NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 4:
OBLIGATIONS OF DATA CONTROLLERS AND ADMINISTRATORS

Module 4: Overview

In this Module, we will learn about:

4.1 differences between Data Controllers and Data Administrators;

4.2 obligations of Data Controllers and Data Administrators; and

4.3 additional (stricter) obligations of Public Institutions.

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 is 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 Controller/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. This was 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 as well as Third Parties to ensure that the Data Administrators and Third Parties maintain the integrity of the Personal Data that comes into their possession. Concepts such as: staff reliability, non-disclosure agreements, training, monitoring, awareness, disciplinary procedures, et. al. must be present in the contracts.

[1]https://ndpracademy.ng/resources/Google%20Spain%20SL,%20Google%20Inc%20v%20AEPD%20and%20Mario%20Costeja%20Gonzalez.pdf

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 or a Third Party 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.[2] 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; and

4.2.6.5 nature of Personal Data shared, etc.

4.3 Obligations of Public Institutions:

4.3.1 Stricter and more stringent obligations are now placed on Data Controllers that are Public Institutions and as well on other Data Controllers and Data Administrators that process Personal Data for or with Public Institutions. This is by virtue of the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[3] (NPIG) which NITDA released on Monday, May 18, 2020.

[2]Article 2.7 of NDPR
[3]Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf

4.3.2 These stricter obligations touch on such subjects as: Lawful Basis (which we dealt with in Module 2 and will not be dwelling on again here); Privacy Policy; and Data Security We shall be re-discussing the latter two in the two succeeding paragraphs.

Privacy Policy of Public Institutions:

4.3.3 Every Public Institution that processes Personal Data must have a widely publicized Privacy Policy containing provisions as prescribed by the NDPR. Recall our discussions on the Privacy Policy in Module 3. The Privacy Policy must be easily accessible to those who use or are affected by the Public Institution's service. Accordingly, the Privacy Policy should be available on the Public Institution's website, digital media, conspicuous parts of its business premises or published in any public media, including by reading it to Data Subjects.[4]

Data Security Architecture and Processes of Public Institutions:

4.3.4 Public Institutions that process Personal Data are mandated to establish information security architecture and processes to assure the security and protection of the privacy of Data Subjects. This can be demonstrated by any and or all of the following NPIG-required data security specific measures and processes:

4.3.4.1

compliance with international information security standards such as the ISO 27001:2013 or any similar standard;[5]

4.3.4.2

ensuring that all Personal Data databases are digital databases with restricted or controlled access – NPIG gave Public Institutions up until Friday, July 17, 2020 to achieve this;[6]

4.3.4.3

mandatory sharing of Personal Data through encrypted formats or other cryptographic methods that protect Personal Data from being easily accessible by unauthorised third parties[7]– in this regard, NPIG prohibits databases from being shared through emails, hard copies and any other file format; and

4.3.4.4

Anonymization or pseudonymization of all Personal Data to be shared with third parties who have a legal basis for their processing;[8]

Data Controllers that Process Personal Data for Public Institutions:

4.3.5 Data Controllers who do business with Public Institutions are not spared from data security obligations in relation to their purposed processing activities as they are required to create separate encrypted platform to process such Personal Data. They are prohibited from granting access to the backend of such databases except for criminal investigation by a law enforcement agency or in obedience to a judicial order.[9]

[4]Article 2.9 of NPIG
[5]Paragraph 2.6(a) of NPIG.
[6]Paragraph 4.0(a) of NPIG.
[7]Paragraph 4.0(b) and (c) of NPIG.
[8]Paragraph 4.0(e) of NPIG.
[9]Paragraph 4.0(d) of NPIG.

4.3.6 Such Data Controllers who do business with Public Institutions also have due diligence obligations on any requested processing activity. As mentioned under Module 2, where a request is made to a Data Controller to process Personal Data on behalf of any Public Institution, it shall evaluate such request to ensure compliance with the NPIG or seek clarification from NITDA within 7 days of receipt of such request. Where it is satisfied that the request to process data meets the requirement set out in the NDPR and NPIG, it must file a report with NITDA stating the following:[10]

4.3.6.1 the purpose and duration for each processing activity;

4.3.6.2 the type and classes of Personal Data to be shared; and

4.3.6.3 an evaluation statement showing that the request complies with provisions of the NPIG.

4.4 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
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.

4.5 Module 4: Summary

4.5.1 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.

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

Further Reading:

1. 2019 Nigeria Data Protection Regulation[11]
2. **Google Spain SL and Google Inc. v. AEPD and Mario Costeja Gonzalez**[12]
3. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[13]

[10]Paragraph 5.0(c)(i) of NPIG.
[11]Available at: https://ndpracademy.ng/resources/Nigeria Data Protection Regulation.pdf
[12]Available at: https://ndpracademy.ng/resources/Google%20Spain%20SL,%20Google%20Inc%20v%20AEPD%20and%20Mario%20Costeja%20Gonzalez.pdf
[13]Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf