR, data processing includes the collection, recording, storage, retrieval, use, disclosure, transmission, erasure and destruction of personal data.

Data Protection Model Under NDPR



Brief review/comparison of the NDPR with Data Protection laws in other Jurisdictions particularly:

- The EU (GDPR)
- UK (Data Protection Act 2018/ UKGDPR)
- USA, South Africa and Kenya

Key definitions under the NDPR (Article 1.3)

- ***Data subject***

A Data Subject means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [Article 1.3 (xiv)].

- ***Data controller***

This means any person who either alone, jointly with other persons or in common with other persons or a statutory body collects and determines the purposes for which personal data is processed or used [Article 1.3 (x)].

Key definitions under the NDPR contd.

- ***Data processor/Administrator***

A data processor/Administrator is a person or organisation that processes data on behalf of a data controller.

Other IT providers are also processors. , outsourced messaging or email providers etc. processing data on behalf of the data controller are Processors. [Article 1.3 (ix)].

- ***Personal data***

Personal data is any information by which a natural person can be identified, whether directly or indirectly. this includes: names, address, phone number, email address, sex, place of origin, location data, post on social media, bank details, thumbprints, photo, movement register, religion, political affiliation, health records/medical reports, etc. [Article 1.3 (xix)].

Key definitions under the NDPR contd.

- ***Processing***

Personal data is processed when it is stored, collected, recorded, adapted, retrieved, archived, used, disclosed, erased, destroyed, classified or when any operation is performed on them whether or not by automated means [Article 1.3 (xxi)].

- ***Consent***

Consent is a freely given, specific, informed and unambiguous statement or clear affirmative action by a data subject which signifies agreement to the processing of his/ her personal data [Article 1.3 (iii)].

Special Categories of personal data

Personal data as defined above includes any information that identifies a natural person, certain category of personal data are special and thus referred to as sensitive personal data, to which the consent of the data subject must first be obtained before they can be processed. Examples include:

- Religious belief
- Sexual orientation
- Medical records
- Political views
- Racial/ ethnic origin
- Criminal record
- Genetic/ Biometric data
- Trade union membership

Brief Introduction to the role of the NITDA as a regulatory authority under the NDPR

The National Information Technology Development Agency (NITDA) is statutorily mandated by the NITDA Act of 2007 to develop regulations for electronic governance and monitoring of the use of information technology and electronic data (section 6 of the NITDA Act). Charged with this function NITDA issued the NDPR to regulate data protection and privacy in Nigeria.

The NITDA formulates policies for public and private institutions in Nigeria around the handling of personal data, commissioning of ICT projects, intergovernmental data sharing, interoperability of governmental ICT databases and an eGovernance initiative.

MODULE 2:

DATA PROCESSING PRINCIPLES

HOLISTIC AND DETAILED REVIEW OF THE 6 PRINCIPLES OF PROCESSING PERSONAL DATA UNDER THE NDPR (The 6ps) – Article 2.1of the NDPR

- Lawfulness: processing activities must be lawful, transparent and fair. There must be a lawful basis for any Personal Data processing activity.

- Specificity: Personal Data must only be collected for specified, explicit and legitimate purposes.

- Adequacy: Personal Data being processed must be adequate and relevant to the processing activity and accordingly limited to such purpose(s).

HOLISTIC AND DETAILED REVIEW OF THE 6 PRINCIPLES OF PROCESSING PERSONAL DATA UNDER THE NDPR (The 6ps) – Article 2.1of the NDPR

- Accuracy: Personal Data must be accurate and kept up to date.
- Storage: Personal Data must be retained only as long as reasonably necessary.
- Security: Personal Data must be processed in a manner that guarantees its security, confidentiality, integrity and availability.

Six NDPR Principles to Ensure Accountability

LAWFULNESS

Transparent and fair –You must process all user data for a specific purpose, clearly and truthfully stated and agreed to by the user

PURPOSE LIMITATION

Collect data for specified, legitimate purposes –purpose all user data for specific purpose. You must gain explicit consent from users for this

INTEGRITY

Data safeguarding – processors must protect user data against unlawful processing or loss, encryption and privacy by design are required

DATA MINIMIZATION

Limit the amount of data – Review all data you store is accurate, up to date and accessible ideally, users can securely update or delete their data themselves

STORAGE LIMITATIONS

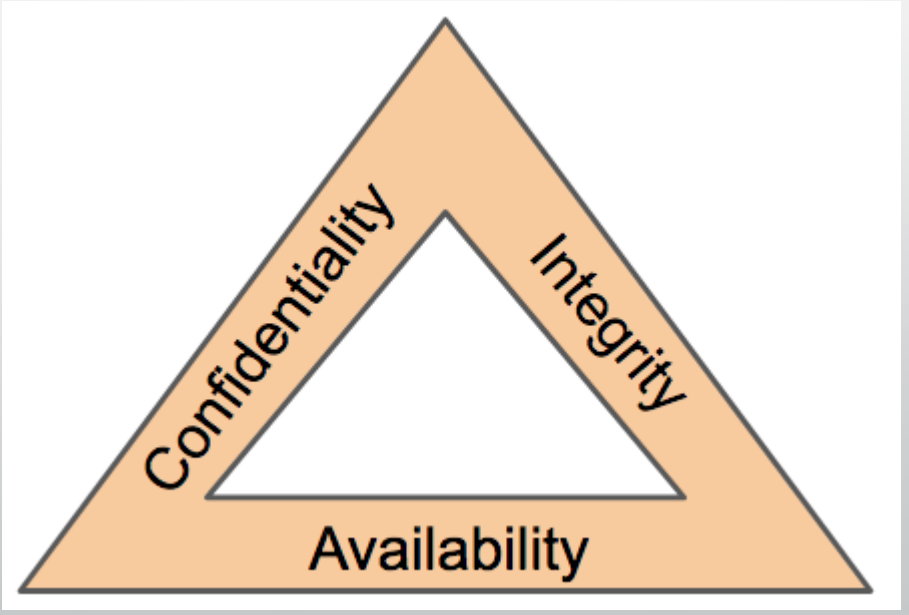
Only keep data you need – if you no longer need a user's data, delete it. If you keep it for longer, use a pseudonym to protect user identities

DATA ACCURACY

Kept up to date – Ensure all data you store is accurate, up to date and accessible, ideally, users can securely update or delete their data themselves

Data Security (Article 2.6 0f the NDPR)

- Personal data must be processed in a manner as to guarantee its confidentiality, integrity and availability. Accordingly the use of USB sticks in the transfer of personal data should be discouraged. Also, the transfer of personal database via email should be avoided.



Data Security (Article 2.6 0f the NDPR)

- Data controllers have a duty to secure all personal data within its control against all foreseeable hazards and breaches, such as theft, cyber attack, manipulation, damage by fire or rain etc.

- The NDPR itemized several security measures for data protection which includes: firewalls, encryption, storing data securely with access to specific authorized individuals and protection of emailing systems, requisite organisational policies etc.

- Data controllers are also encouraged to implement one information security standard (such as ISO 27001, COBIT 2019, NIST etc.

Data Security contd.

Accountability

Data Controller & Data Processor must:

- Implement appropriate technical & organisational measure to ensure and demonstrate compliance (e.g. training, policies, procedures, processes, audits etc.)
- Maintain relevant documentation (such as record of processing activities, data inventory, personal data, categories of data subjects, transfers to 3rd countries, retention policy, security measures etc.)
- Implement data protection by design (e.g. data minimisation, pseudonymisations, transparency, security)
- Use Data Protection Impact Assessments /Risk Assessments
- Appoint a Data Protection Officer

Privacy Notice (Article 2.5 of the NDPR)

- The Data Controller or Data Administrator must prior to collecting Personal Data, provide certain information to the Data Subject. This information should be contained in a Privacy Policy or Notice that must be conspicuously included in the medium by which the Personal Data is being collected.

- This is a very important responsibility of the Data Controller or Data Administrator who must ensure that the Privacy Policy or Notice and its information must be expressed in clear and easily understandable language.

Contents of a Privacy Notice

The Privacy Notice must, among other information, state:

- The rights of the Data Subject, that is, the rights to consent, access, object, be forgotten, rectification, restrict processing and Personal Data portability.

- The purpose and or lawful basis of the processing activity; that is whether as a result of: consent, contractual obligation, legal obligation, legitimate interest, public interest or vital interest;

- The technical methods used to collect and store Personal Data, for example, cookies, JWT, web tokens, data footprint. Artificial intelligence etc.

Contents of a Privacy Notice

The Privacy Notice must, among other information, state:

- The identity and contact details of the Data Controller and its representative(s);
- Where there is one, the DPO’s contact details;
- How long the Personal Data will be stored for;
- The details of the supervisory authority, for example NITDA, to lodge complaints with if the Data Subject’s rights are infringed;
- The available remedies in the event of violation of the Privacy Policy and the time frame for the remedies

MODULE 3:

LAWFUL BASES FOR PROCESSING

Lawful bases for processing data under the NDPR – Article 2.2

Lawful Processing of Personal Data (Article 2.2. NDPR)

- The Data Subject has given **consent** to the processing of his or her Personal Data for one or more specific purposes. The consent must be unambiguous, must be seen to be freely given (informed) by a clear affirmative act.
- The Processing is necessary for the **performance of a contract** to which the Data Subject is party to or in order to take steps as the request of the Data Subject prior to entering into a contact
- Processing is necessary for compliance with **legal obligation** to which the Controller is subject to.
- Processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person, and
- Processing is necessary for the **performance of a task carried out in the public interest** or in exercise of official public mandate vested in the Controller

EXCEPTIONS UNDER THE NDPR

The NDPR does not apply to:

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

Section 2.1 of the NDPR Implementation Framework, 2020.

Contents of a data sharing agreement

Data Sharing Agreements - A DSA must amongst other things:

- identify at least one lawful basis for sharing data,
- always share personal data fairly and in a transparent manner.
- ensure it is reasonable and proportionate.
- ensure individuals know what is happening to their data unless an exemption or exception applies.
- ensure personal data is processed securely, with appropriate organisational and technical measures in place and;
- have policies and procedures that allow data subjects to exercise their individual rights with ease.


Thank you!

Any

Question