NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 1:
INTRODUCTION TO NIGERIA PRIVACY RIGHTS LAW

Module 1: Overview

In this Module, we will learn about, the:

1.1 basis of and conversations on Nigeria's privacy rights laws;

1.2 structure of the 2019 Nigerian Data Protection Regulations (**NDPR**); and

1.3 material and territorial scope of the NDPR.

1.1 The Basis of Nigeria's Privacy Rights Laws:

1.1.1 Nigerian Law is sourced from the following 5 major sources:

1.1.1.1 1999 Constitution of the Federal Republic of Nigeria (the Constitution);

1.1.1.2 Nigerian legislations;

1.1.1.3 Judicial decisions;

1.1.1.4 Received English Law – comprised of the Common Laws of England, the Doctrines of Equity and the Statutes of General Application that were in force in England on January 1, 1900; and

1.1.1.5 Customary and Islamic laws.

1.1.2 Of the above 5, only the first 4 have developed laws or rules on privacy rights in the context in which privacy rights is globally recognised.

1.1.3 The Constitution guarantees the privacy rights of Nigerian citizens. It states that: The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic, communications is hereby guaranteed and protected.[1] This right is however not absolute as the same Constitution states that the guaranteed privacy right can be infringed upon by any other law made

i in the public interest on matters of defence, safety, order, morality or health;

ii for protecting the rights and freedom of other persons.[2]

1.1.4 The National Information Technology Development Agency (NITDA) Act, 2007 has become a major Nigerian legislation on privacy rights law in light of the NDPR. NITDA's function includes the development of guidelines for electronic governance and monitoring the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information. [3]

1.1.5 The NDPR is a January 25, 2019 regulation of NITDA. Its preamble references NITDA's function to develop regulations for electronic governance and generally monitor electronic communications. Accordingly, it has been argued if NITDA can regulate privacy rights in general, given the limitation of its functions to electronic communications. It is noteworthy however that NITDA itself was established to implement Nigeria's National Information Technology Policy of 2000 where Strategy 13.3(ii) created the mandate of ensuring the protection of individual and collective privacy, security, and confidentiality of information.

[1] Section 37 of the Constitution.

[2] Section 45 of the Constitution.

[3] Section 6(c) of the NITDA Act.

1.1.6 NDPR has 4 main objectives which are, to:

1.1.6.1 safeguard the rights of Data Subjects to the privacy of their Personal Data;

1.1.6.2 foster safe conduct for transactions involving the exchange of Personal Data;

1.1.6.3 prevent manipulation of Personal Data; and

1.1.6.4 ensure that Nigerian businesses remain competitive in international trade through the best practice safeguards afforded by NDPR.

1.1.7 The only post-NDPR judicial decision was in **Paradigm Initiative for Information Technology v. Nigerian Identity Management Commission (NIMC).**[4] The FHC was called to decide whether NIMC had the right to collect personal data without adequate security and regulatory framework to guide the process. The FHC took judicial notice of the NDPR and dismissed the case on the basis that the issues complained of by the Plaintiff had been addressed with the making of the NDPR. In the absence of any other judicial pronouncement, it is currently safe to conclude that Nigerian Law recognizes the NITDA Act and NDPR as the relevant legal regime for Personal Data protection and processing activities in Nigeria.

1.2 Structure of NDPR:

1.2.1 NDPR is divided into the preamble and 4 parts. The parts must be read in conjunction with the preamble in order to fully understand what the NDPR requires.

1.2.2 Part 1 states NDPR's objectives, scope and defines its special terminologies and abbreviations.

[4] Unreported Decision of the Federal High Court of Nigeria (FHC) in Suit No. FHC/ABJ/CS/58/2019 delivered Hon. Justice Ijeoma L. Ojukwu on Friday, 28th day of June, 2019.

1.2.3 Part 2 deals with the principles of lawful data processing and obtaining consent. It goes further to highlight the how and why of privacy policies, data security and third-party data processing contracts. Other subjects include, Data Subject objections, penalties for defaults and foreign transfers of Personal Data.

1.2.4 Part 3 is exclusive to the rights of Data Subjects.

1.2.5 Part 4 details the mechanisms for the implementation of NDPR, the Administrative Redress Panel (ARP) for dealing with complaints and breaches; and the local and international cooperation required for the implementation of NDPR.

1.3 NDPR's Material and Territorial Scope:

1.3.1 NDPR has a limited scope. It seeks only to protect the Personal Data of Data Subjects.

1.3.2 A Data Subject is an identified or identifiable natural person who:

(i) is a Nigerian citizen, regardless of where he or she lives; or

(ii) lives in Nigeria, regardless of his or her nationality.

Accordingly, NDPR regulates the processing of the Personal Data of these Data Subjects, regardless of where the Personal Data processing activities take place.

1.3.3 A natural person must be identifiable by his or her Personal Data. In other words, by the nature of the Personal Data, the Data Subject must easily be identified or identifiable, whether directly or indirectly. Accordingly, Personal Data 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.[5]

[5] See the definition section of the NDPR.

[6] Ibid.

1.3.4 Included the above samples of Personal Data are a special category of Personal Data known as Sensitive Personal Data. They are Personal Data relating to religious or other beliefs, sexual orientation, health or biometrics, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.[6]

1.3.5 A natural person is a living individual, accordingly, NDPR's scope does not extend to the protection of the data of artificial persons (for example, corporates) or a non-living human person. NDPR does not protect the Personal Data of a dead person, with the exception of the deceased person's estate where the Personal Data relates to a Data Subject such as a beneficiary of the estate.

1.3.6 NDPR promotes the Data Subject's rights to the ownership and control of his or her Personal Data. This rights particularly become relevant when the Personal Data is being processed by Data Controllers or Data Administrators. Since data processing is carried out on an increasingly global scale, it is important that Data Subjects understand their rights to and control of their Personal Data.

1.3.7 NDPR applies to all Personal Data processing transactions notwithstanding the means by which the Personal Data processing is being conducted or intended to be conducted.

1.3.8 NDPR will not deny any Nigerian citizen or any foreigner living in Nigeria, the other privacy rights that they may be entitled to under any law, regulation, policy or contract for the time being in force in Nigeria or in any foreign jurisdiction. Accordingly, any Nigerian citizen or any foreigner living in Nigeria, can in addition to the NDPR, enforce any of their other privacy rights.

1.3.9 NDPR regulates all Data Controllers or Data Administrators whose main establishment, typically their headquarters, is located in Nigeria. This regardless of where the actual Personal Data processing activities take place. Accordingly, a Data Controller or Data Administrator that outsources its Personal Data processing activity outside Nigeria is still subject to NDPR.

1.3.10 NDPR regulates any Personal Data processing activity on goods or services, regardless of payment or consideration. Accordingly, marketing and data sharing activities are as subject to NDPR as direct sales is.

1.3.11 Processing activities that monitor Data Subjects' behaviour are similarly regulated by NDPR. Accordingly, organisations that employ cookies on their websites will have to review their grounds for doing so in relation to Data Subjects under the NDPR.

1.4 Definitions of Common Terms in Module 1:

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

	Term	Meaning
1.4.1	Data Administrator	An organisation or individual that processes Personal Data, usually at the instance of the Data Controller.
1.4.2	Data Controller	An organisation or individual who determines the purposes for and the manner in which Personal Data is processed or to be processed.
1.4.3	Data Subject	This is an identified or identifiable natural person who: (i) is a Nigerian citizen, regardless of where he or she lives; or (ii) lives in Nigeria, regardless of his or her nationality
1.4.4	GSM	Global System for Mobile Communication.
1.4.5	IMEI Address	International mobile equipment identity, usually 15 or 17 digits, that identifies the user of a mobile phone.
1.4.6	IMSI Address	International mobile subscriber identity, usually of 15 digits, assigned to GSM, UMTS or LTE subscribers.
1.4.7	IP Address	Internet protocol address that is assigned to each device that is connected to a computer network.
1.4.8	MAC Address	Media access control address assigned to a network interface controller.

	Term	Meaning
1.4.9	NDPR	Nigeria's 2019 Data Protection Regulation which came in force on January 25, 2019.
1.4.10	Nigeria	The Federal Republic of Nigeria
1.4.11	Nigerian Law	The sum of all the laws that are in force in Nigeria.
1.4.12	NITDA	Nigeria's National Information Technology Development Agency.
1.4.13	Personal Data	This is the heart of NDPR. It means 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.
1.4.14	Personal Data Processing	This refers to any operation on Personal Data, 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.
1.4.15	Sensitive Personal Data	They are Personal Data relating to religious or other beliefs, sexual orientation, health or biometrics, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.
1.4.16	UMTS	Universal Mobile Telecommunications Service.

1.5 Module 1: Summary

1.5.1 The NITDA Act and NDPR are currently the legal basis of privacy rights conversation in Nigeria.

1.5.2 NDPR is divided into the following 4 parts and subject matters:

1.5.2.1 Part 1 – NDPR objectives, scope and definitions

1.5.2.2 Part 2 – Personal Data processing principles

1.5.2.3 Part 3 – Rights of Data Subjects

1.5.2.4 Part 4 – Implementation and remedies

1.5.3 NDPR's material and territorial scope extends to:

1.5.3.1 all Nigerian citizens in whatever jurisdiction they live;

1.5.3.2 all living natural persons that live in Nigeria;

1.5.3.3 all Personal Data processing activities carried out by all Data Controllers and Data Administrators situated in Nigeria regardless of the jurisdiction where the processing activity takes place

Further Reading:

1. Sections 37 and 45 of the Constitution of the Federal Republic of Nigeria, 1999.
2. 2019 Nigeria Data Protection Regulation[7]
3. National Information Technology Development Act 2007[8]
4. **Paradigm Initiative for Information Technology v. Nigerian Identity Management Commission (NIMC)**

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

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

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, and because the Personal Data being processed is legally that of the Data Subject, there is 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 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 lawful purpose 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 not to give consent or withdraw consent from 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 B if it is incompatible with the original purpose A for which the Personal Data was given.

2.2.7.1 The purposes of the Personal Data processing also need 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 the 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) and 3.1(7)(c) 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 if the inaccurate Personal Data.

2.2.9.2 Inaccurate Personal Data should either be updated or deleted.

2.2.10 **Storage:**

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

2.2.9.10.2 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.

2.2.9.10.3 It is typically expected that Data Controllers have a data retention policy

2.2.11 **Security:**

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

2.2.9.11.2 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.

2.2.9.11.3 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.

2.2.9.11.4 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

2.2.9.11.5 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.

2.2.9.11.6 Organisational roles and responsibilities should clearly be set out in 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.

2.2.9.11.7 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(iii) 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.

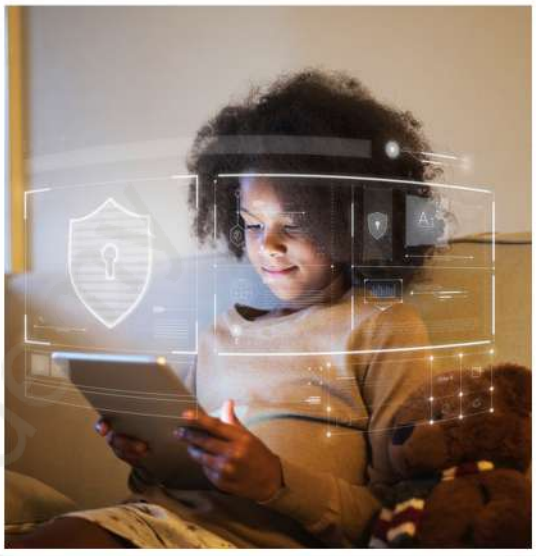
2.3.6 Explicit consent from the Data Dubject is one way of legitimising the processing activity on Sensitive Personal Data. Where however Sensitive Personal Data needs to be processed and explicit consent cannot be obtained, other lawful basis for processing activity can be invoked. For example, legitimate 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 and 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 relates 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.

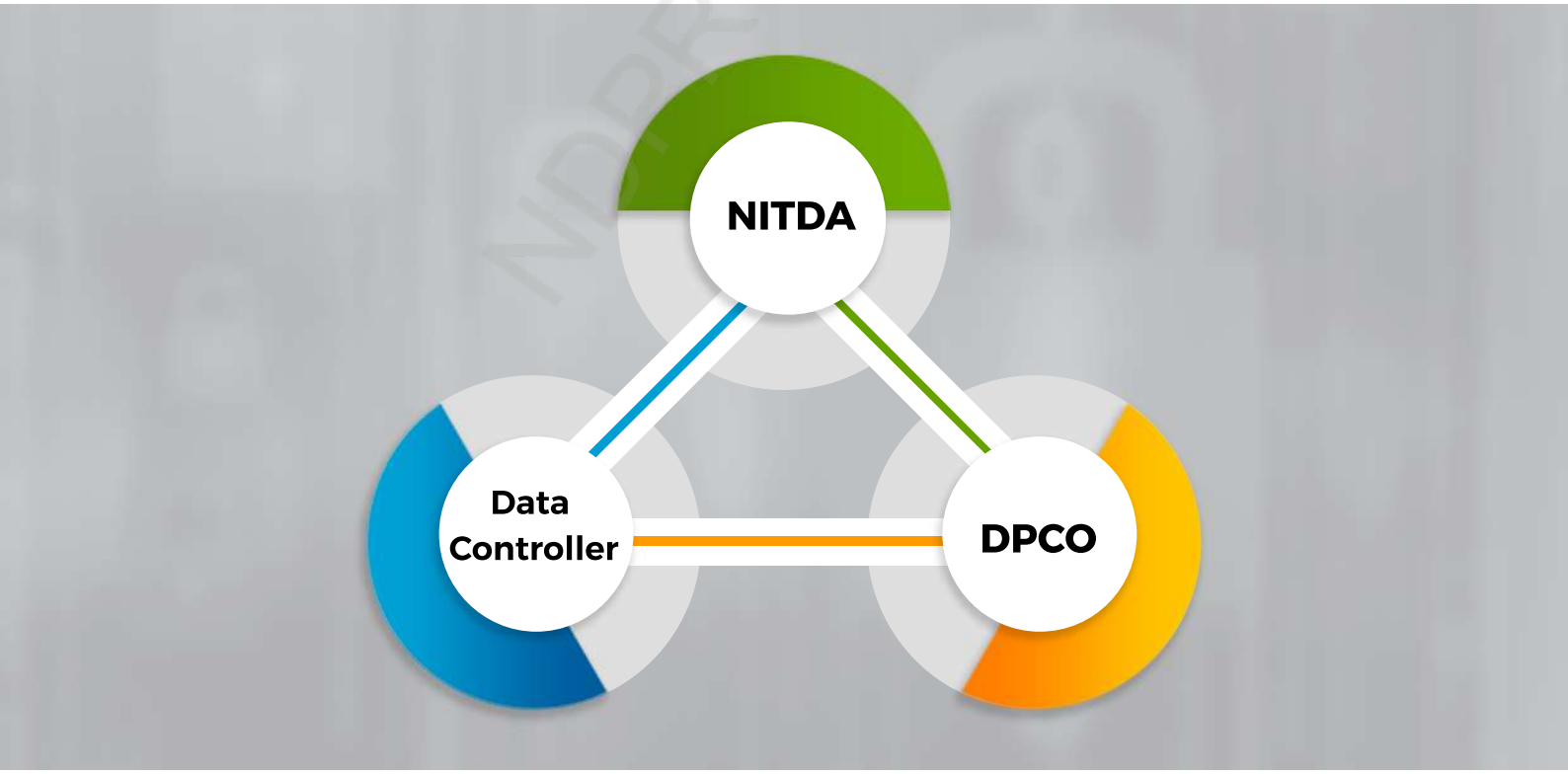
2.4.4 The Data Controller or Data Administrator is to ensure continuous capacity building for its DPO and all its other personnel that are involved in any form of Personal Data processing. [12]

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 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 NDPR
[12] Article 4.1(4) of 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
2.5.1	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 be used 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.

2.6.3 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

NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 3:
RIGHTS OF DATA SUBJECTS

Module 3: Overview

In this Module, we will learn about each of the 8 rights of Data Subjects, which are, the:

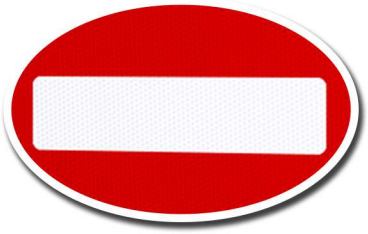
3.1 Right to be Informed

3.2 Right of Consent

3.3 Right of Access

3.4 Right to Object

3.5 Right of Rectification



3.6 Right to Restrict Processing

3.7 Right of Personal Data Portability

3.8 Right to be Forgotten

3.1 The Right to be Informed:

3.1.1 The Data Controller or Data Administrator must prior to collecting Personal Data, provide certain information to the Data Subject.[1] This information should be contained in a Privacy Policy that must be conspicuously included in the medium by which the Personal Data is being collected.[2]

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

3.1.3 The Privacy Notice must, among other information, state:

3.1.3.1 All the rights of the Data Subject, that is, the rights to consent, access, object, be forgotten, rectification, restrict processing and Personal Data portability.[3]

3.1.3.2 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;[4]

3.1.3.3 The technical methods used to collect and store Personal Data, for example, cookies, JWT, web tokens et.al.;[5]

3.1.3.4 The identity and contact details of the Data Controller and its representative(s);[6]

3.1.3.5 Where there is one, the DPO's contact details;[7]

[1] Article 3.1(7) of NDPR
[2] Article 2.5 of NDPR
[3] Articles 2.5(a) and 3.1(7)(i) and (h) of NDPR
[4] Articles 2.5(c)(f) and 3.1(7)(c)(d)(k) and (m) of NDPR
[5] Article 2.5(d) of NDPR
[6] Article 3.1(7)(a) of NDPR
[7] Article 3.1(7)(b) of NDPR

3.1.3.6 Any further recipients of the Personal Data, that is, if it is to be shared or passed on to anyone else, for example, a Data Administrator; [8]

3.1.3.7 How long the Personal Data will be stored for; [9]

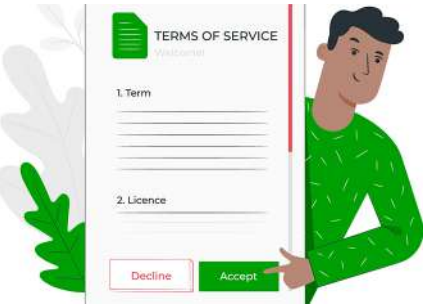
3.1.3.8 The details of the supervisory authority, for example NITDA, to lodge complaints with if the Data Subject's rights are infringed; [10]

3.1.3.9 The available remedies in the event of violation of the Privacy Policy and the time frame for the remedies; [11]

3.1.3.10 Where decision-making is automated, for example, by way of profiling, the processing activity must be explained and the likely impact it will have on the Data Subject; [12] and

3.1.3.11 Where applicable, that the Data Controller intends to transfer [13] the Personal Data to a foreign country or international organization and the existence or otherwise of an Adequacy Decision [14] by NITDA in respect of that foreign country or international organization; [15]

3.1.4 It should be clear how this practice supports the principle of lawful fair and transparent processing as discussed in Module 2 in the circumstance that it gives Data Subjects greater oversight of their Personal Data that is the possession of Data Controllers and Data Administrators.



3.2. The Right of Consent:

3.2.1 Data Subjects have a right to consent to the processing of their Personal Data. [16] In this regard, where there is no other lawful basis for a processing activity, the Data Controller must must expressly request for the consent of the Data Subject before subjecting the Personal Data to any processing activity.

[8] Articles 2.5(e) and 3.1(7)(e) of NDPR
[9] Article 3.1(7)(g) of NDPR
[10] Articles 2.5(g) and 3.1(7)(j) of NDPR
[11] Article 2.5(g)(h) of NDPR
[12] Article 3.1(7)(l) of NDPR
[13] We shall discuss local and international transfers of Personal Data in detail in Module 5.
[14] An Adequacy Decision is a decision taken by NITDA, either by itself or in conjunction with the office of the Attorney-General of the Federation that a country, jurisdiction or international organization has an adequate level of Personal Data protection in place.

3.2.2 The right to consent also includes the right to withdraw consent at anytime. Accordingly, before obtaining the consent of the Data Subject, the Data Controller must expressly let the Data Subject know of his ability to withdraw same consent at any time.[17]

3.2.3 It is the Data Controller's responsibility to ensure that the Data Subject has legal capacity to give consent. Specifically, the Data controller must be able to show that the Data Subject has validly given his or her consent.

3.2.4 As explained while the discussing the right to be informed, the Data Controller must inform the Data Subject in the Privacy Notice of the Data Subject's right to consent and or withdraw consent.[18]

3.3 The Right of Access:

3.3.1 Data Subjects have the right to access or retrieve from the Data Controller the Personal Data they provided to a Data Controller. The Personal Data must be provided by the Data Controller to the Data Subject in a structured and commonly used format.[19]

3.3.2 Given this responsibility on the Data Controller, it is advisable that the Data Controller have in place, a data inventory which easily identifies where all Personal Data is located as to guarantee easy retrieval. Such a system should reduce the effort required to respond to a Data Subject's access request, commonly referred to as DSAR.

3.3.3 NDPR requires that a Data Controller have in place appropriate measures to ensure the processing of Personal Data in a concise, transparent, intelligible and easily accessible form.[20] Accordingly, a Data Controller should have a good DSAR response mechanism in place. A good DSAR system would ensure that Data Subjects can easily request for their Personal Data under a formal process.

[15] Article 3.1(7)(f)(n) and 3.1(8) of NDPR
[16] Article 1.3 (xiv) of NDPR
[17] Article 2.3.2(c) of the NDPR
[18] Article 2.3(2) of the NDPR
[19] Regulations 3.1 (15) of the NDPR
[20] Article 3.1(1) of NDPR

3.3.4 NDPR requires that DSARs have to be responded to within one month of receipt the DSAR.[21] Such response includes acceding to the Data Subject's request or give reasons why the request may not be attended to and or informing the Data Subject of his or prerogative to lodge a complaint with NITDA in the event the Data Subject does not agree with the reasons given by the Data Controller

3.3.5 Unless NITDA states otherwise, Data Controller cannot charge the Data Subject for responding to a DSAR.[22] NDPR however recognizes the possibility of vexatious, excessive and or repetitive requests. In such instances, the Data Controller is allowed to charge a reasonable fee commensurate to its administrative costs for providing the Data Subject with the required information. Alternatively, the Data Controller can write the Data Subject, stating its refusal to act on the DSAR. Such a letter should be copied to NITDA.[23] The Data Controller has the burden of showing that the Data Subject's DSAR is unfounded or excessive.[24]

3.3.6 DSARs are required to be responded to in writing, including electronically, in structured, concise, commonly-used, transparent, intelligible and machine-readable format using clear and plain language.[25] This is particularly important where the Data Subject is a child. The DSAR can be responded to orally at the request of the Data Subject.[26]

3.3.7 The Data Controller has the responsibility of satisfying itself of the identity of the Data Subject before responding to a DSAR. In this case, the Data Controller will be within its right to request the Data Subject to provide such additional information as the Data Controller may require to satisfy itself of the Data Subject's identity.[27] The identity of the Data Subject should not be proven only by oral communication.[28]

[21] Article 3.1(2) of NDPR
[22] Article 3.1(3) of NDPR
[23] Article 3.1(3)(a) and (b) of NDPR
[24] Article 3.1(4) of NDPR
[25] Article 3.1(14) of NDPR
[26] Article 3.1(1) of NDPR
[27] Article 3.1(5) of NDPR
[28] Article 3.1(1) of NDPR

3.4 The Right to Object:

3.4.1 Data Subjects generally have a right to object to the Data Controller undertaking processing activities on their Personal Data. Data Controllers are mandated to provide Data Subjects with a medium or mechanism for objecting to any form of processing activity.[29]

3.4.2 Generally, where a Data Subject objects to a processing activity on his or her Personal Data, the Data Subject may do any of the following:

3.4.2.1 Request the Data Controller to rectify any error on the Personal Data;

3.4.2.2 Restrict the Data Controller from carrying out any further processing activity on the Personal Data;

3.4.2.3 Request the Data Controller to transfer the Personal Data to another Data Controller; or

3.4.2.4 Request the Data Controller to delete the Personal Data.

3.4.3 The instances where a Data Subject can object to processing activity being carried out on his or her Personal Data are discussed in the succeeding paragraphs.

3.4.4 The Data Subject has the right to object to a Data Controller using his or her Personal Data for marketing purposes.[30] It is assumed that the lawful basis for a Data Controller to process Personal Data for marketing purposes will be the consent of the Data Subject, in which case, the Data Controller should stop the relevant processing activity as soon as it receives the Data Subject's objection. Precisely, the Data Controller should delete the Personal Data,[31] in the circumstance that the Data Subject has withdrawn his or her consent.

[29] Article 2.8(b) of NDPR

[30] Article 2.8(a) of NDPR

[31] Article 3.1(9)(c) of NDPR

3.4.5 Until a resolution of their contentions, a Data Controller must restrict itself from any further processing activity where the Data Subject objects to the processing, while the Data Controller seeks to rely on its legitimate interest as the basis for its processing activity.[32]

3.4.6 NDPR addresses the right of Data Subjects to object to the automated processing of their Personal Data. Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling. This explains the NDPR states emphatically that before collection of information, information about automated decision making and profiling must have been given to the Data Subject, as well as the necessary safeguards.[33]

3.4.7 There are limited instances where the Data Controller can continue its processing activity, in spite of the Data Subject's objection expressed in the form of a restriction on processing activities. These limited instances include where the Data Controller requires the processing activity for:

1. Establishing, exercising or defending legal claims;
2. Protection of the rights of another natural or legal person; or
3. Reasons of important public interest in Nigeria; [34]
4. In the case of automated processing, where the processing is based on explicit consent.

3.4.8 With the exception of processing activities such as marketing, the Data Subject's right to object to the processing of his or her Personal Data is not an absolute right and may in most cases be overridden by other lawful basis of processing such as: contract, legal obligation, legitimate interest, public interest and vital interest.

[32] Article 3.1(11)(d)
[33] Article 3.1 (7L)
[34] Article 3.1(12)

3.5 The Right to Rectification:

3.5.1 The right to rectification may typically follow the Data Subject's exercise of his or her right to object to a processing activity on the ground that the Personal Data with the Data Controller requires updating.[35]

3.5.2 Where a Data Subject changes his or her name or address, the Personal Data held by a Data Controller may no longer be accurate or incomplete. The Data Subject has a right to request that his or her Personal Data be updated and be made accurate or complete.

3.5.3 A Data Controller may protect this by having some sort of customer preference centre or portal that allows Data Subjects to manage their own personal information and update it as appropriate.

3.5 The Right to Rectification:

3.6.1 Data Subjects can restrict a Data Controller from processing activities on their Personal Data in the following instances, that is, if the:

3.6.1.1 Data Subject contests the accuracy of the Personal Data;

3.6.1.2 Data Subject believes that his or her Personal Data is being processed unlawfully but does not want the Personal Data erased, then they can instead request that the Data Controller restrict certain elements of its processing activity. For example, Data Subjects may want to restrict Data Controllers from using their Personal Data for direct marketing purposes only;

3.6.1.3 If the Personal Data is no longer needed for the purposes that it was collected but has continued relevance to the exercise of a legal claim; and

[35] Article 3.1(7)(h) of NDPR

3.6.1.4 If a Data Subject claims that the impact on their privacy outweighs the legitimate interests of the Data Controller in processing. In these instances, the Data Subject can again request that the processing activity be restricted while the legitimacy of the processing is being investigated.[36]

3.6.2 The right to restriction gives the Data Subject greater control over their Personal Data and, most importantly, greater transparency over how their Personal Data is being processed.

3.7 The Right to Personal Data Portability:

3.7.1 The right to data portability is the right of Data Subjects to have their Personal Data transmitted from one Data Controller to another without any form of let or hinderance.[37]

3.7.2 Data Subjects have the right to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one environment to another in a safe and secure way, without hindering usability. Data Controllers must provide Data Subjects with a copy of their Personal Data in a structured, commonly used and machine-readable format.

3.7.3 The right to portability only applies when, the:

3.7.3.1 Personal Data was provided by the Data Subject;

3.7.3.2 Personal Data is processed by automated means; and

3.7.3.3 Personal Data is being processed based on consent or where it is necessary to fulfil a contract.

3.7.4 Where a Data Subject invokes his or her right to Personal Data portability, the Data Controller must not hinder the transmission of the Personal Data to the new Data Controller.

[36] Article 3.1(11) of NDPR

[37] Article 3.1(15) of the NDPR

3.8 The Right to be Forgotten:

3.8.1 The right to be forgotten is also known as the right of erasure. This right entitles Data Subjects to request Data Controllers or Data Administrators to delete the Data Subject's Personal Data.[38] This right is typically exercised where the:[39]

3.8.1.1 Personal Data is no longer necessary for the purposes for which it was collected; or

3.8.1.2 Data Subject withdraws his or her consent on the processing activity and there is no other lawful basis for processing; or

3.8.1.3 Data Subject objects to the processing and there are no overriding legitimate grounds for processing; or

3.8.1.4 Personal Data has been unlawfully processed; or

3.8.1.5 Personal Data is to be erased for compliance with a legal obligation.

3.8.2 While this right remains controversial to the extent that the technical difficulties of entirely removing a Data Subject's Personal Data might undermine a Data Controller's real ability to fully comply, international case law both upholds this right and offers precedent that, where total erasure is impossible, suppression of the Personal Data may be a suitable alternative. In 2016, the Belgian Court of Cassation[40] ordered a newspaper to anonymise an online version of its 1994 newspaper article concerning a fatal road traffic accident that the applicant had caused through drunk driving. Since he had spent his conviction, the court upheld his right to be forgotten.

[38] Article 3.1(9) of NDPR

[39] Article 3.1(11) of NDPR

[40] Olivier G v. Le Soir (29 April 2016, n° C 15 0052 F). Available at:

3.9 Definitions of Common Terms in Module 3:

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

	Term	Meaning
3.9.1	Adequacy Decision	Adequacy Decision A decision taken by NITDA, either by itself or in conjunction with the office of the Attorney-General of the Federation that a country, jurisdiction or international organization has an adequate level of Personal Data protection in place.
3.9.2	DSAR	Data Subject access request made pursuant to the Data Subject's right of access.
3.9.3	JWT	JSON web token. A compact URL safe means of representing data to be transferred between two parties.
3.9.4	Privacy Policy	A medium through which Data Subjects are to be informed of their rights and other information of the Data Controller in relation to their Personal Data.

3.10 Module 3: Summary

3.10.1 The Data Controller or Data Administrator must prior to collecting Personal Data, correctly and accurately inform the Data Subject vide the Data Controller or Data Administrator's Privacy Policy.

3.10.2 Data Subjects have a right to consent to the processing of their Personal Data as well as withdraw their consent at anytime.

3.10.3 Data Subjects have the right to access or retrieve their Personal Data from Data Controllers in a structured and commonly used format.

3.10.4 Save in exceptional cases, Data Subjects generally have the right to object to Data Controllers undertaking processing activities on their Personal Data.

3.10.5 A Data Subject has the right to request from the Data Controller that his or her Personal Data be updated and be made accurate or complete at anytime.

3.10.6 Data Subjects can generally restrict a Data Controller from undertaking processing activities on their Personal Data in certain instances.

3.10.7 Save in exceptional cases, Data Subjects generally have the right to object to Data Controllers undertaking processing activities on their Personal Data.

3.10.8 A Data Subject has the right to request from the Data Controller that his or her Personal Data be updated and be made accurate or complete at anytime.

3.10.9 Data Subjects can generally restrict a Data Controller from undertaking processing activities on their Personal Data in certain instances.

Further Reading:

1. 2019 Nigeria Data Protection Regulation [41]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007 [42]
4. Olivier G v. Le Soir 29 April 2016, n° C 15 0052 F [43]

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

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

[43] https://wilmap.law.stanford.edu/sites/default/files/2018-02/20160429-Belgian%20Supreme%20Court-RTBF%20case.pdf

NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 4:
OBLIGATIONS OF DATA CONTROLLERS AND ADMINISTRATORS

Module 4: Overview

In this Module, we will learn about, the:

4.1 differences between Data Controllers and Data Administrators; and

4.1 obligations of Data Controllers and Data Administrators

4.1 The Data Controller and the Data Administrator: Differences

4.1.1 We got introduced to the concepts of the Data Controller and the Data Administrator in Module 1. Please recall that we defined the Data Controller as an organisation or individual who determines the purposes for and the manner in which Personal Data is processed or to be processed. The Data Administrator was defined as an organisation or individual that processes Personal Data, usually at the instance of the Data Controller. Given these two separate definitions, we should readily conclude that there are differences between the two roles.

4.1.2 The major difference lies in the Data Controller being the principal of the Personal Data processing activity while the Data Administrator is the agent of the Data Controller.

4.1.3 NDPR places greater obligations on the Data Controller as the Data Administrator, more often than not, carries out its processing activities on the instruction of the Data Controller.

4.1.4 Some other actors in the Personal Data processing space are those we refer to as Third Parties. Do you recall the definition from Module 2? A Third Party is 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, processes or has access to the Personal Data of the Data Subjects of the Data Controller or Data Administrator.

4.1.5 These Third Parties typically do not have contracts or other legally binding relationships with the Data Controller, otherwise they would have been Data Administrators. They usually come into possession of the Personal Data of the Data Subjects by other lawful means. An example of a Third Party could be an auditor of a Data Administrator.

4.1.6 Depending on the context, a Data Aggregator could easily be any of a Data Controller, Data Administrator or Third Party. Data Aggregators are online service providers who create platforms to process Personal Data whether or not collected by themselves. They include search engine platforms, payment or fintech solutions etc.

4.1.7 In **Google Spain SL and Google Inc. v. AEPD (Agencia Espanola de Proteccion de Datos) and Mario Costeja Gonzalez**[1] the Court held that Google by the use of its search engine is a Data Controller in the circumstance that it collects data, including Personal Data stored on the internet, and which data it subsequently retrieves, records, stores and discloses or makes available to its users. It is irrelevant that the search engine undertakes these processing activities in respect of data generally, in as much as it collects Personal Data in the process.

4.2 The Data Controller and the Data Administrator: Obligations

4.2.1 Data Administrators must only process Personal Data according to the documented instructions from the Data Controller. NDPR's standards require the relationship of the Data Controller and Data Administrator to be in writing, in a contractual binding document.

4.2.2 Data Controllers must ensure that there are confidentiality clauses in their contracts with Data Administrators to ensure that the Data Administrators and Third Parties maintain the integrity of the Personal Data that comes into their possession. Concept such as: staff reliability, non-disclosure agreements, training, monitoring, awareness, disciplinary procedures, et. al. must be present in the contracts.

[1](C-131/12), available at:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN

4.2.3 Prior to their execution of a formal contract, the Data Controller needs to establish and be satisfied of the Personal Data security controls and processes that the Data Administrator has in place. The Data Controller must be satisfied with the effectiveness of these security controls. Data Administrators need to be able to assist Data Controllers by taking appropriate technical and organizational measures to protect Personal Data that come into their possession.

4.2.4 The Data Administrator must respect and observe the conditions for Personal Data processing as set out in its contract with the Data Controller. The contract needs to authorize the Data Administrator to undertake the relevant processing activity being undertaken by the Data Administrator or to be undertaken by any Third Party who may act on the Data Administrator's behalf.

4.2.5 Data Controllers need to pay particular attention to the termination clause in their agreements with Data Administrators. Essentially, the termination clause needs to state what the Data Administrator must do with the Personal Data after the completion of the processing activity. Options open to the parties include the Data Administrator securely deleting the Personal Data or returning the Personal Data to the Data Controller.

4.2.6 Data Controllers and Data Administrators will take responsibility for the processing activities of their Third Parties. Data Controllers are required to publish a list of Third Parties with whom Personal Data may be shared. This publication must be included in the audit filing report and must contain:

4.2.6.1 categories of the Third-Party recipients;

4.2.6.2 name of Third Parties;

4.2.6.3 jurisdiction of Third Parties;

4.2.6.4 purpose for sharing Personal Data with Third Parties;

[2]Article 2.7 NDPR

4.2.6.5 nature of Personal Data shared, etc.

4.3 Definitions of Common Terms in Module 3

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

Term	Meaning
Data Aggregator	They are online service providers who create platforms to process Personal Data whether or not collected by themselves. They include search engine platforms, payment or fintech solutions etc.

4.4 Module 4: Summary

4.4.1 Data Administrators often obtain their contractual right to process Personal Data from the Data Controller. The Data Controller is ultimately responsible for the infractions of the Data Administrator by virtue of their principal and agent relationship.

4.4.2 Data Controllers and Data Administrators must ensure that a documented contract is in place between them.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[3]
2. **Google Spain SL and Google Inc. v. AEPD and Mario Costeja Gonzalez**[4]

[3] Available at: ndpracademy.ng/resources/Nigeria Data Protection Regulation.pdf
[4] ***(C-131/12),*** available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN

NDPR Academy® Foundation Course

MODULE 5:
LOCAL AND INTERNATIONAL TRANSFERS OF PERSONAL DATA

Module 5: Overview

In this Module, we will learn about, the:

5.1	5.2	5.3
the requirements for the transfer of Personal Data;	the special requirements for the foreign transfer of Personal Data; and	local and international cooperation on Personal Data protection



5.1 Requirements for Transfer of Personal Data:

5.1.1 Transfer of Personal Data is a Personal Data processing activity. You may recall our definition of Personal Data processing from Module 1 - any operation on Personal Data, 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.

5.1.2 You may also recall the consent principle from Module 2 where we stated that 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.[1] We had also stated that for consent to be valid under NDPR, the following conditions must co-exist:

5.1.2.1 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.

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

5.1.2.3 There must be separate consent for separate Personal Data processing activity, accordingly, there should be no bundled consent. [2]

5.1.3 What all of the foregoing points to is that transfer of Personal Data, often being a separate processing activity, that is, different from the purpose why the Personal Data was collected in the first place, requires the express consent of the Data Subject. Accordingly, NDPR prohibits a Data Controller or Data Administrator from transferring Personal Data to any

[1] Article 1.3(iii) of NDPR.
[2] Article 2.1 (1)(a) of NDPR

5.1.3 person except where the consent of the Data Subject is obtained without fraud, coercion or undue influence.[3] In other words, before undertaking transfer of Personal Data, the Data Controller or Data Administrator should expressly obtain the consent of the Data Subject.

5.1.4 You may need to distinguish between the obligation of the Data Controller or Data Administrator to expressly obtain the consent of the Data Subject prior to transferring the Data Subject's Personal Data, from the right of the Data Subject to Personal Data portability. You may recall from Module 3 that the 7th right of Data Subjects is the right to have their Personal Data transmitted from one Data Controller to another without any form of let or hinderance.[4] While the Data Subject in exercising his or her right to Personal Data portability does not require the consent of the Data Controller or Data Administrator, the Data Controller or Data Administrator on the other hand have an obligation to obtain the express consent of the Data Subject before transferring the relevant Personal Data to anyone.

5.2 Special Requirements for Foreign Transfer of Personal Data:

5.2.1 A foreign transfer of Personal Data (**Foreign Transfer**) is the transfer of Personal Data to a foreign country. A foreign country is any sovereign State, or an autonomous or semiautonomous territory within the international community (**Foreign Country**).[5]

5.2.2 NDPR requires that any transfer of Personal Data to a Foreign Country must be done with the supervision of the Honourable Attorney General of the Federation (**AGF**) and subject to an Adequacy Decision[6] by NITDA.[7]

5.2.3 In arriving at an Adequacy Decision, NITDA shall rely on the AGF's opinion on the legal system of the Foreign Country. The key areas that will be reviewed on the Foreign Country include:

5.2.3.1 its regime on rule of law and respect for human rights and fundamental freedoms;

5.2.3.2 the application of its general and sectoral legislations on Personal Data protection;

5.2.3.3 its indices of public security and defence, national security and criminal law administration;

5.2.3.4 the access of its public authorities to Personal Data;

[3]Articles 2.1 and 2.3(2) of NDPR
[4]Article 3.1(15) of NDPR
[5]Article 1.3 of NDPR
[6]Recall our definition of Adequacy Decision in Module 3 – a decision taken by NITDA, either by itself or in conjunction with the office of the AGF that a country, jurisdiction or international organization has an adequate level of Personal Data protection in place
[7]Article 2.11(a) of NDPR

5.2.3.5 the effectiveness and enforceability of its Personal Data protection laws (including case laws) or rules, especially rules for the transfer of Personal Data to another foreign country or international organization;

5.2.3.6 the existence and effective functioning of one or more independent supervisory authorities with responsibility for ensuring and enforcing compliance with Personal Data protection rules, including adequate enforcement powers, for assisting and advising the Data Subjects in exercising their rights and for cooperation with relevant Nigerian authorities; and

5.2.3.7 the regional or international commitments (conventions, multilateral) it has entered into on Personal Data protection.

5.2.4 Currently, NITDA has made Adequacy Decisions for 37 countries (known as the Whitelist), which are: the European Union's 28 countries and each of Angola, Argentina, Australia, Brazil, Canada, Cape Verde, China, Ghana, Iceland, Israel, Japan, Kenya, New Zealand, Norway, Switzerland, Uruguay and United States of America.[8]

5.2.5 Where a Data Controller or Data Administrator intends to transfer Personal Data to a Foreign Country that is not on the Whitelist, it must, in addition to obtaining the explicit consent of the Data Subject, satisfy any of the following conditions:

5.2.5.1 inform the Data Subject, prior to obtaining the Data Subject's consent, of the possible risks of the Foreign Transfer;

5.2.5.2 the Foreign Transfer must be necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

5.2.5.3 the Foreign Transfer must be necessary for the performance of a contract, which is in the interest of the Data Subject, between the Data Controller and another person;

5.2.5.4 the Foreign Transfer must be necessary for important reasons of public interest;

5.2.5.5 the Foreign Transfer must be necessary for the establishment, exercise or defence of legal claims; and

5.2.5.6 where the Data Subject is physically or legally incapable of giving consent, then the Foreign Transfer must be necessary in order to protect the vital interests of the Data Subject or that of other persons; and

[8] See generally, the NDPR Implementation Framework, available at: https://nitda.gov.ng/it-frameworks
The United States of America is limited to companies certified under the US Privacy Shield.

5.2.5.7 where the Data Subject is answerable in duly established legal action/claim, civil or criminal, in the Foreign Country.

5.3.1 NITDA has a mandate to develop local and international relationships to facilitate the effective implementation of NDPR and related legislations.[9]

5.3.2 To this end, NITDA is required to:

5.3.2.1 provide international mutual assistance frameworks for international notifications, complaints, referrals, investigative assistance and information exchange. Before doing this, NITDA has to ensure that such Foreign Countries have appropriate Personal Data protection safeguards and fundamental rights and freedoms;

5.3.2.2 engage stakeholders in discussions and activities that further international cooperation in the enforcement of NDPR and related legislations;

5.3.2.3 promote the exchange of Personal Data protection legislations and practices.

5.3 Definitions of Common Terms in Module 5:

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

	Term	Meaning
5.4.1	AGF	Honourable Attorney General of the Federation of Nigeria.
5.4.2	Foreign Country	Any sovereign State, or an autonomous or semiautonomous territory within the international community.
5.4.3	Foreign Transfer	The transfer of Personal Data to a Foreign Country.
5.4.4	Whitelist	A list of Foreign Countries of which NITDA has made Adequacy Decisions.

5.5 Module: Summary

5.5.1 A Data Controller or Data Administrator is prohibited from transferring Personal Data to any person except where the consent of the Data Subject is obtained without fraud, coercion or undue influence.

5.5.2 Any transfer of Personal Data to a Foreign Country must be done further to NITDA's Adequacy Decision on that Foreign Country. In the absence of an Adequacy Decision, the Data Controller or Data Administrator must in addition to obtaining the explicit consent of the Data Subject, satisfy NITDA on the adequacy of the Personal Data protection regime of the Foreign Country, among other requirements.

5.5.3 NITDA has a mandate to develop local and international relationships to facilitate the effective implementation of NDPR and related legislations with the supervision of the AGF.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[10]
2. National Information Technology Development Act 2007[11]
3. NDPR Implementation Framework (Discussion Draft)[12]

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

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

[12] Available at : https://nitda.gov.ng/it-frameworks/

NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 6:
DATA PROTECTION COMPLIANCE PROCESSES: AUDITS AND IMPACT ASSESSMENTS

Module 6: Overview

In this Module, we will learn about, the:

6.1 the compliance requirements under the NDPR

6.2 Data Protection Audits (DPAs); and

6.3 Data Protection Impact Assessments (DPIAs).

6.1. The NDPR Compliance Requirements:

6.1.1 NDPR compliance requirements refer to the major practices or processes NDPR requires that a Data Controller or Data Administrator must undertake. These major process requirements are set out below:

6.1.1.1 All Data Controllers must have made their Data Protection Policies publicly available on or before April 25, 2019;[1]

6.1.1.2 A Data Controller must either designate one of its personnel as its DPO or outsource the function;[2]

6.1.1.3 All Data Controllers or Administrators must appoint a DPCO;

6.1.1.4 All Data Controllers or Administrators that processed the Personal Data of more than 1,000 Data Subjects within 6 months from January 25, 2019, must undergo and file, through its DPCO, an initial Data Protection Audit Report (**Initial DPA Report**) with NITDA not later than July 25, 2019;[3]

6.1.1.5 All Data Controllers or Administrators that annually process the Personal Data of more than 2,000 Data Subjects, must undergo and file, through its DPCO, an Annual Data Protection Audit Report (**Annual DPA Report**) with NITDA not later than March 15 of the following year;[4]

6.1.1.6 Data Controllers that intend to undertake new projects that would involve Personal Data processing should carry out a DPIA to identify possible areas where breaches may occur and device means of addressing such risks.

6.1.1.6 Data Controllers must immediately notify (within 72 hours) NITDA in the event of a data breach.[5]

[1] Article 4.1(1) of NDPR
[2] Article 4.1(2) of NDPR
[3] Article 4.1(5) and 4.1(6) of NDPR. This date was subsequently revised by NITDA to October 25, 2019.
[4] Article 4.1(7) of NDPR.
[5] NDPR Implementation Framework currently under discussion.

6.1.2 Let us now turn to discussing the DPA and DPIA in detail.

6.2. Data Protection Audits:

6.2.1 A Data Protection Audit (DPA) is a DPCO's investigation or examination of the record, processes and procedures of a Data Controller or Data Administrator to verify their compliance with NDPR's requirements.

6.2.2 You may recall our engagement of the concept of the DPCO from Module 2 where we defined a DPCO as 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.[6] Accordingly, a major purpose of DPCOs is the conduct of DPAs on Data Controllers and Data Administrators.

6.2.3 NDPR provides for the Initial DPA and an Annual DPA. Both DPAs cover the same scope save for the differences highlighted in the succeeding paragraphs.

6.2.4 The Initial DPA is required to be carried out within 6 (six) months from NDPR's commencement date on January 25, 2019.[7] The July 25, 2019 due date was subsequently moved forward by NITDA to October 25, 2019. All Data Controllers or Administrators that processed the Personal Data of more than 1,000 Data Subjects within 6 months from NDPR's commencement were due to file Initial DPA Report through their DPCOs.[8]

6.2.5 The Annual DPA is required to be carried out annually by all Data Controllers or Administrators that process the Personal Data of a minimum 2,000 Data Subjects in the preceding year. The Annual DPA Report is required to be filed on or before March 15 of the next year.[9] The first set of Annual DPA Reports in Nigeria are due to be filed on March 15, 2020 in respect of data processing activities that occurred between January and December 2019.

6.2.6 A DPA Report is expected to disclose all of the following information, that is, the:

6.2.6.1 nature of the Personal Data, that is, the personally identifiable information, that the Data Controller or Data Administrator collects; the relevant Data Subjects would include the Data Controller or Data Administrator's employees, clients/customers, employees' family members, visitors to the Data Controller or Data Administrator's premises et.al.;

[6] Article 1.3(xiii) and 4.1(4) of NDPR
[7] Article 4.1.5 of the NDPR
[8] Article 4.1(5) and 4.1(6) of NDPR.
[9] Article 4.1(7) of NDPR.

6.2.6.2 purpose for which Personal Data is being collected; naturally, this purpose must be one of the lawful basis for Personal Data collection – recall these 6 from Module 2 - (in no order of importance): Consent, Contract, Legal Obligation, Legitimate Interest, Public Interest and Vital Interest?;

6.2.6.3 form and details of the notices given to Data Subjects on the processing of their Personal Data – recall our definition of Privacy Policy/Notice from Module 3 – a medium through which Data Subjects are to be informed of their rights and other information of the Data Controller in relation to their Personal Data;

6.2.6.4 nature of the access that will be given to Data Subjects, further to DSAR[10] , for the Data Subject to or request for a review, amendment, correction, supplementation, or deletion of the relevant Personal Data;

6.2.6.5 form of consent obtained from the Data Subject, where such is the case;

6.2.6.6 information security policies and practices of the Data Controller or Data Administrator;

6.2.6.7 policies and practices of the Data Controller or Data Administrator for the proper use (including privacy and protection), monitoring and reporting of Personal Data breaches;

6.2.6.8 policies and practices of the Data Controller or Data Administrator on DPIAs, particularly how technologies will impact the privacy or security of the Personal Data that they process or intend to process.

6.2.7 The NDPR Implementation Framework, which is a document currently under discussion, sets out varying questions that may be administered by the DPCO on the Data Controller or Data Administrator, with the view of eliciting responses that will be useful for the DPCO in generating its DPA Report on the Data Controller or Data Administrator.

6.2.8 However, at the heart of an audit exercise is, verification. The essence of an audit is to verify the existence or otherwise of information. Accordingly, it will be insufficient for a DPCO to simply base its DPA Report on the responses of the Data Controller or Data Administrator to the DPCO's questionnaire. The DPCO must proceed to further verify any reference

[10] Recall our definition of DSAR in Module 3: Data Subject access request made pursuant to the Data Subject's right of access

document or other document that the Data Controller or Data Administrator alludes to in its responses to the DPCO's questionnaire. For example, it will be prudent audit practice for the DPCO to verify the existence or accurateness of any policy, contract or other document that the Data Controller or Data Administrator alludes to. It will not be good practice for the DPCO to simply confirm the existence or accuracy of a document or other information which the DPCO cannot independently verify.

6.2.9 A DPA Report is concluded with a Verification Statement sworn to by the DPCO. The text of the Verification Statement reads:

I _[*insert name of DPCO's personnel*]_ of _[*insert name of DPCO*] _ a licensed Data Protection Compliance Organization (DPCO) under Article 4.1(4) of the Nigeria Data Protection Regulation (NDPR) hereby make this statement on oath that the Data Audit Report (DAR) herein filed by _[*insert name of Data Controller or Data Administrator*]_ is conducted in line with the NDPR and that it is an accurate reflection of _[*insert name of Data Controller or Data Administrator*]'s Personal Data management practices.

Signature License Number Date

6.2.10 Given that the DPA Report must be attested to on oath, it is imperative that DPCOs carefully validate the DPA Report before making their verification Statement on oath and filing the DPA Report with NITDA. A statement made on oath which the maker knows to be untrue is a criminal act which attracts the sanction of imprisonment.

6.3 Data Protection Impact Assessments:

6.3.1 DPIA is a risk assessment done to ascertain the possible implication of certain Personal Data processing activities. For example, DPIA is required to be conducted to identify possible areas where breaches may occur and the means by which the risk of those breaches may be mitigated.

6.3.2 DPIAs are not mandatory for all Personal Data processing activities. The following processing activities or situations have however been highlighted as requiring DPIAs, that is, where:

6.3.2.1
the Personal Data or Data Subject will be evaluated or profiled;

6.3.2.2
there will be automated decision-making on the Personal Data

6.3.2.3 there will be systemic monitoring of the Personal Data or Data Subject;

6.3.2.4 Sensitive Personal Data will be processed;

6.3.2.5 the Data Subjects are vulnerable persons;

6.3.2.6 new or innovative technologies are to be deployed for Personal Data processing activities

6.3.3 A typical DPIA Report is required to retain such information as, the:

6.3.3.1 description of the envisaged Personal Data processing activities;

6.3.3.2 purpose of the processing activity;

6.3.3.3 legitimate interest pursued by the Data Controller or Data Administrator;

6.3.3.4 assessment of the necessity and proportionality of the processing activity in relation to the purpose of the processing activity;

6.3.3.5 assessment of the risks to the rights and freedoms of Data Subjects; and

6.3.3.6 mitigation measures being proposed to address the

6.3.4 Data Controllers or Data Administrators are required to have policies and

6.4 Definitions of Common Terms in Module 3:

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

	Term	Meaning
6.4.1	Annual DPA	The Data Protection Audit required to be undertaken by Data Controllers or Data Administrators that annually process the Personal Data of more than 2,000 Data Subjects.
6.4.2	DPA	Data Protection Audit, which could be either an Initial DPA or Annual DPA.
6.4.3	DPIA	Data Protection Impact Assessment, required to be undertaken by Data Controllers or Data Administrators at the start of a new project which will require the processing of Personal Data.

	Term	Meaning
6.4.4	DPA Report	A report issued by the DPCO of its findings from a DPA.
6.4.5	DPIA Report	A report issued by the DPCO of its findings from a DPIA.
6.4.6	Initial DPA	The first Data Protection Audit required to be undertaken by Data Controllers or Data Administrators that processed the Personal Data of more than 1,000 Data Subjects within NDPR's first 6 months.
6.4.7	NDPR Implementation Framework	A document due to be issued by NITDA and which will explain in greater details, the administrative processes of the NDPR.
6.4.8	Verification Statement	A statement that will be made on oath, verifying a DPCO's DPA Report on a Data Controller or Data Administrator.

6.5 Module 6: Summary

6.5.1 NDPR has some time-sensitive compliance requirements including the filing of DPA Reports and DPIA Reports.

6.5.2 DPA Reports, whether initial or annual are required to contain specific information, on oath, on the policies and practices of the Data Controller or Data Administrator.

6.5.3 DPIAs are not mandatory but are required to be undertaken in certain circumstances, especially where there are associated risks with the intended Personal Data processing activities.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[11]
2. National Information Technology Development Act 2007[12]
3. NDPR Implementation Framework (Discussion Draft)[13]

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

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

[13] Available at: https://ndpracademy.ng/resources/NDPR Implementation Framework.pdf

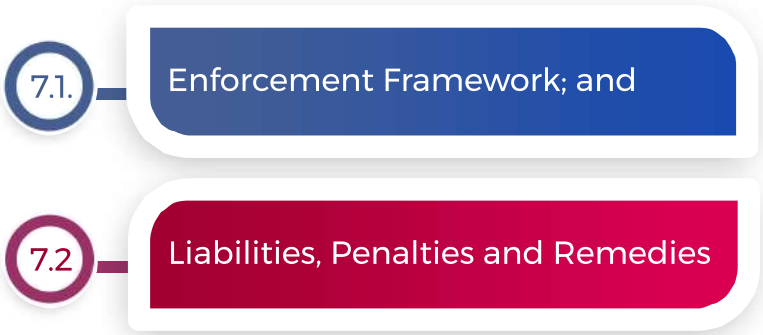
NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 7:
NDPR LIABILITIES, PENALTIES AND REMEDIES

Module 7: Overview

In this Module, we will learn about, the NDPR's:



7.1. NITDA'S Enforcement Framework

7.1.1 NITDA's enforcement framework for NDPR is comprised of the following 5: Surveillance, Complaint Filing, Investigations, Administrative Sanctions; and Criminal Prosecution. We shall now turn to understanding each.

7.1.2 **Surveillance:** Surveillance refers to NITDA's specific and deliberate monitoring activity for the purpose of identifying a breach of the NDPR. This becomes necessary in the circumstance that Data Controllers or Data Administrators may or may not be in deliberate breach of the NDPR. A non-deliberate breach of the NDPR is however still a breach. NITDA adopts surveillance to also co-opt other relevant stakeholders to identify NDPR breaches and report breaches to NITDA.

7.1.3 **Complaint Filings:** The Data Subject, a compliance officer, civil society,[1] government agency or any person who believes that a Data Controller or Data Administrator is not complying with the NDPR can file a Complaint with NITDA.

7.1.4 Data Controllers and Data Administrators also have a duty to self-report Personal Data breaches.[2] You may recall from Modules 2 and 4, the obligations placed on Data Controllers and Data Administrators to have policies and procedures for monitoring and reporting violations of privacy and Personal Data protection policies. The NDPR Implementation Framework sets the time-threshold for Data Controllers or Data Administrators at 72 (seventy-two) hours of their knowledge of the Personal Data breach. The Data Controller or Data Administrator's report must include,

7.1.4.1 date or time/period during which the violating acts or omissions occurred;

7.1.4.2 description of the circumstances of the loss or unauthorised access or disclosure, for example, the cause of the breach;

[1] Article 4.1(8) of NDPR
[2] Article 4.1 (5)(i) of NDPR

7.1.4.3 description of the Personal Data involved in the loss or unauthorised access or disclosure;

7.1.4.4 an assessment of the risk of harm to Data Subjects as a result of the loss or unauthorised access or disclosure;

7.1.4.5 an estimate of the number of Personal Data and or Data Subjects that are at real risk of significant harm as a result of the loss or unauthorised access or disclosure;

7.1.4.6 description of remedial actions or any steps the Data Controller or Data Administrator has taken to reduce the risk of harm to Data Subjects;

7.1.4.7 description of any steps the Data Controller or Data Administrator has taken to notify the Data Subject of the loss or unauthorised access or disclosure; and

7.1.4.8 name and contact information of the Data Controller or Data Administrator's personnel or other person who can attend to NITDA's queries on the loss or unauthorised access or disclosure.

7.1.5 Complaints must be in writing and can be filed in paper format or electronically, for example, by email. NITDA may prescribe additional procedures for filing Complaints, as well as the place, manner and other details of filing.

7.1.6 The Complaint must disclose, the:

7.1.6.1 the name of the Data Controller, Data Administrator, Third Party or other person that is the subject of the Complaint (altogether **Concerned Entity**);

7.1.6.2 the violating acts or omissions of the Concerned Entity must be described;

7.1.7 Upon receipt of a Complaint, NITDA may take any of the following actions:

7.1.7.1 contact the Concerned Entity for enquiry;

7.1.7.2 review of earlier filed Annual DPA Report, if any, of the Concerned Entity;

7.1.7.3 issue a Personal Data protection compliance query;

7.1.7.4 impose administrative sanctions;[3] and

7.1.7.5 prosecute the Concerned Entity.

[3] Paragraphs 7.1.6 to 7.1.9 discusses Administrative Sanctions in detail.

7.1.8 **Investigations:** NITDA may by itself, or through an Administrative Redress Panel (**ARP**)[5] set up for that purpose, investigate any Complaint filed against a Concerned Entity when a preliminary review or the facts indicates a possible violation of the provisions of any regulatory instrument, especially the NDPR by the Concerned Entity. NITDA may by its officers or through designated DPCOs, investigate any filed complaint and may also do so based on a special audit or spot check. Investigations may include a review of the policies, procedures, or practices of the Concerned Entity and of the circumstances of the alleged violation. NITDA will, at the time of the initial written communication to the Concerned Entity, indicate the basis of its audit or investigation.

7.1.9 **Administrative Sanctions:** NITDA can impose administrative sanctions for any breach of the NDPR. NITDA will do this through an ARP that may be set up for such purpose. An ARP is set up with the mandate of investigating and hearing of complaints. To this end, ARP:

7.1.9.1 will invite the Concerned Entity to respond to the Complaint;

7.1.9.2 may, pending the outcome of the investigation, make administrative orders to protect the subject-matter of the Complaint;

7.1.10 ARPs, which will be composed of accomplished information technology professionals, public administrators and lawyers, has 28 (*twenty-eight*) days to investigate, conclude and determine the appropriate redress on any Complaint.

7.1.11 ARP's procedural rules is to be drawn up by a panel of experts. The rules are to feature the following principles:

7.1.11.1 preference for online dispute resolution mechanism;

7.1.11.2 fair hearing, fairness and transparency;

7.1.11.3 written processes, such that oral presentations are limited to the barest minimum;

7.1.11.4 decisions must clearly:

7.1.11.4.1 state the proof of violation;

[5] Paragraphs 7.1.6 to 7.1.9 discusses the ARP in detail.

7.1.11.4.2 identify the Concerned Entities in an anonymised, pseudonymised or summarised format;

7.1.11.4.3 state the violated NDPR provision and the acts or omissions which exacerbated the breach.

7.1.11.5 in reaching its decision, the ARP, NITDA or a Court may consider:

7.1.11.5.1 the nature, gravity and severity of the breach complained of;

7.1.11.5.2 the number of Data Subjects affected and damages suffered by them;

7.1.11.5.3 opportunities for curtailment left unexplored by the Concerned Entity;

7.1.11.5.4 whether the Concerned Entity has a reputation or history of data or other criminal or corporate breaches;

7.1.11.5.5 the number of employees in the Concerned Entity's establishment;

7.1.11.5.6 the possible impact of a fine on the Concerned Entity's overall contribution to the Nigerian economy.

7.1.12 The administrative sanctions or orders that can be made by any of the ARP, NITDA or the Court could include any of the following:

7.1.12.1 suspension of the Concerned Entity's service pending further investigations;

7.1.12.2 issuance of a public notice to warn the public to desist from patronizing or doing business with the Concerned Entity;

7.1.12.3 refer the Concerned Entity to its self-regulatory organization (SRO) for appropriate sanctions; a SRO in this case may be a trade association of self-interest organisation that the Concerned Entity is a member of.

7.1.13 **Criminal Prosecution:** Where NITDA has determined that a Concerned Entity's breach of the NDPR affects national security, sovereignty and cohesion, it may seek to prosecute the officers of the Concerned Entity pursuant to its criminal prosecution powers.[6] In this regard, NITDA will seek a fiat of the Honourable Attorney General of the Federation. It may also file a petition with any prosecuting authority in Nigeria. These prosecuting authorities include, the; Economic and Financial Crimes Commission, Department of State Security, Nigerian Police Force, Independent Corrupt Practices Commission; and Office of National Security Adviser to the President of the Federal Republic of Nigeria.

[6] Section 17(1) and (3) of NITDA Act

7.2 Liabilities, Penalties and Remedies:

7.2.1 A Data Controller that is found to be in breach of the Personal Data rights of a Data Subject, will be liable, in addition to any other criminal liability, to the following penalties:[7]

Number of Data Subjects	Penalty
<10,000	1% (*one percent*) of the Data Controller's annual gross revenue of the preceding year or N2million (*Two Million Naira*), whichever is higher.
>10,000	2% (*two percent*) of the Data Controller's annual gross revenue of the preceding year or N10million (*Ten Million Naira*), whichever is higher.

7.2.2 The NDPR Implementation Framework which is currently being discussed ahead of its release proposes that breach of a Data Subject's privacy rights be a strict liability offence. What this means is that the intent, knowledge or otherwise of the Data Controller is not required to establish its culpability. Accordingly, the fact that the breach of a Data Subject's privacy rights occurred is conclusive of the commission of an offence and for which the above penalties will be imposed.

7.2.3 The Data Subject may also seek redress for the violation of his or her privacy rights in a civil court of competent jurisdiction.[8] The Data Subject may in such instances sue both or either of the Data Controller or Data Administrator in tort, for the wrong.

7.2.4 A Data Administrator that breaches the terms of its contract with a Data Controller can similarly be sued for breach of contract by the Data Controller.

7.3 Definitions of Common Terms in Module 7:

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

	Term	Meaning
7.3.1	ARP	The Administrative Redress Panel, set up for the purpose of investigating any Complaint.

[7] Article 2.10 of NDPR
[8] Article 4.2(1) of NDPR

	Term	Meaning
7.3.2	Complaint	A formal notification of the breach of the NDPR submitted to NITDA by any of a Data Subject, a compliance officer, civil society, government agency or any person who believes that a Data Controller or Data Administrator is not compliant with the NDPR
7.3.3	Concerned Entity	Any of the Data Controller, Data Administrator, Third Party or other person that is the subject of a Complaint
7.3.4	SRO	Self-Regulating Organisation, a trade association of self-interest organisation that a Concerned Entity is a member of

7.4 Module 7: Summary

7.4.1 NDPR's enforcement framework is comprised of the following 5: Surveillance, Complaint Filing, Investigations, Administrative Sanctions; and Criminal Prosecution.

7.4.2 A Data Controller that is found to be in breach of the Personal Data rights of a Data Subject, will be liable, in addition to any other criminal liability to fines that could be up to 2% of its annual gross revenue in the preceding year or N10million, whichever is higher.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[9]
2. National Information Technology Development Act 2007[10]
3. NDPR Implementation Framework (Discussion Draft[11]

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

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

[11] Available at: https://ndpracademy.ng/resources/NDPR Implementation Framework.pdf