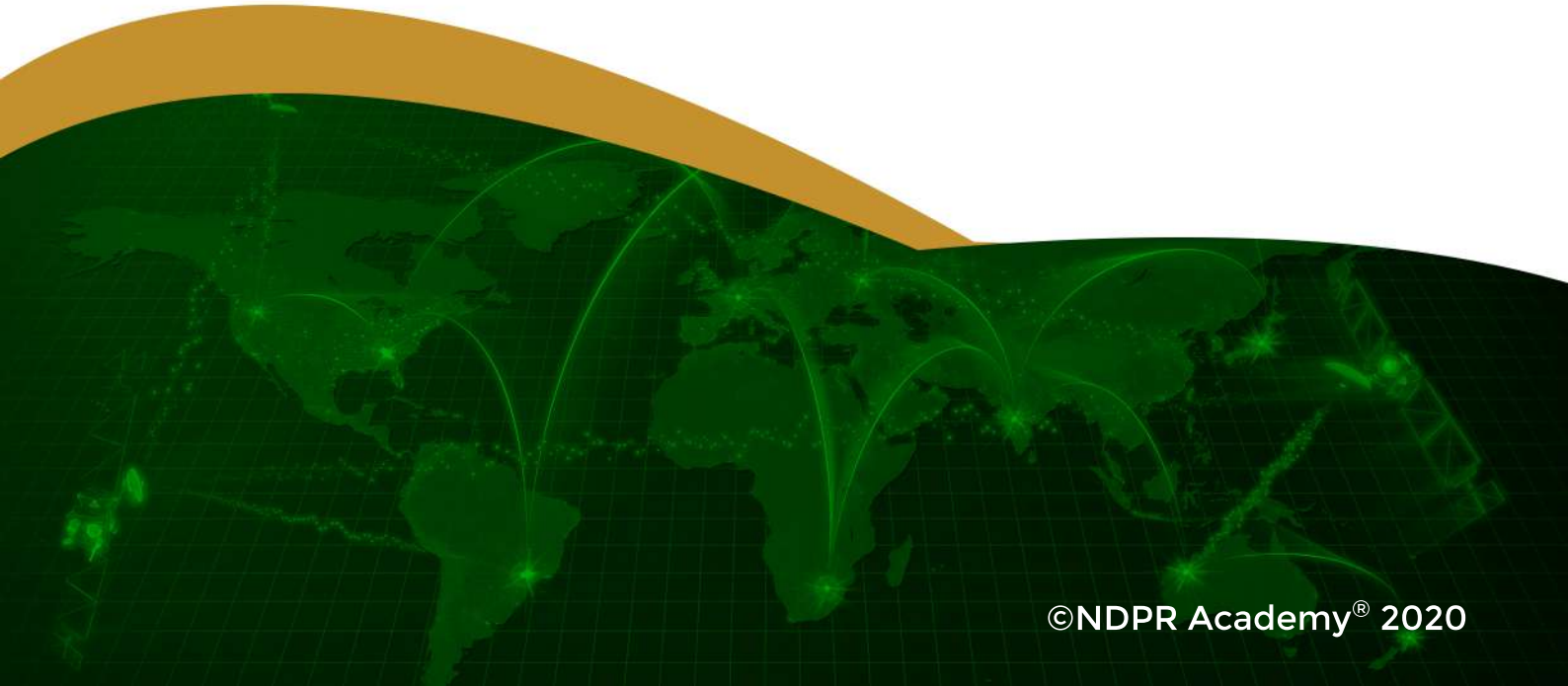
NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 5:
LOCAL AND INTERNATIONAL TRANSFERS OF PERSONAL DATA



Module 5: Overview

In this Module, we will learn about:

5.1 the requirements for the transfer of Personal Data;

5.2 the special requirements for the foreign transfer of Personal Data; and

5.3 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.

[1]Article 1.3(ii) of NDPR

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.[3] Accordingly, NDPR prohibits a Data Controller or Data Administrator from transferring Personal Data to any person except where the consent of the Data Subject is obtained without fraud, coercion or undue influence.[4] In other words, before undertaking transfer of Personal Data, the Data Controller or Data Administrator should 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 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 seventh 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.[5] 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 has an obligation to obtain the express consent of the Data Subject before transferring the relevant Personal Data to a third party for any reason whatsoever.[6]

5.1.5 There are special rules for the transfer of Personal Data where the Data Controller is a Public Institution. Please recall our definition of a Public Institution from Module 1. The NPIG provides, among others, the special rules to be observed by Public Institutions and their partners in relation to transference or sharing of Personal Data; whether from or to the Public Institution or to an approved third party. These rules include that:

5.1.5.1 Personal Data can only be shared with a Public Institution through encrypted formats or other cryptographic methods to avoid unauthorized third-party access.[7]

5.1.5.2 Further to 5.1.5.1, databases of Personal Data cannot be shared with a Public Institution through emails, hardcopies or non-encrypted or non-cryptographed formats.[8]

5.1.5.3 Data Controllers who make use of Personal Data that are of interest to Public Institutions for purposes of predictive analysis, forecasting, mapping or intelligence gathering, must anonymize or pseudonymize such Personal Data before sharing them with approved third parties.[9]

[2]Article 2.1 (1)(a) of NDPR and Paragraph 8.2(c) of the Draft Implementation Framework
[3]Article 2.3(2)(e) of NDPR.
[4]Articles 2.1(1)(a)(ii) and 2.3(2)(e) of NDPR
[5]Article 3.1(15) of NDPR
[6]Article 2.3(2)(e) of NDPR.
[7]Paragraph 4.0(b) of NPIG.
[8]Paragraph 4.0(c) of NPIG.
[9]Paragraph 4.0(e) of NPIG.

5.1.5.4 Data Controllers who possess any Personal Data of interest to a Public Institution, upon a valid request for such Personal Data by the Public Institution, are generally obligated to transfer such Personal Data to the Public Institution,[10] subject however to the Data Controller undertaking the following processes (with the exception of a request made for purposes of security or law enforcement[11]):

5.1.5.4.1 the Data Controller should evaluate the request to ensure compliance with the NPIG or seek clarification from NITDA within seven (7) days of receiving the request; and

5.1.5.4.2 providing NITDA with the following details:

a. the purpose and duration of the Personal Data processing activity;

b. the type and class of Personal Data to be shared with the Public Institution;

c. an evaluation statement showing that the request for Personal Data made by the Public Institution is in compliance with NPIG's provisions.

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).[12]

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[13] by NITDA.[14]

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:

[12]Article 1.3 of NDPR

[13]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.

[14]Article 2.11(a) of NDPR

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;

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 agreements) 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.[15]

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;

[15]See generally, the Draft Implementation Framework, available at: https://ndpracademy.ng/resources/Nigeria%20Data%20Protection%20Regulation%202019%20Implementation%20Framework.pdf.
The United States of America is limited to companies certified under the US Privacy Shield.

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 between the Data Controller and another person, and which transfer must be in the interest of the Data Subject,;

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;

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; or

5.2.5.7

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

5.2.6 Save in the cases of health emergency, national security and crime prevention, a Public Institution is required to obtain the consent of the Data Subjects before processing their Personal Data outside Nigeria.[16]

5.3 Local and International Cooperation on Personal Data Protection:

5.3.1 NITDA has a mandate to develop local and international relationships to facilitate the effective implementation of NDPR and related legislations.[17]

[15]Paragraph 2.3(e) of NPIG.
[16]Article 4.3(a) of NDPR
[17]Article 4.3(a) of NDPR

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.

5.4 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 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[18]
2. National Information Technology Development Act 2007[19]
3. NDPR Implementation Framework[20]
4. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[21]

[18]Available at: ndpracademy.ng/resources/Nigeria Data Protection Regulation.pdf
[19]Available at: https://ndpracademy.ng/resources/NITDA-act-2007.pdf
[20]Available at: https://ndpracademy.ng/resources/Nigeria%20Data%20Protection%20Regulation%202019%20Implementation%20Framework.pdf
[21]Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf