NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 2:
PRINCIPLES OF PERSONAL DATA PROCESSING

Module 2: Overview

In this Module, we will learn about, the:

2.1 Meaning and basis of Personal Data processing

2.2 6 principles of Personal Data processing (6Ps)

2.3 Nature and limitations of "Consent" as a lawful basis for Personal Data processing activities

2.4 NDPR compliance framework

2.1 Meaning + Basis of Personal Data Processing:

2.1.1 Please recall our definition of Personal Data and Personal Data processing in Module 1. We defined Personal Data as: any information relating to a Data Subject and could include information such as: a name; address; photograph; bank details; identification number; location data; an online identifier; the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject; posts on social networking websites; medical information; and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number and others.

2.1.2 Personal Data processing is defined as: any operation, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. To aid our appreciation, we will re-set out these key Personal Data processing activities below:

- 2.1.2.1 Collection
- 2.1.2.2 Recording
- 2.1.2.3 Organisation
- 2.1.2.4 Structuring
- 2.1.2.5 Storage
- 2.1.2.6 Adaptation/Alteration
- 2.1.2.7 Retrieval

2.1.2.8 Consultation

2.1.2.9 Use

2.1.2.10 Disclosure by Transmission

2.1.2.11 Dissemination/Making available

2.1.2.12 Alignment/Combination

2.1.2.13 Restriction

2.1.2.14 Erasure/Deletion

2.1.3 Personal Data processing activities are typically carried out by Data Controllers, Data Administrators or other third-party for the purposes of their business or other reasons personal to them. However, because the Personal Data being processed is legally that of the Data Subject, there is a need to protect the rights of the Data Subject in the course of such Personal Data processing activities.

2.2 6 Principles of Personal Data Processing:

2.2.1 A summary of the 6Ps are:

2.2.1.1 **Lawfulness:**
There must be a lawful basis for any Personal Data processing activity.

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

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

2.2.1.4 **Accuracy:**
Personal Data must be accurate and kept up to date.

Storage:

2.2.1.5 Personal Data must be retained only for as long as necessary.

Security:

2.2.1.6 Personal Data must be processed in a manner as to guarantee its security – confidentiality, integrity and accessibility.

2.2.2 At the centre of each and all of the 6Ps is the concept of "accountability". Accountability in the context of the NDPR simply means that Data Controllers and Data Administrators are accountable to Data Subjects on what they do with the Personal Data that they process. The simple rule is this: anyone who is entrusted with or in possession of the Personal Data of a Data Subject owes a duty of care to the Data Subject. NITDA has made the NDPR to ensure and enforce this concept of accountability.

2.2.3 The duty of accountability extends to a Data Controller or Data Administrator's relationship with anyone who processes Personal Data but cannot be defined as the Data Controller or Data Administrator (Third Party). The Data Controller or Data Administrator must take reasonable measures to ensure that such Third Party does not have a record of violating the general principles of Personal Data processing and that the Third Party is accountable to NITDA or a regulatory authority for data protection within or outside Nigeria.

2.2.4 Every Data Controller or Data Administrator will be liable for the actions or inactions of Third Parties who handle the Personal Data of their Data Subjects. Third parties include directors, shareholders, servants and privies of the third party. The distinction between legal and natural persons is of no relevance in culpability.

2.2.5 We shall now turn to expatiating on each of the 6Ps.

2.2.6 **Lawfulness:**

2.2.6.1 Personal Data must only be processed for a lawful purpose and must be done in a fair and transparent manner. Accordingly, NDPR does not recognise any Personal Data processing that is carried on for an unlawful purpose. For example, NDPR states that no consent should be sought, given or accepted in any circumstance that may promote the direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts [1]

[1]Article 2.4(1) of NDPR

2.2.6.2 Further, lawfulness requires that there must be a lawful basis for any processing activity. Put differently, if there is no lawful basis, the processing activity should not take place. The lawful basis for Personal Data processing could, in no order of importance, be any of the following:

2.2.6.2.1

Consent, that is, the Data Subject has given consent to the processing of his or her Personal Data.[2]

2.2.6.2.2

Contract, that is, the Personal Data processing is necessary for the performance of a contract to which the Data Subject is a party.

2.2.6.2.3

Legal Obligation, that is, the Personal Data processing is required for the performance of a legal obligation to which the Data Controller is subject.

2.2.6.2.4

Legitimate Interest, that is, the Personal Data processing activity is being carried out for the legitimate business interest of the Data Controller.

2.2.6.2.5

Public Interest, that is, the Personal Data processing is necessary for the performance of a task carried out in the public interest or in the exercise of public mandate vested in the Data Controller.

[2]More of the "Consent" concept will be discussed in 2.3 below.

2.2.6.2.6

Vital Interest, that is, the Personal Data processing is necessary for the protection of the vital interest of the Data Subject or another natural person.

2.2.6.3 Fair processing means that the Data Controller must explain to the Data Subject, who the Data Controller is; the purposes for which the Persona Data is being processed; how long the Personal Data will be retained for; who the Personal Data will or may be shared; and explaining the rights of Data Subject, including the right to give, refuse or withdraw consent for the processing activity.

2.2.6.4 The Data Controller and or Data Administrator must be transparent in their communications with the Data Subject.

2.2.7 Specificity:

2.2.7.1 Personal Data must only be collected for specified, explicit and legitimate purposes. Therefore, save the Data Controller's Privacy Policy states otherwise, Personal Data cannot be used for a new purpose if it is incompatible with the original purpose for which the Personal Data was given.

2.2.7.2 The purpose of the Personal Data processing also needs to be explicit. The Data Controller must state and explain to the Data Subject what will happen to each Personal Data collected and what the lawful basis for each processing activity is.[3] As will be seen in Module 3, the Data Subject has the right to consent or refuse consent to each processing activity.

2.2.8 Adequacy:

2.2.8.1 This principle is also known as the Personal Data Minimisation principle. It requires Data Controllers and Data Administrators to ensure that the Personal Data that they process is adequate, relevant and limited to what is necessary for the purpose of processing.

2.2.8.2 Personal Data that is unnecessary, unneeded and goes beyond what is relevant or necessary should not be collected or processed. Personal Data must not be kept on a "just in case" basis. Any collected Personal Data that is surplus to the processing requirement is a breach of this principle and increases the risk of the Data Controller.

[3] Articles 2.1(1)(a) of NDPR

2.2.9 **Accuracy:**

2.2.9.1 Personal Data needs to be accurate and, where required, updated with the accurate information.

2.2.9.2 The use for which the Personal Data is kept will determine the extent of accuracy required. For example, medical Personal Data needs to be updated regularly to avoid a situation where a wrong treatment is given to the Data Subject on account of records containing inaccurate Personal Data.

2.2.9.3 Inaccurate Personal Data should either be updated or deleted.

2.2.10 **Storage:**

2.2.10.1 Personal Data must be stored or retained only for as long as necessary for the purpose for which it was collected.[4]

2.2.10.2 The Data Controller is required to consider the legal or regulatory requirement to retain the Personal Data as well as its legitimate business reasons for retaining the Personal Data.

2.2.9.3 It is typically expected that Data Controllers have a data retention policy. This policy, among other things should contain processes for informing the Data Subject on the period for which his Personal Data will be stored. Where this period cannot be ascertained, the criteria used by the Data Controller in determining retention periods must be communicated to the Data Subject.

2.2.11 **Security:**

2.2.11.1 Personal Data must be processed in a manner as to guarantee its confidentiality, integrity and accessibility.

2.2.11.2 The Data Controller has the unassailable duty to secure all Personal Data within its control against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements. The Data Controller must have organisational and technical controls in place to protect Personal Data in its possession from the risks of unauthorised disclosure, hacking, corruption, etc.

2.2.11.3 Personal Data must be processed in a manner appropriate to the maintenance of its security. The Data Controller must comply with the basic minimum standards of information security management.

2.2.11.4 If Personal Data is being processed to provide a service that is no longer required, such Personal Data should be deleted, anonymised or suppressed.

[4] Article 2.1(c) of NDPR

2.2.11.5 Confidentiality ensures that only authorised personnel have access to the relevant Personal Data. Integrity ensures that the Personal Data is accurate at all times. Availability ensures that the Personal Data is readily accessible by the Data Subject and authorised personnel.

2.2.11.6 Organisational roles and responsibilities should clearly be set out by the Data Controller such that information security can easily be demonstrated. There must be appropriate technical and organisational controls in place at each stage of Personal Data processing activities. A Responsible-Accountable-Consulted and Informed (RACI) matrix could be employed to achieve this.

2.2.11.7 A regulator such as NITDA will typically need to be comforted on the controls and processes around access authorisation; the safeguards against corruption and breaches; and the Data Controller or Data Administrator's general approach to security and the implementation of data protection by design.[6]

2.3 Revisiting the Consent Principle:

2.3.1 Consent of the Data Subject means any freely given, specific, informed and unambiguous indication through a statement or a clear affirmative action by the Data Subject that he or she wishes or agrees to the processing of his or her Personal Data.[7] Accordingly and for example, when assessing whether consent is freely given, account will be taken of whether the performance of a contract is not unnecessarily conditional on consent to process Personal Data.

2.3.2 3 types of consent are readily highlightable:

2.3.2.1 **Implied Consent:**	2.3.2.2 **Explicit Consent:**	2.3.2.3 **Opt-out Consent:**
Participating and volunteering of Personal Data in certain conditions can be implied consent.	Subject gives clear, documentable consent; for example, tick a box, sign a form, send an email or sign a paper.	You are in, except you choose to opt out.

2.3.3 To be valid consent under NDPR, the following must co-exist:

[5] Article 2.1(d) of NDPR
[6] See Article 2.6 of NDPR
[7] See Article 1.3(c) of NDPR

2.3.3.1 There must be transparency, that is, there must be an explicit Privacy Policy stating the type of Personal Data collected, how it is processed, who processes it, the security standard in place to protect the Personal Data, etc.

2.3.3.2 Consent cannot be implied, accordingly, silence, pre-ticked boxes or inactivity does not constitute consent.

2.3.3.3 There must be separate consent for separate Personal Data processing activity, accordingly, there should be no bundled consent. An exception to this rule is in the case of further processing of Personal Data for archiving, scientific research, historical research, statistical purposes or public interest purposes. In these instances, additional consent does not need to be obtained after the initial consent of the Data Subject had been obtained.[8]

2.3.4 The Data Subject can request and receive/retrieve the Personal Data he or she gave. The Data Subject can additionally enquire how his or her Personal Data is being used and who has access to it. This obligation requires that Data Controllers keep adequate record of these facts.

2.3.5 Sensitive Personal Data such as race/ethnicity, political affiliation, religious beliefs, trade union membership, biometric details, sexual orientation, health data, etc. require specific and higher standards of consenting. A tick box would not suffice in the processing of Sensitive Personal Data.

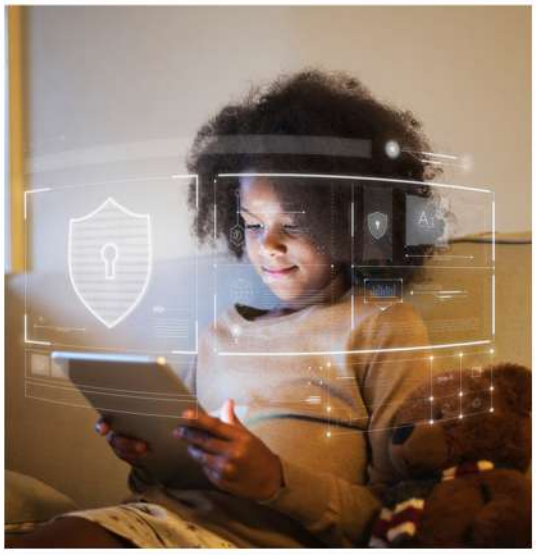
2.3.6 Explicit consent from the Data Dubject is one way of legitimising the processing activity on Sensitive Personal Data. Where however Sensitive Personal Data needs to be processed and explicit consent cannot be obtained, other lawful basis for processing activity can be invoked. For example, legitimate interest or legal obligation; that is, where the processing activity is necessary to fulfil the legal obligations of the Data Controller or Data Subject. Sensitive Personal Data may also be processed to protect the vital interest of an individual or public interest. Processing activity may in this wise, be carried out by a foundation or not-for-profit organisation, such as a religious group or political party.

2.3.7 Personal Data that has been made public by the Data Subject, for example, by the Data Subject publishing it on social media, will not require the consent of the Data Subject before the Personal Data can be processed only if it can be justified that one of the grounds for processing is for lawful reasons, public interest or other reasons among the legal basis .

[8] Article 2.1 (1)(a) of NDPR

2.3.8 Due to the high risk of Sensitive Personal Data, appropriate risk assessments (for example by way of a data protection impact assessment (DPIA) should be carried out before undertaking any processing activity on them. Data Controllers and Data Administrators need to implement a higher level of control to safeguard Sensitive Personal Data than they would for ordinary Personal Data.

2.3.9 NDPR applies to processing activities on the Personal Data of minors or children as their consent is similarly required. However, and unlike the GDPR that generally defines minors or children for its general purposes as anyone under 16 years old, NDPR is silent on the qualification for minors or children. Further and unlike the GDPR that provides extensively for how minors and children's consent is to be obtained from persons who hold parental responsibility over them, NDPR is silent on this requirement.



2.3.10 It is instructive to always remember the following:

2.3.10.1 No Personal Data should be obtained except the specific purpose of collection is made known to the Data Subject.

2.3.10.2 The Data Controller is under an obligation to ensure that the consent of the Data Subject has been obtained without fraud, coercion or undue influence.

2.3.10.3 The Data Controller must be able to demonstrate that the Data Subject has consented to the processing of his or her Personal Data and that the Data Subject had the legal capacity to give the consent at the time he or she did.

2.3.10.4 Where the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent should be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

2.3.10.5 Prior to giving consent, the Data Subject should be informed of his rights and the method to withdraw his consent at any given time. The withdrawal of consent shall not affect the lawfulness of the previous processing activities carried out on the basis of initial consent.

[9] Article 8 of the GDPR. Each Member State of the European Union is at liberty to revise down this definition.

2.3.10.6 Where Personal Data may be transferred to a third party for any reason whatsoever, the Data Controller must ensure that the Data Subject can withdraw his or her consent in the same manner in which he or she gave the consent. For example, where consent was given through an online tick box, then the Data Controller must ensure the Data Subject can also untick same box to revoke/withdraw his or her consent.

2.3.10.7 Online tick boxes are still valid forms of consent. There must be some affirmative action to demonstrate consent; accordingly, inaction will not suffice. Pre-ticked boxes are also not valid.

2.3.11 In the circumstance that the Data Subject can withdraw his or her consent at any time, consent is sometimes considered the weakest of the lawful basis for Personal Data processing activities. Accordingly, it is advisable that consent should not be relied upon as the sole basis for Personal Data processing activities.

2.4 NDPR Compliance Framework:

2.4.1 One of NDPR's novelty is its compliance structure. It creates a nouveau class of professionals known as Data Protection Officers (DPO) and Data Protection Compliance Organizations (DPCO).

2.4.2 A Data Controller may designate one of its personnel, who must be based in Nigeria,[11] as its DPO or outsource the function. The DPO's role is to ensure that the Data Controller adheres to the NDPR and the Data Controller's own Personal Data privacy instruments and directives. [11]

2.4.3 The NDPR Implementation Framework document (currently under discussion) requires a Data Controller to appoint a DPO in any of the following instances, that is, where the:

2.4.3.1 Data Controller is a Government organ, Ministry, Department, Institution or Agency;

2.4.3.2 core activities of the Data Controller relate to usual processing of large sets of Personal Data;

2.4.3.3 Data Controller processes Sensitive Personal Data in the regular course of its business; and

2.4.3.4 Data Controller processes critical national databases consisting of Personal Data.

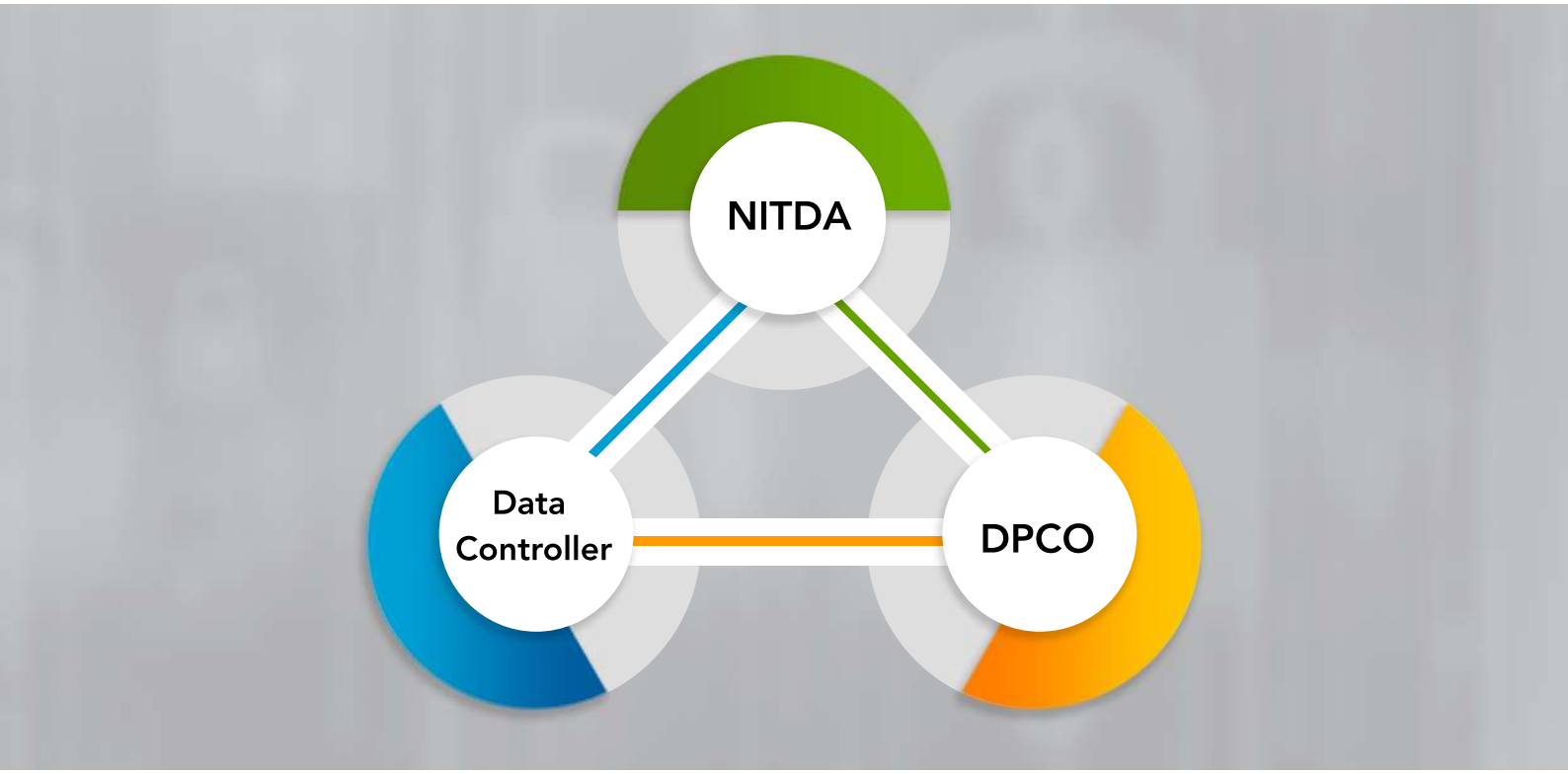
2.4.4 The Data Controller or Data Administrator is to ensure continuous capacity building for its DPO and all its other personnel that are involved in any form of Personal Data processing. [12]

2.4.5 While the Data Controllers or Data Administrators that mandatorily require a DPO are stated by NDPR, all Data Controllers or Data Administrators require a DPCO.

2.4.6 A DPCO is any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with NDPR or any foreign data protection law or regulation having effect in Nigeria.[13] A Data Controller or Data Administrator requires a DPCO for the purpose of ensuring adherence to the NDPR, relevant data privacy instruments and the Personal Data protection policies of the Data Controller or Data Administrator.

2.4.7 DPCOs are subject to the NDPR and other NITDA regulations and directives that are to be periodically issued. [14]

2.4.8 The DPCO framework is a strategic approach to NDPR's enforcement as it considers the Nigerian context and promotes enforcement in a non-obstructive, compliance promoting approach. NDPR uses a triangular compliance model.



[10] See Article 4.2 of NDPR

[11] See Article 1.3 of the NDPR

[12] Article 3.1.4 of the NDPR

2.4.9 A DPCO may be any of a professional services consultancy firm, information technology service provider, audit firm or law firm. The organisation is required to demonstrate some experience or certification in any of the following areas of knowledge: data science, data protection and privacy, information privacy, information audit, data management, information security, data protection legal services, information technology due diligence, European Union (EU) General Data Protection Regulation (GDPR) implementation and compliance, cyber security and cyber security law, data analytics and data governance.

2.4.10 DPCOs are licensed to provide services including:

2.4.10.1 Data protection regulations compliance and breach services for Data Controllers and Data Administrators.

2.4.10.2 Data protection and privacy advisory services

2.4.10.3 Data protection training and awareness services

2.4.10.4 Data regulation contracts drafting and advisory

2.4.10.5 Data protection and privacy breach remediation planning and support services

2.4.10.6 Information privacy audit

2.4.10.7 Data privacy breach impact assessment

2.4.10.8 Data protection and privacy due diligence/investigation

2.4.10.9 Outsourced DPO

2.5 Definitions of Common Terms in Module 2:

We set out below, a glossary of the new terms and abbreviations used in this Module:

	Term	Meaning
2.5.	6Ps	All of the principles of Lawfulness, Specificity, Adequacy, Accuracy, Storage and Security.
2.5.2	DPCO	Data Protection Compliance Organisation
2.5.3	DPIA	Data Protection Impact Assessment is a risk assessment advised to be carried out by a Data Controller or Data Administrator that processes Sensitive Personal Data.

	Term	Meaning
2.5.4	DPO	Data Protection Officer
2.5.5	EU	European Union
2.5.6	GDPR	EU's General Data Protection Regulation which came in force on May 25, 2018
2.5.7	Lawful Basis	The lawful basis for any Personal Data processing activity. They are (in no order of importance): Consent, Contract, Legal Obligation, Legitimate Interest, Public Interest and Vital Interest.
2.5.8	RACI	The Responsible-Accountable-Consulted-Informed matrix which a Data Controller or Data Administrator could use to define organisational roles and responsibilities in demonstrating the security processes of its Personal Data processing activities. Security is one of the 6Ps.
2.5.9	Third Party	A person or entity that is not the Data Controller or Data Administrator but by virtue of his/her/its relationship with the Data Controller or Data Administrator, it processes or has access to the Personal Data of the Data Subjects of Data Controller or Data Administrator.

2.6 Module 2: Summary

2.6.1 Personal Data processing includes each and every act of the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction of Personal Data.

2.6.2 The 6 mandatory principles of Personal Data processing are: Lawfulness, Specificity, Adequacy, Accuracy, Storage and Security. The concept of accountability underlies all 6Ps as NDPR holds the Data Controller and Data Administrator responsible for every Personal Data that they process.

2.6.3 The Data Subject's consent must be freely given, specific, informed and unambiguously indicate through a statement or a clear affirmative action that he or she wishes or agrees that his or Personal Data should be processed. This consent can also be freely withdrawn, hence making consent not a guaranteed lawful basis for Personal Data processing.

2.6.4 The Data Subject, Data Controller, Data Administrator, NITDA, DPCO and DPO are at the heart of the NDPR compliance framework.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[15]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007 [16]

[15]Available at: ndpracademy.ng/resources/Nigeria Data Protection Regulation.pdf

[16]Available at: ndpracademy.ng/resources/NITDA-act-2007.pdf