Understanding GDPR and Nigeria's Data Protection Regulations

INTRODUCTION

- **Data privacy is a global priority. Both GDPR (EU law) and NDPR (Nigeria's regulation) ensure customer data is collected, processed, and stored responsibly.**

- **NDPR (Nigeria Data Protection Regulation) governs the use and protection of personal data in Nigeria, while GDPR (General Data Protection Regulation) regulates the use and protection of personal data across European Union member states.**

- **Relevance to Olive Monies: As an international money transfer operator, compliance builds customer trust and regulators as well as supports secure cross-border remittances**

GDPR AND NDPR REGULATION AWARENESS TRAINING OBJECTIVES

01 Core principles of Data protection.

02 Personal data and what constitutes personal

03 data subject rights, data breach and reporting

04 Legal bases for processing Personal data

05 Data controller, data processor and employees responsibilities

What is Personal Data?

Personal Data is any information that relates to an identified or identifiable individual, either directly (e.g., name, ID number) or indirectly (e.g., location data, online identifier).

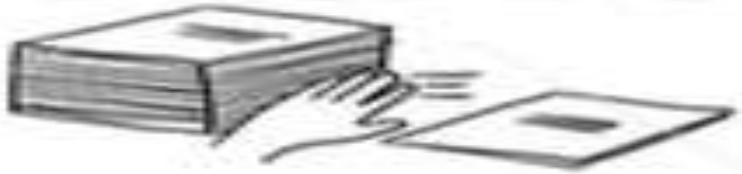
Principles for the Processing of Personal Data under the GDPR

Lawfully

Fairly

Transparent

Purpose



Minimisation

Accuracy

Storage Limit

Integrity

Accountability

bject (DS)
ersons whose
data (PD) is
a controller or
line with art. 3
DPR.

Allow the rectification of inaccurate
provision of supplementary data.

Right to Erasure - "Right to be For
Erase the PD, when a DS request so
are no legitimate grounds for retaini

Right to Restriction of Processing
Impede the processing of PD under
situations stated in Art. 18, e.g. it is

Notification Obligation
Notify any rectification or erasure or
of processing to each Recipient. Exe

Right to Data Portability
If Art.20(1) applies, give back the PD
required and allow the transfer to an

Legal Bases for Processing Personal Data

	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	Can withdraw consent
Contract	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interests	✓	✓	✓	✓	✗	✗
Public Tasks	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓

So, What's the Difference Between a Data Controller and a Data Processor?

Data subject

The individual that the information relates to

Data controller

The legal 'person' who determines how the data will be processed

Data processor

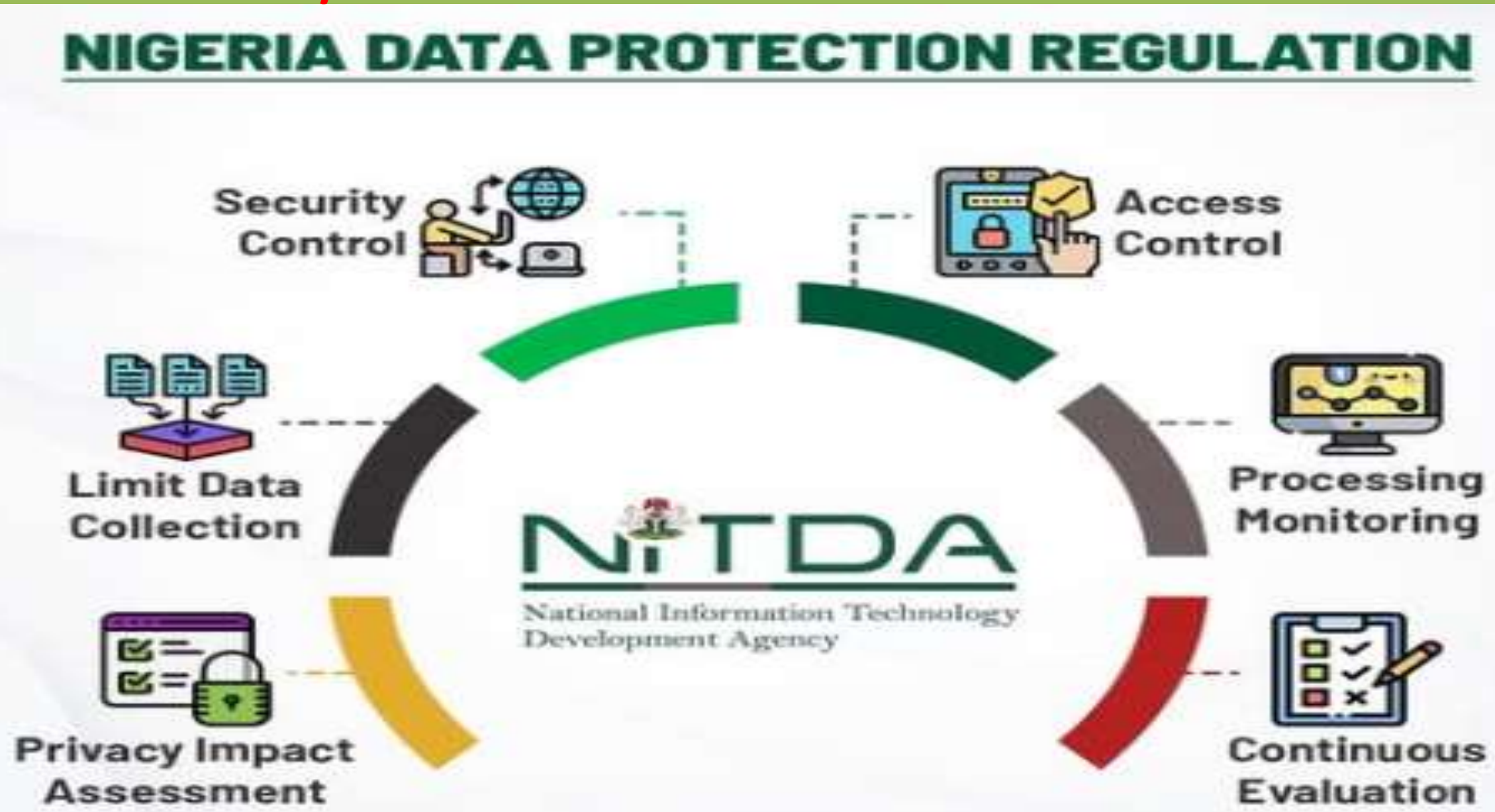
A third party who processes personal data on behalf of the data controller

A data breach occurs when sensitive, confidential, or protected information is accessed, disclosed, or used without authorization.

Examples:
An employee accidentally emails customer banking details to the wrong recipient.

Hackers gain unauthorized access to a company's database and steal customer personal information.

GDPR/NDPR TOOLS FOR DATA BREACH PREVENTION



Major Data Privacy Breaches: Multichoice and Fidelity Bank Fined Heavily

Multichoice:

The Nigeria Data Protection Commission (NDPC) fined Multichoice ₦766,242,500 for illegally transferring Nigerians' personal data across borders and adopting intrusive, unfair, and disproportionate data processing practices, in violation of the Nigeria Data Protection Act (NDPA).

Despite being ordered to implement remedial steps, NDPC found the company's response unsatisfactory and placed all Multichoice data-collection outlets under heightened scrutiny, warning of further severe penalties for continued non-compliance.

Fidelity Bank:

In a separate case, Fidelity Bank Plc was fined ₦555,800,000 by the NDPC in August 2024 for processing customers' personal data without informed consent — including misuse of cookies and mobile banking tools.

The fine, representing 0.1% of the bank's 2023 gross revenue, was increased due to the bank's lack of cooperation and "arrogant disposition" during the investigation. Fidelity Bank disputed the findings, insisting no breach occurred.

Employees' Responsibilities in Handling Personal Data

Collect only necessary data required for transactions and ensure customers are informed about its purpose.

Protect customer data by keeping it secure from unauthorized access, disclosure, or misuse.

Use personal data strictly for transactions and compliance purposes.

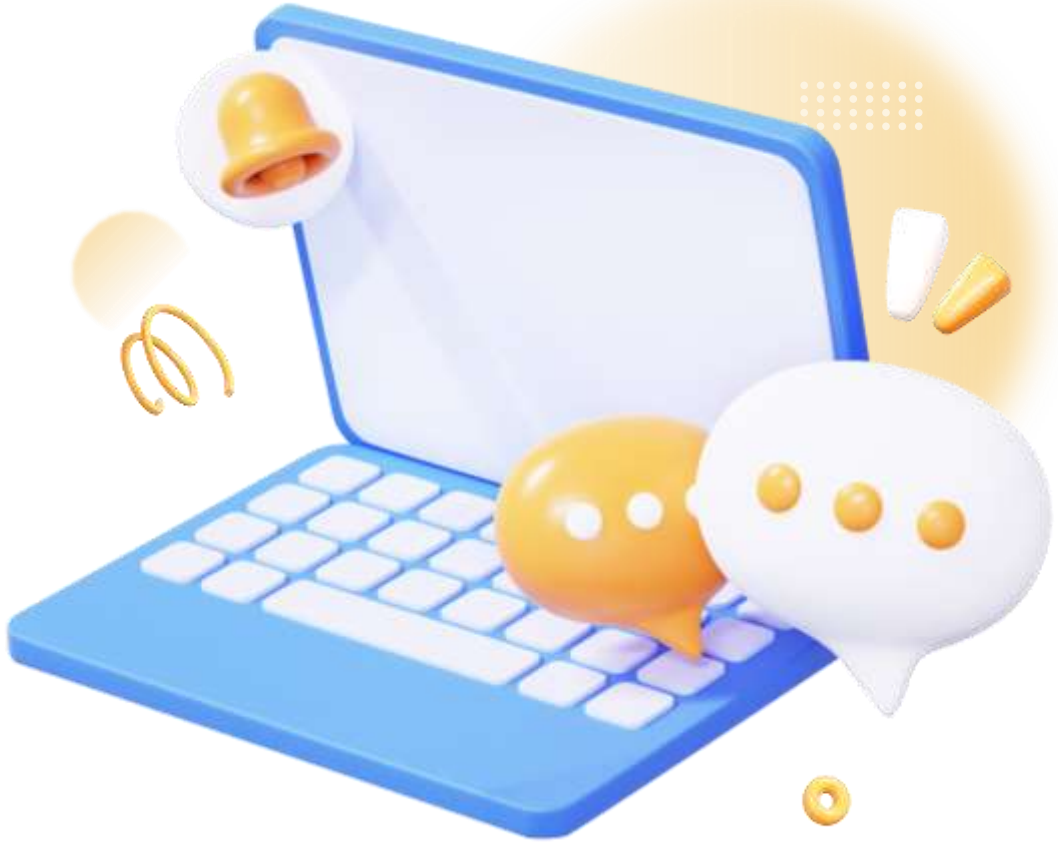
Comply with internal policies and regulations (e.g., GDPR, NDPR, AML/CFT) and participate in regular data protection training.

Respect customer rights by promptly forwarding requests for access, correction, or deletion of data to the compliance or Data Protection Officer.

Report any data breaches or suspicious activity immediately to the appropriate authority within the company.

CONCLUSION

At Olive Monies, protecting personal data is not just about compliance—it is about trust. By handling customer information lawfully, securely, and transparently, we safeguard our customers, meet regulatory expectations, and strengthen our reputation as a reliable international money transfer service.



Thank You