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 or Notice 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 or Notice 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 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 and 3.1 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 third party; [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 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.

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

[16] Article 1.3(xiv) of NDPR

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]

3.2.5 Where the Data Controller is a Public Institution, more specific rules apply on Data Subjects' rights of consent. Public Institutions cannot subject Personal Data to certain processing activities unless the consent of the Data Subject is first sought and obtained. This is regardless of the fact that other lawful basis exists for the processing activities. These processing activities include:

3.2.5.1

Tracking or tracing the Data Subject or subjecting the Personal Data to automatic or digital decisions in the absence of a Federal law to that effect;[19]

3.2.5.2

Making a new direct marketing communication to a Data Subject who has not previously given consent to such communication; [20]

3.2.5.3

Processing the Sensitive Personal Data of the Data Subject;[21] in this case, the Public Institution must make a direct, unambiguous and distinct request for the consent of the Data Subject;[22]

3.2.5.4

Using Personal Data for a purpose other than as specified to the Data Subject at the point of collecting the Personal Data; [23]

3.2.5.5

Processing the Personal Data of a child, in which case the consent of the parent or guardian of the child must be obtained; [24]

[17] Article 2.3.2(c) of the NDPR
[18] Article 2.3(2) of the NDPR
[19] Paragraph 3.1(b) of NPIG
[20] Paragraph 2.3(a) of NPIG
[21] Paragraph 2.3(b) of NPIG
[22] Paragraph 2.4 of NPIG
[23] Paragraph 2.2(h) and 2.3(c) of NPIG
[24] Paragraph 2.3(d) of NPIG

3.2.5.6 Processing Personal Data outside Nigeria;[25] and

3.2.5.7 Undertaking automated processing of Personal Data such that the decision or result to be derived from the process will have a legal effect on the Data Subject.[26]

3.2.6 Instances of health emergency, national security and crime prevention are the exceptional circumstances that a Public Institution may do away with the consent of the Data Subject.[27]

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.[28]

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.[29] 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.

[25] Paragraph 2.3(e) of NPIG
[26] Paragraph 2.3(f) of NPIG
[27] Paragraph 2.5 of NPIG
[28] Article 3.1(15) of the NDPR
[29] 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.[30] Such response includes acceding to the Data Subject's request or giving reasons why the request may not be attended to and or informing the Data Subject of his prerogative to lodge a complaint with NITDA in the event that 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.[31] 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.[32] The Data Controller has the burden of showing that the Data Subject's DSAR is unfounded or excessive.[33]

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.[34] 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.[35]

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.[36] The identity of the Data Subject should not be proven only by oral communication.[37]

3.3.8

A Public Institution cannot, without an express law to that effect, deny a Data Subject, a privilege, access or right accorded by Nigerian Law (including the right of access to Personal Data) on the basis that the Data Subject refused or failed to provide certain Personal Data to it or another Public Institution.[38]

[30] Article 3.1(2) of NDPR
[31] Article 3.1(3) of NDPR
[32] Article 3.1(3)(a) and (b) of NDPR
[33] Article 3.1(4) of NDPR
[34] Article 3.1(14) of NDPR
[35] Article 3.1(1) of NDPR
[36] Article 3.1(5) of NDPR
[37] Article 3.1(1) of NDPR
[38] Paragraph 3.1(a) of NPIG

3.3.9 Further and in relation to Personal Data processing by Public Institutions, a Data Subject cannot be denied access to judicial interpretation or redress on the use of his Personal Data. Specifically, no judicial prohibition should be sought in this regard except where it is for temporarily concealing the information of a litigant until a final decision is made on the matter by the court.[39]

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.[40]

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.[41] 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.

[39] Paragraph 3.1(c) of NPIG

[40] Article 2.8(b) of NDPR

[41] Article 2.8(a) of NDPR

Precisely, the Data Controller should delete the Personal Data, in the circumstance that the Data Subject has withdrawn his or her consent. [42]

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. [43]

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 why 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.[44] This position is further emphasised by paragraph 3.1 (b) of the NPIG which shall be considered in the paragraphs below.

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;[45]
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.

[42] Article 3.1(9)(c) of NDPR
[43] Article 3.1(11)(d) of NDPR
[44] Article 3.1(7)(l) of NDPR
[45] Article 3.1(12); Paragraph 2.5 of the NIPG

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.[46]

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.

3.6 The Right to Restrict Processing:

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

[46] 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.[47]

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.[48]

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.

[47] Article 3.1(11) of NDPR

[48] Article 3.1(15) of 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.[49] This right is typically exercised where the:[50]

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[51] 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.

[49] Article 3.1(9) of NDPR

[50] Article 3.1(11) of NDPR

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

In **Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González**,[52] the Court ordered Google Spain to delete the information it had posted regarding Mr. Gonzalez which connected him to a previously concluded legal proceeding for recovery of social security debts.

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 of his rights regarding such personal data via 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 any time.

[52] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131#t-ECR_62012CJ0131_EN_01-E0001

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 any time.

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 The right to data portability is the Data Subject's right to have his or her Personal Data transmitted from one Data Controller to another without any form of hinderance. However, this is subject to public interest and exercise of a legal duty by the Controller

3.10.8 The right to be forgotten or the right of erasure entitles Data Subjects to request Data Controllers to delete their Personal Data.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[53]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007 [54]
4. The Guidelines for the Management of Personal Data by Public Institutions (NPIG)[55]
5. Olivier G v. Le Soir 29 April 2016, n° C 15 0052 F[56]
6. Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González[57]

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

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

[55] Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf

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

[57] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131#t-ECR_62012CJ0131_EN_01-E0001