NDP ACADEMY

MODULE 1:

PRINCIPLES OF PERSONAL DATA PROCESSING: LAWFULNESS IN FOCUS

Module 1: Overview

In this Module, we will learn about:

1.1 Overview of Personal Data Processing Principles;

1.2 The 6 Lawful Bases of Personal Data processing: Practical Considerations; and

1.3 Practical Consideration of the Consent Basis.

1.1 Overview of Data Processing Principles

1.1.1 Recall in Module 2 of the Foundation Course, we examined the 6 Principles of Data Processing, which are summarized as follows:

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

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

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

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

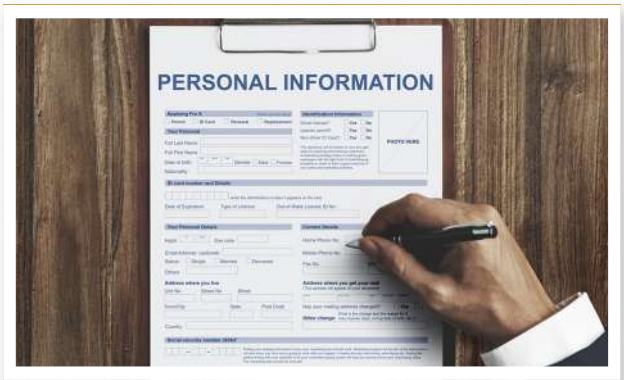
1.1.1.5 **Storage**: Personal Data must be retained only for as long as necessary.

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

1.2 The 6 Lawful Bases of Personal Data Processing: Practical Considerations

1.2.1 You may recall from the Foundation Class that Personal Data processing includes such activities as the following, when undertaken on Personal Data: collection, recording, organisation, structuring, storage, adaptation/alteration, retrieval, consultation, use, disclosure by transmission, dissemination/making available, alignment/combination, restriction, and erasure/deletion.

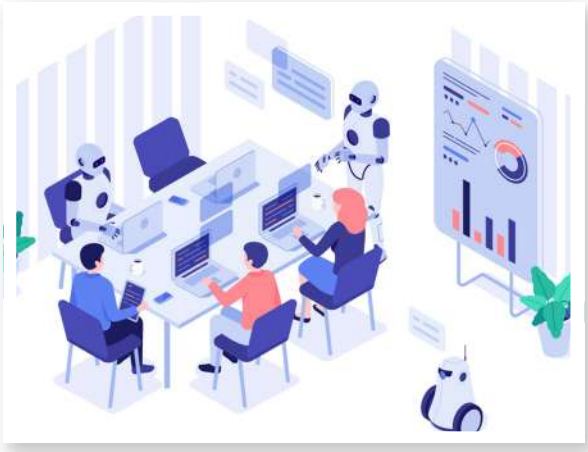
1.2.2



The principle of lawfulness of Personal Data processing is in two parts which states that: (a) Personal Data must only be processed for lawful purposes and must be processed in a fair and transparent manner; and (b) there must be a legal basis for each Personal Data processing activity. It is the second part that this section of the Module focuses on.

1.2.3 There must be a lawful basis for each Personal Data processing activity that is typically carried out by Data Controllers, Data Administrators or other third-parties. Where there is no lawful basis, no Personal Data processing activity should take place.

1.2.4 NDPR does not recognise Personal Data processing activities that are carried on for unlawful purposes. For instance, the 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] Accordingly, where Personal Data is "processed" for an illegitimate or illegal purpose, such circumstance will not be regarded as processing under the Nigeria Data Protection Regulation.



[1] Article 2.4(a) of NDPR

Think Time

The Syndicate is a textile manufacturing company which carries out textile manufacturing as a cover for its human trafficking activities. In the course of its trafficking activities, it collects and stores information such as names, phone number, email address, BVN, Date of Birth of the people it traffics. On the 16th of May 2019, its system was hacked and the Personal Data of Mr. Smith who was smuggled out of Nigeria to the United States is leaked. Mr. Smith is concerned about the breach and wants to report the breach to NITDA. What would you advise Mr. Smith?

1.2.5 A Data Controller can base its Personal Data processing activity on any of the 6 lawful bases of Personal Data processing recognised by the NDPR. The 6 bases are:

1.2.5.1 **Contract:** in which case, the Personal Data processing activity is necessary for the performance of a contract to which the Data Subject is a party.

1.2.5.2 **Legal Obligation:** in which case, the Personal Data processing activity is required for the performance of a legal obligation to which the Data Controller is subject.

1.2.5.3 **Legitimate Interest:** in which case, the Personal Data processing activity is being carried out for the legitimate business interest of the Data Controller.

1.2.5.4 **Public Interest:** in which case, the Personal Data processing activity is necessary for the performance of a task carried out in the public interest or in the exercise of a public mandate vested in the Data Controller.

1.2.5.5 **Vital Interest:** in which case, the Personal Data processing activity is necessary for the protection of the vital interest of the Data Subject.

1.2.5.6 **Consent:** in which case, the Data Subject has given consent to the processing of his or her Personal Data.[2]

1.2.6 All of the above 6 are the NDPR's cognizable lawful bases for Personal Data processing activities. It is significant that "lawful" prefixes their description as they must be applied lawfully and particularly in line with the NDPR. Thus, in basing data processing activities on any of the 6 lawful bases, that data processing activity and its relevant lawful basis must absolutely respect all the earlier discussed 6 Personal Data processing principles. For example, in basing a data processing activity on Consent of the Data Subject being its lawful basis, the Data Controller is required to, among others, abide by the first of the 6 principles of Personal Data processing, to wit, the Consent must be for a specific, legitimate and lawful processing activity. [3]

1.2.7 We shall now consider each of them with more practical details, but shall specially reserve the legal basis of Consent to be discussed in the next sub-section of this Module.

Contract

1.2.8 Personal Data processing is lawful if it is necessary for the performance of a contract to which the Data Subject is a party or necessary in order to take steps at the request of the Data Subject prior to entering into a contract.[4] For instance, documented contracts are daily being entered into; a process which typically entails the need for the confirmation of the identities of the relevant parties to the contract.

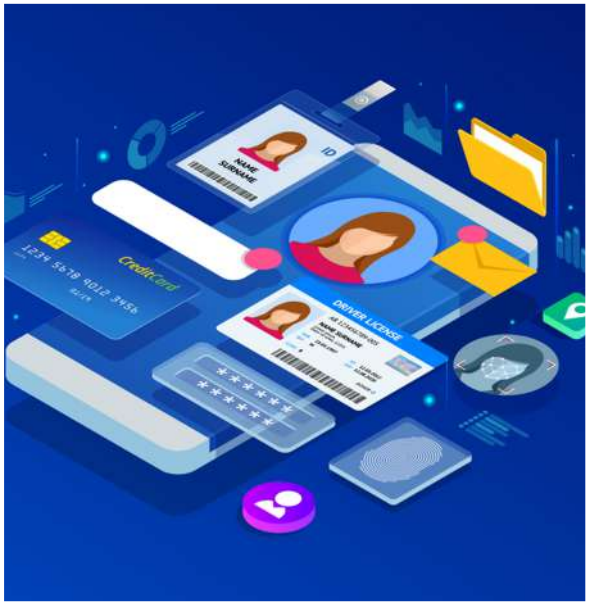
In this regard, Personal Data such as name, address, (occupation sometimes) may usually be exchanged and processed. Such processing is allowed under the NDPR as it is done in order to ensure the formation and performance of a contract of which the Data Subject is a party. Accordingly, Personal Data processing is lawful where undertaken at the instance of the Data Subject prior to and or subsequent to entering into a contract.

2 More of the "Consent" basis will be discussed below

3 Article 2.1(1)(a) and 2.4(a) of NDPR.

4 Article 2.2(b) of the NDPR.

1.2.9 Thus, where as part of ensuring that Ms. Beatrice considers him as a suitable tenant for a possible leasehold transaction, Mr. Adams submits his Personal Data to Ms. Beatrice for her due diligence. Ms. Beatrice's collection, storage and use (all Personal Data processing activities) of Mr. Adams' Personal Data for her due diligence, whether or not a lease agreement is eventually executed, are all validated under the lawful basis of the contract that informed the Personal Data processing activities. According to the NDPR, the processing was undertaken in order to take steps at the request of the Data Subject, prior to entering into the contract. [5]



Think Time

Denzel Corporation, an automobile manufacturing company wants to hire Smith, who has specialty in inspecting vehicle engines to verify authenticity and also detect any defects in the engine. However, the Company states that before Smith can be hired and before the formal signing of a Contract of Employment, he would have to provide the Company with such Personal Data as his name, address, phone number/email, details of his next of kin as well as Sensitive Personal Data relating to his ethnicity, religion and criminal records. Is Denzel Corporation right to request for such Personal Data? Can Smith sue Denzel Corporation under the NDPR if Denzel Corporation eventually chooses not to hire Smith on the ground that Smith refused to provide his Personal Data?

Legal Obligation

1.2.10 A Data Controller may process Personal Data on the basis of the legal obligation imposed on the Data Controller to do so. Legal obligation in this regard means that such Data Controller is required by law to conduct such processing activities on such Personal Data. Thus, where the provisions of a law require that a Data Controller process the Personal Data of a Data Subject, such data processing activity is said to be undertaken under the lawful basis of Legal Obligation.

[5] See Article 2.2(b) of NDPR and also Article 6(1)(b) of the EU GDPR

1.2.11 For example, when the Central Bank of Nigeria (CBN) directed deposit-taking banks in Nigeria to hold records of their customers and retain such for a prescribed period, the CBN directive was the lawful basis of the Personal Data processing activities undertaken by the deposit-taking banks in this regard. Typically, the deposit-taking banks will collect, analyse, store, use, transfer and possibly delete (all Personal Data processing activities) the following Personal Data of the customer: name, phone number, email address, home address, bank verification number, details of next of kin et. al.

1.2.12 A Public Institution that intends to process Personal Data on the ground of its Legal Obligation is required to get the prior approval or endorsement of any of the President of the Federal Republic of Nigeria (**President**), the Governor of the relevant State in Nigeria (**Governor**), a Federal Minister of the Federal Republic of Nigeria (**Minister**) or the Chief Executive Officer (**CEO**) of the Public Institution. [6]

1.2.13 Further, the Public Institution is required to keep a record of all its Personal Data processing activities on this basis.[7] The record must show:

1.2.13.1 the approval or endorsement mention in 1.2.12 above;

1.2.13.2 the purpose of the processing activity while disclosing the Legal Obligation that informs the processing;

1.2.13.3 the output sought for the processing activity and the manner in which such output will be applied for the benefit of Data Subjects;

1.2.13.4 the proof of compliance with the mandatory data security requirements in NPIG, which are that, it must:

1.2.13.4.1 establish compliance with adequate international information security processes and standards such as ISO 27001:2013 or similar standards;

1.2.13.4.2 undertake DPIA as appropriate and submit its DPIA Report to NITDA; and

1.2.13.4.3 retain the services of a licensed DPCO.[8]

[6] Paragraphs 2.2(g)(iii),(h) and 6(a) of the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 (the "NDPR Public Institutions Guidelines" or "NPIG").

[7] Paragraph 6 of NPIG.

[8] Paragraphs 2.6 and 2.8 of NPIG.

1.2.13.5 an undertaking to protect, not deanonymize, and not to use the Personal Data for another purpose than initially intended.

Think Time

NAFDAC by the powers given to it through the NAFDAC Act recently released regulations to pharmaceutical companies, pharmacies and hospitals to collect the names, addresses, information on health and ethnicity of persons to whom drugs were sold to. ALyv Clinic has issued a notice to its staff and wards. Mr, Ajayi who always buys his drugs from ALyv Clinic is surprised at this new practice and has approached you to advice on what ground the hospital is collecting his information. Would there be any change to your advice if the Clinic further asked for his criminal records in addition to the above information mandated by NAFDAC? If ALyv Clinic was a government hospital what would be the first thing it would do if processing Personal Data under the basis of legal obligation?

Legitimate Interest

1.2.14 Personal Data processing may be on the basis of the legitimate interest of the Data Subject[9] or the legitimate business interest of the Data Controller or a third party.[10]

1.2.15 The concept of "legitimate interest" is not defined by the NDPR. The EU GDPR also does not define it, although it describes the instances of the legitimate interest of a Data Controller to include: marketing activities, networking and information security, fraud prevention, promotion and continuation of business activities to the extent allowed by law. [11]

1.2.16

Further, while the NDPR identifies the concept of legitimate interest with the Data Controller or other third party, NPIG states that it is the legitimate interest of the Data Subject that forms the lawful basis for Public Institutions. [12]

1.2.17 Where a Data Controller intends to base its Personal Data processing activity on Legitimate Interest, then it must, prior to collecting (a Personal Data processing activity) Personal Data, inform the Data Subject of the legitimate interests pursued by the Data Controller or the third party.[13] Deriving from the EU GDPR's application of the legitimate interest concept, it is safe to conclude that the legitimate interest of the Data Controller extends to lawful activities for the security, expansion and promotion of the business of the Data Controller or a third party. Accordingly, where a Data Controller intends to use Personal Data for such security, expansion and promotion activities, it must disclose all of such facts in its Privacy Notice.

9 Paragraph 2.2(f) of NPIG.
10 Articles 3.1(7)(d), 3.1(9)(c) and 3.1(11)(d) of the NDPR.
11 Recital 47 of the EU GDPR
12 Paragraph 2.2(f) of NPIG.
13 Article 3.1(7)(d) of NDPR

1.2.18 Given the largely subjective nature of basing Personal Data processing activities on the Data Controller's Legitimate Interest, it is advisable to complement Legitimate Interest as a basis of Personal Data processing with other more established lawful basis.

Think Time

Nine Gates Solutions (NGS) is a telecommunications company established and carrying out its business activities in Nigeria. NGS' business development strategy involves the creation of market intelligence contents and weekly distribution of such content to over 1 million Data Subjects on its database. At the base of each of such weekly distributed content are the options for: (i) the recipient to unsubscribe from receiving the particular mail; and (ii) the recipient to request NGS to delete his/her information from the NGS' database. Uwem's lawyer has written to NGS that Uwem's Data Subject rights have been breached because Uwem did not consent to receive the weekly distributed content. NGS' in-house Counsel has approached you that she believes NGS has distributed the weekly distributed content further to its legitimate interest, more so as Uwem's Personal Data is on its database because Uwem had patronized the services of the company in time past. What would you consider in advising NGS' in-house Counsel?

Public Interest

1.2.19

Personal Data of a Data Subject may be processed on the basis of Public Interest. This covers all data processing activities necessary for the performance of a task carried out in the interest and for the benefit of the general public or in the exercise of a public mandate vested in the Data Controller.[14]

1.2.20

While not exclusive to them, Public Institutions are more likely to process Personal Data on the basis of Public Interest. A Public Institution that intends to process Personal Data on the ground of its legal obligation is required to get the prior approval or endorsement of any of the President, the Governor, a Minister, or the Public Institution's CEO.[15]

[14] Article 2.2(e) of NDPR.
[15] Paragraphs 2.2(g)(iii) and 6(a) of NPIG.

1.2.21 Similar to processing on the basis of Legal Obligation, the Public Institution is required to keep a record of all its Personal Data processing activities on the Public Interest basis.[16] The record must show:

1.2.21.1 the official approvals or endorsement mention in 1.2.20;

1.2.21.2 the purpose of the processing activity while disclosing the Public Interest that informs the processing;

1.2.21.3 the output sought for the processing activity and the manner in which such output will be applied for the benefit of Data Subjects;

1.2.21.4 the proof of compliance with the mandatory data security requirements in NPIG, which are that, it must:

1.2.21.4.1 establish compliance with adequate international information security processes and standards such as ISO 27001:2013 or similar standards;

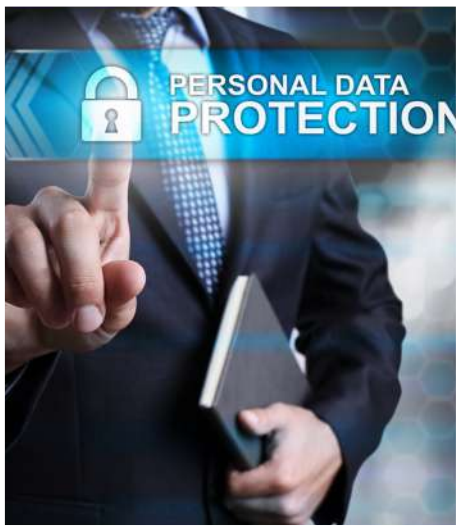
1.2.21.4.2 undertake DPIA as appropriate and submit its DPIA Report to NITDA; and

1.2.21.4.3 retain the services of a licensed DPCO.[17]

1.2.21.5 an undertaking to protect, not deanonymize, and not to use the Personal Data for another purpose.

16 Paragraph 6 of NPIG.
17 Paragraphs 2.6 and 2.8 of NPIG.

1.2.22 In the wake of the COVID-19 pandemic in Nigeria and in a bid to curtail and manage its spread, Public Officers were placed at entry ports in Nigeria to obtain Personal Data from in-bound Data Subjects. The category of Personal Data included names, addresses, health information, travel history. Concerns were raised on the privacy issues associated with these processing activities. NITDA duly issued a Public Notice confirming that the lawful bases for the Personal Data processing activities are Public Interest and Vital Interest. Therefore, where Personal Data is processed in order to ensure the protection of the general public, maintain public safety and ensure security of the populace, such processing would be covered by the legal basis of Public Interest.



Think Time

Due to the high rate of COVID-19 in Nigeria, the government has initiated a nationwide lockdown, mandating that before anyone goes out, such person must be registered and cleared by the NCDC. Information required include Name, Gender, health information including hospital records. Mrs. Peterson, who lives with her 11 year old son has approached you to enquire whether her son would be required to provide his information and what the process is. Would your answer be different if the local government where Mrs. Peterson stays was conducting a census to confirm the number of children living in that area?

Vital Interest

1.2.23

Vital Interest as a lawful basis for Personal Data processing applies not just to the interest of the Data Subject but extends to the interests of any other natural person. Personal Data is processed on the lawful basis of Vital Interest if the processing is undertaken to save the life of the Data Subject or another natural person in a case where the Consent of the Data Subject cannot be obtained. Accordingly, Vital Interest cannot validly be used as the basis for processing the health data of the Data Subject or a third party in a situation where either the Data Subject or third party is able to provide Consent for the processing activity.

1.2.24

A Public Institution that intends to process Personal Data on the basis of Vital Interest is required to get the prior approval or endorsement of any of the President, the Governor, a Minister, or the Public Institution's CEO.[18]

1.2.25

Similar to processing on the bases of Legal Obligation and Public Interest, a Public Institution is required to keep a record of all its Personal Data processing activities on the Vital Interest basis.[19] The record must show:

1.2.25.1 the official approval or endorsement mention in 1.2.24;

[18] Paragraphs 2.2(g)(iii) and 6(a) of NPIG.

[19] Paragraph 6 of NPIG.

1.2.25.2 the purpose of the processing activity while disclosing the Vital Interest that informs the processing;

1.2.25.3 the output sought for the processing activity and the manner in which such output will be applied for the benefit of the Data Subject;

1.2.25.4 the proof of compliance with the mandatory data security requirements in NPIG, which are that, the Public Institution must:

1.2.25.4.1 establish compliance with adequate international information security processes and standards such as ISO 27001:2013 or similar standards;

1.2.25.4.2 undertake DPIA as appropriate and submit its DPIA Report to NITDA; and

1.2.25.4.3 retain the services of a licensed DPCO.[20]

1.2.25.5 the purpose of the processing activity while disclosing the Vital Interest that informs the processing;

Think Time

Jack was driving home on a lonely road one night when he collided with a cement truck belonging to DGO Cement Ltd and driven by Ahmed, an employee of DGO Ltd. As a result of the impact, Jack was knocked unconscious. Ahmed, following the relevant DGO Ltd protocol, promptly alerted the DGO Cement Ltd Control Room, where instructions were given to Ahmed to obtain Jack's phone, get relevant family members' phone numbers, take pictures of the accident scene and get the registration details of Jack's car. The DGO Cement Ltd Control Room thereafter promptly contacted the nearest General Hospital which rushed to the scene and took Jack to the hospital. Included in the Personal Data that Ahmed obtained from Jack's phone is that of Jack's wife, Aisha, a lawyer and human rights activist. Aisha has wind of the fact that her Personal Data (name, phone number and house address) are still in DGO Cement Ltd's database and intends to sue DGO Cement Ltd under the NDPR for collecting her Personal Data without her Consent. What would you advise her? Will your answer be different if the basis for her proposed legal claim is on the fact that DGO Cement Ltd contacted her 6 months after the incident with an offer for her to buy 3 bags of DGO Cement for the price of 1?

[21] Paragraphs 2.6 and 2.8 of NPIG.

1.3 Practical Considerations of the Consent Basis:

1.3.1 Consent, as a lawful basis for Personal Data processing, is perhaps the one with the stringiest conditions and accordingly judged as relatively, most unreliable. We have accordingly secluded it to be specifically discussed under this separate sub-section of this Module. Given the fact that there are 5 other lawful bases for Personal Data processing, Data Controllers need to be circumspect in relying on Consent as the lawful basis for their Personal Data processing activities.

1.3.2 Consent of a Data Subject means any freely given, specific, informed and unambiguous indication given either through a statement or by a clear affirmative action done by the Data Subject indicating that he or she wishes or agrees to the processing of his or her Personal Data.[21] The highlighted 4 conditions are essential to the validity of a Data Controller's assertion that the Consent is the lawful basis for its processing of Personal Data. It is essential that the above 4 conditions are present in any circumstance where Consent is deemed by the Data Controller to be the legal basis on which the Personal Data of the concerned Data Subject is processed. Accordingly, the absence of any one of the above conditions may fault the Data Controller's position that Consent was actually given by the Data Subject for the processing of his Personal Data, thereby exposing the Data Controller to a possible breach liability in the event that such Data Controller was relying on Consent alone. It is advisable therefore that Data Controllers, before processing Personal Data of Data Subjects should try as much as possible to have more than one legal basis for such processing activity as this would serve to reduce the Data Controller's exposure to liabilities under the NDPR.

We shall now turn to each of these conditions.

Free Consent

1.3.3 Consent must be freely given; that is, without fraud, coercion or undue influence.[22] The Data Subject must be free to decide whether or not to give Consent to the Data Controller to process his or her Personal Data. In this regard, account will be taken of whether the performance of a contract is not unnecessarily conditional on consent to process Personal Data. In other words, Consent of the Data Subject must not be tied to the Data Controller's performance of a pre-existing obligation. Accordingly, there is no valid Consent in a situation where a Data Controller refuses to deliver the Data Subject's purchased goods unless the Data Subject agreed that the Data Controller can use the Data Subject's Personal Data for marketing purposes.

[22] Article 1.3(c) of NDPR and Article 4(11) of GDPR.
[23] Article 2.3(2) of NDPR

1.3.4

The concept of Free Consent is particularly relevant in the Data Subject's right to withdraw his consent at any time. Accordingly, the Data Subject can freely give his Consent and also freely withdraw same at any time before, during and after the Personal Data processing activity. The withdrawal of Consent would not affect the legality of any processing activity done before the Consent was withdrawn by the Data Subject. Accordingly, where the Data Subject gives Consent to the processing of his Personal Data and then subsequently withdraws such Consent, any processing activity done before the withdrawal would still be lawful.

1.3.5

Notwithstanding the provisions of the Privacy Policy on the manner in which Consent can be withdrawn, Consent may be freely withdrawn in other ways including by contacting the Data Controller through email, phone call etc communicating such withdrawal of consent, opting out or unsubscribing, physical communication etc. The effectiveness of any of these medium of communication are subject to the obligation of the Data Controllers to verify identity and confirm that the instruction rightly proceeds from the Data Subject.[23]

1.3.6 The concept of Free Consent is also relevant to the Consent of children. The Consent of a Data Subject that is a child or minor is similarly required as those of other Data Subjects. However, and unlike the GDPR that generally defines minors or children for its general purposes[24] as anyone under 16 years old, the NDPR through the Data Protection Implementation Framework document provides that a child, for the purposes of the NDPR is any person below the age of 13 years.[25] Further and unlike the GDPR that provides extensively for how a minor and child's Consent is to be obtained from persons who hold parental responsibility over the child, NDPR is silent on this requirement. The silence of the NDPR will however not apply to Public Institutions who are expressly required to mandatorily obtain the Consent of a parent or guardian when the Personal Data of a child is to be processed.[26] The exception to this Consent requirement are in the instances of health emergency, national security and crime prevention.[27]

1.3.7

The provisions of the Implementation Framework suggests that a child is capable of giving Consent under the NDPR,[28] when by the relevant template audit question, a Data Controller is required to communicate its Privacy Policy in a way a child can understand. The NDPR Implementation Framework further provides that a Data Controller whose processing activity targets children shall ensure its privacy policy is made in a child-friendly form with the aim of making children and their guardians have a clear understanding of the data processing activity before grant of consent.[29] You may recall that the contents of a Privacy Policy include the circumstances in which Consent is to be obtained; suggestive that once a child has been so informed and does whatever is required, the child's Consent will be deemed to have been

[23] Article 3.1(5) of NDPR.

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

[25] While NDPR is silent on the age of a child and the qualifying age for legal capacity, NITDA has indicated intentions of making provisions on this in the final versions of the Draft Implementation Framework.

[26] Paragraph 2.3(d) of NPIG.

[27] Paragraph 2.5 of NPIG.

[28] Appendix A 4.3 of the Draft Implementation Framework, which is a template audit question, states "If your organisation offers services directly to children, have you communicated privacy information in a clear, plain way that a child will understand?" This is suggestive that a response given to a child such clear and plain question is reasoned within the context of the Draft Implementation Framework.

[29] Article 5.5 of the Implementation Framework

obtained. NDPR conversely provides that where processing is based on Consent, the Data Controller must demonstrate that the Data Subject has consented and has the legal capacity to give such Consent.[30] This means the Data Subject must also have the legal capacity to give Consent and which invariably means that minors or children (words that the NDPR did not define) would be incapable of giving Consent. As noted above, NPIG is specific that, save in the instances of health emergency, national security and crime prevention, the Consent of a parent or guardian is to be obtained by a Public Institution for it to process the Personal Data of a child.

Think Time

Mr. Yusuf is an employee of Beta Life Insurance, an insurance company with different branches in Nigeria. He also runs a complimentary card printing business on the side. By virtue of his employment position with Beta Life Insurance, he has access to the personal data of clients who use the service of the insurance company. Mr. Yusuf makes copies of this personal data and proceeds to contact these clients by repeatedly sending emails and text messages urging them to patronize his complimentary card printing business. Is there any lawful legal basis for his action?

Specific Consent

1.3.8 Personal Data should not be obtained from a Data Subject except the specific purpose of collection is first communicated to the Data Subject.[31]

1.3.9 Where Consent is requested in a written declaration which contains other matters, such request for Consent should be presented to the Data Subject using clear and plain language in a manner clearly distinguishable from any other matters in such written declaration. Simply put, where the Consent of a Data Subject is to be obtained in a document which also contains other matters, such request for consent should be easily distinguishable from these other matters on such document.

[30] Article 2.3(2)(a) of NDPR.
[31] Article 2.3(1) of NDPR.

1.3.10 While NDPR states that a Data Subject can give Consent for one or more Personal Data processing activity,[32] the Implementation Framework states that there should be no bundled consent as separate Consent should be given for different use of Personal Data.[33] It expressly provides that there must be consent for different types of data uses.

1.3.11

Please note that NDPR exempts further consent where the Personal Data is to be used and processed 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.[34] Also please take note of the documentation obligations on Public Institutions where the basis of processing or the additional purpose of the use of Personal Data is for Public Interest. This was as discussed at paragraphs 1.2.21 above.

Informed Consent

1.3.12 Prior to providing his Personal Data and giving Consent, the Data Controller must inform the Data Subject of the Data Subject's rights and the method for him to withdraw his Consent at any given time.[35]

1.3.13 You may recall the Right of a Data Subject to be Informed of his Data Subject's Rights from Module 3 in the Foundation Course. Thus a Data Controller must have an explicit Privacy Policy[36] which informs the Data Subject on issues relating to his Personal Data in a form which is clearly understandable by the Data Subject. You may also recall from Modules 2 and 3 in the Foundation Course that a Privacy Policy should include, in addition to any other information, information stating:

[32] Article 2.2(a) of NDPR.
[33] Article 8.2(c) of the Implementation Framework
[34] Article 2.1 (1)(a) of NDPR
[35] Article 2.3(2)(c) of NDPR.
[36] Article 2.5 and 3.1(7) of NDPR.

1.3.13.1

all the rights of the Data Subject, that is, the rights to be informed, to consent, access, object, be forgotten, rectification, restrict processing and Personal Data portability;[37]

1.3.13.2

the purpose and or lawful basis of the processing activity; that is whether as a result of: Consent, Contract, Legal Obligation, Legitimate Interest, Public Interest or Vital Interest;[38]

1.3.13.3

the purpose and description of the Personal Data to be collected by the Data Controller. Essentially, this means that in the course of collection and processing of Personal Data by the Data Controller, such Data Controller would typically be required to inform the Data Subject of the purpose for which such Personal Data is collected and used;

1.3.13.4

what actions would constitute the Data Subject's consent. Typically, Data Controllers may state what action, if done by the Data Subject, would constitute consent. It is typical to see actions like "By providing us with your Personal Data, you hereby consent to our processing of such Personal Data" or clicking on "I Accept"/ "Ok" icons on the website as applicable;

1.3.13.5

the technical methods to be used in the collection and storage of the Personal Data, for example, cookies, JSON Web Tokens (JWT) etc.;

1.3.13.6

the identity and contact details of the Data Controller and its DPO, if any;

1.3.13.7

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;[39]

1.3.13.8

how long the Personal Data will be stored for. However, where the Data Controller cannot explicitly state the duration for which the Personal Data will be stored, it may state the criteria for which it would use to determine the duration for the storage of such Personal Data;[40]

1.3.13.9

the details of the supervisory authority, for example NITDA, for the Data Subject to lodge complaints with if the Data Subject's rights are infringed; [41]

1.3.13.10

available remedies put in place by the Data Controller in the event of violation of the Privacy Policy and the timeframe for the remedy to take place;

1.3.13.11

the existence of any limitation clause – in which case, please note that no limitation clause will avail any Data Controller who acts in breach of the NDPR; [42]

1.3.13.12

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; and

[37] Articles 2.5(a) and 3.1(7)(i) and (h) of NDPR
[38] Articles 2.5(c)(f) and 3.1(7)(c)(d)(k) and (m) of NDPR
[39] Articles 2.5(e) and 3.1(7)(e) of NDPR
[40] Article 3.1(7)(g) of NDPR
[41] Articles 2.5(g) and 3.1(7)(j) of NDPR
[42] Article 2.5(i) of NDPR.

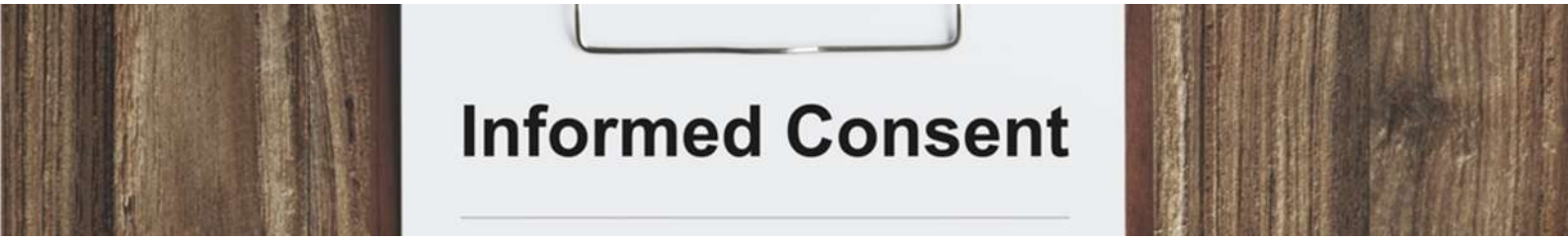
1.3.13.13

where applicable, that the Data Controller intends to transfer[44] the Personal Data to a foreign country or international organization and the existence or otherwise of an Adequacy Decision [45] by NITDA in respect of that foreign country or international organization;[46]

1.3.14 The concept of Informed Consent is of special relevance to the processing of the Personal Data of minors as both the NDPR[47] and the Implementation Framework [48] require that the Privacy Policy of the Data Controller must be communicated in a plain way that a child will understand.

Think Time

Blurredbank Plc is a commercial bank established and carrying on banking activities in Nigeria. It regularly sends out security updates to its clients via email and text messages, informing them of new updates in the Bank's system as well as security measures that have been put in place by the bank. What would you advice the Bank in the event that a customer objects to receiving such materials/updates? Would the basis of legitimate interest avail the Bank in such circumstances to the extent of overriding the objection made by the Data Subject?



[44] We shall discuss local and international transfers of Personal Data in detail in Module 5.

[45] 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.

[46] Article 3.1(7)(f)(n) and 3.1(8) of NDPR

[47] Article 3.1(1)

[48] Appendix A 4.3 of the Draft Implementation Framework

Unambiguous Indication of Consent:

1.3.15 The Implementation Framework provides that Consent cannot be implied. Accordingly, silence, pre-ticked boxes, opt-out consent or inactivity does not constitute Consent. NDPR does not recognize implied consent and accordingly, it will not suffice for a Data Controller to process the Personal Data of a Data Subject based on implied consent obtained through pre-ticked boxes, opt-out Consent and other forms of implied consent.

1.3.16 Where Consent is a legal basis on which a Data Controller intends to process the Personal Data of a Data Subject, such Consent must be requested for in an intelligible and easily accessible form and it must be clearly and explicitly given. It cannot be ambiguously inferred.

1.3.17

2.4.16 A higher form of Personal Data - Sensitive Personal Data typically requires a higher standard of Consent. Accordingly, a tick box may not suffice to indicate that a Data Subject has given his consent to the processing of his Sensitive Personal Data. Consent in the case of Sensitive Personal Data is required to be express and distinct from any form of Consent previously given or given together with it. Accordingly, where Sensitive Personal Data is to be processed, the Data Subject must give explicit consent to such processing.[50]

1.3.18

While explicit Consent from the Data Subject is one way of legitimising the processing activity on Sensitive Personal Data, there could be instances where Sensitive Personal Data needs to be processed and explicit Consent cannot be obtained. In such cases, other lawful basis for processing can be invoked.

1.3.19

In all, the obligation to obtain the valid Consent of the Data Subject is on the Data Controller as it is required to demonstrate that the Data Subject has consented to the processing of his or her Personal Data.[51]

[49] Paragraph 8.2(e) of the Draft Implementation Framework.
[50] Article 2.3(2)(a) of NDPR.
[51] Article 2.3(2)(a) of NDPR.

1.3.20 It is advisable that Consent should be the basis of last – resort upon which Personal Data processing activities are carried out by a Data Controller. This is due to the diverse arguments and circumstances under which the basis of Consent may be rebuffed. Arguments may arise on issues such as the degree of Consent given, activities covered by such Consent etc. Further, and as seen on the issues that border the freedom to give Consent and withdraw it, the Data Subject may, among his other rights, withdraw Consent at any time before, during and after a processing activity.

Consent for Public Institutions

1.3.21 Save for cases of health emergency, national security and crime prevention, Public Institutions must mandatorily obtain the Consent of the Data Subject before undertaking any of the following Personal Data processing activities:

1.3.21.1	new direct marketing or communication to a Data Subject who has not previously given Consent;
1.3.21.2	processing of Sensitive Personal Data such as race, belief, medical or sexual orientation data in which case direct, unambiguous, and distinct communication of request for Consent shall apply;
1.3.21.3	using Personal Data for a purpose other than as specified to the Data Subject;
1.3.21.4	processing of the Personal Data of a child, in which case the Consent of the parent or guardian must be obtained;
1.3.21.5	processing Personal Data outside Nigeria; and
1.3.21.6	undertaking automated processing to help in making a decision that will have legal effect on the Data Subject.

52

[52] Paragraphs 2.3, 2.4 and 2.5 of NPIG.

1.3.22 In addition to the higher standard of Consent prescribed by the Implementation Framework (which states that a tick of a box would not suffice), NPIG further states that specific Consent is required for Sensitive Personal Data. Such method includes a direct, unambiguous and distinct communication of request for Consent by any electronic means or in writing, based on the circumstances of each case. Due to the peculiarities of the information gathering process of Public Institutions, more often than not, Public Institutions process Sensitive Personal Data and would need to ensure strict compliance with this requirement.

Think Time

Imagin8 Football is a football academy that assists in the training of youngsters to become professional football players. It specifically focuses on children between the ages of 8 to 12. As part of its onboarding process, information on the children such as their gender, ethnicity, religion and genetics is recorded by the Academy. On its Privacy Policy, the Academy makes use of a lot of big words, stating that it is "scrupulous and focuses on an integration of athletics, comprehension and apprehension with the objective of forging the perfect athlete who is both erudite and vigorous". Also, the Privacy Policy has the email address and contact information of its Mr. Daniel, its head coach. Based on your understanding of Nigerian Data Protection laws, advice the Academy.

1.4 Module Summary

1.4.1 Data Controllers and Administrators are to adhere to the 6 principles of Personal Data Processing.

1..4.2 Data Controllers and Administrators are to ensure that there is at least a lawful basis for every Personal Data processing activity. Excluding Consent, the Legitimate Interest of the Data Controller is the least most attractive Lawful Basis; given the proclivity to dispute on it.

1.4.3 While Consent, as a Lawful Basis must be freely given, specific, informed and unambiguously indicated through a statement or a clear affirmative action, it is the least dependable Lawful Basis of Personal Data processing. It is advisable that Consent is combined with any other Lawful Bases.

Further Reading

1. 2019 Nigeria Data Protection Regulation[53]
2. European Union's General Data Protection Regulation[54]
3. National Information Technology Development Act 2007[55]
4. NDPR Implementation Framework[56]
5. Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 [57]

[53] Available at: http://taxtech.com.ng/download/Nigeria%20Data%20Protection%20Regulation.pdf

[54] Available at:REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (europa.eu)

[55] Available at: http://taxtech.com.ng/download/NITDA-act-2007.pdf

[56] Available at: Legislations - NDP Academy

[57] Available at: https://ndpacademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf

Case Study 1

The Prosecution of Guerin Media Limited

Guerin Media Limited is a Dublin based design and publishing agency offering print, publishing, branding, and advertising solutions. The Data Protection Commission (DPC) received unrelated complaints from three individuals about unsolicited marketing emails that they had received from Guerin Media Limited. In all cases, the complainants received the marketing emails to their work email addresses. None of the complainants had any previous business relationship with Guerin Media Limited. The marketing emails did not provide the recipients with an unsubscribe function or any other means to opt out of receiving such communications. Some of the complainants replied to the sender requesting that their email address be removed from the company's marketing list. However, these requests were not actioned, and the company continued to send the individuals further marketing emails. In one case, nine marketing emails were sent to an individual's work email address after he had sent an email request to Guerin Media Limited to remove his email address from its mailing list.

The DPC's investigation into these complaints established that Guerin Media Limited did not have the consent of any of the complainants to send them unsolicited marketing emails and that it had failed in all cases to include an opt-out mechanism in its marketing emails. The DPC had previously received four similar complaints against Guerin Media Limited during 2013 and 2014 in which the company had also sent unsolicited marketing emails without having the consent of the recipients to receive such communications and where the emails in question did not contain an opt-out mechanism. On foot of the DPC's investigations at that time, the DPC warned Guerin Media Limited that it would likely face prosecution by the DPC if there was a recurrence of such breaches. Taking account of the previous warning and the DPC's findings in its current investigation, the DPC decided to prosecute Guerin Media Limited for 42 separate breaches.

The prosecutions came before Naas District Court on 5 February 2018 and the company pleaded guilty to four sample charges out of the total of 42 charges. The Court convicted Guerin Media Limited on all four charges and imposed four fines each of €1,000, i.e. a total of €4,000. The company was given a period of six months in which to pay the fine. It also agreed to contribute towards the prosecution costs incurred by the DPC.

This case is an important demonstration that any organisation engaging in electronic direct marketing activities should carefully establish the basis on which it processes Personal Data particularly the legal basis of consent and how it can demonstrate this. The case also illustrates the importance of including an opt-out mechanism in each and every electronic direct marketing communication as failure to do so may constitute an offence, (in addition to any offences in relation to failure to obtain consent) in respect of each such email/ message.

Case Study 2

The Prosecution of AA Ireland Limited

In December 2017 the DPC of Ireland received a complaint from an individual who had received unsolicited marketing text messages from AA Ireland Limited. He informed the DPC that he had recently received his motor insurance renewal quotation from his current insurance provider and had decided to shop around to try to get a more competitive quotation. One of the companies he telephoned for a quotation was AA Ireland Limited. The complainant informed the DPC that he had expressly stated to the agent who answered his call that he wanted an assurance his details would not be used for marketing purposes and that he had been given that assurance by the agent. The phone call continued with the agent providing a quotation. The complainant noted that the quotation was higher than the renewal quotation from his current insurance provider and the complainant had indicated to the agent that he would not be proceeding with the quotation offered by AA Ireland Limited. The complainant informed the DPC that at this point in the call he had reiterated to the agent that he should not receive marketing material and he was once again assured by the agent that this would not happen.

However, a day after the phone call in question the complainant received a marketing text message from AA Ireland Limited offering him €50 off the quote provided. A further similar text message was sent to his mobile phone one day later. The complainant stated in his complaint that he felt that this action was a blatant breach of his very clear and precise instructions that he did not wish to receive any marketing communications.

During investigation by the DPC, AA Ireland Limited confirmed that it had sent both text messages to the complainant and admitted that it had not obtained consent to send these messages to the complainant. The company acknowledged that the complainant had requested that he not receive marketing messages, that the complainant's request should have been actioned and that his details should not have been used for marketing purposes. The company claimed that the incident arose because of human error. It explained that the correct process had not been followed by the agent so that the complainant's details had been recorded with an opt-in for him to receive marketing messages therefore resulting in marketing text messages being sent to him.

As the DPC had previously issued a warning in separate circumstances to AA Ireland Limited in relation to unsolicited marketing communications, in this instance the DPC decided to initiate prosecution proceedings. At Dublin Metropolitan District Court on 14 May 2018 AA Ireland Limited entered a guilty plea to one offence. It also agreed to cover the prosecution costs incurred by the DPC. In lieu of a conviction and fine, the Court applied Section 1(1) of the Probation of Offenders Act.