NDPR ACADEMY

NDPR Academy® Foundation Course

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

Module 6: Overview

In this Module, we will learn about, the:

6.1 the compliance requirements under the NDPR

6.2 Data Protection Audits (DPAs); and

6.3 Data Protection Impact Assessments (DPIAs).

6.1. The NDPR Compliance Requirements:

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

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

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

6.1.1.3 All Data Controllers or Administrators must appoint a DPCO;

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

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

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

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

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

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

6.2. Data Protection Audits:

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

6.2.2 You may recall our engagement of the concept of the DPCO from Module 2 where we defined a DPCO as any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with NDPR or any foreign data protection law or regulation having effect in Nigeria.[6] Accordingly, a major purpose of DPCOs is the conduct of DPAs on Data Controllers and Data Administrators.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signature License Number Date

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

6.3 Data Protection Impact Assessments:

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

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

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

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

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

6.3.2.4 Sensitive Personal Data will be processed;

6.3.2.5 the Data Subjects are vulnerable persons;

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

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

6.3.3.1 description of the envisaged Personal Data processing activities;

6.3.3.2 purpose of the processing activity;

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

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

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

6.3.3.6 mitigation measures being proposed to address the

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

6.4 Definitions of Common Terms in Module 3:

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

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

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

6.5 Module 6: Summary

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

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

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

Further Reading:

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

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

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

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