NDP ACADEMY

MODULE 5:

DATA PROTECTION COMPLIANCE AUDITS

Module 5: Overview

In this Module, we will learn about:

5.1. The nature and objectives of DPCAs;

5.2. DPCA Methodology: Checklist and Report; and

5.3. Post-DPCA Report Issues: Audit Recommendations

5.1 Nature and Objectives of DPCA:

5.1.1 You may recall from the Foundation Course (Module 6), some of the Data Controller or Data Administrator's compliance requirements under the NDPR; particularly the requirement to undertake a Data Protection Compliance Audit (DPCA) and file the DPCA Report with NITDA within the timelines specified by the NDPR and NITDA.

5.1.2 A DPCA is an audit, inspection and review of a Data Controller's policies, processes, and procedures to assess the Data Controller's compliance with the provisions of the NDPR and related directives of NITDA. The DPCA Report is the expected product of a DPCA.

5.1.3

From our engagement in Module 2 of the Foundation Course, you may recall the concept of the DPCO 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[1].

[1] Article 2.4(a) of NDPR

5.1.4 Accordingly, one of the major roles of the DPCOs is the conduct of DPCAs on Data Controllers and Data Administrators. While a DPCA may be conducted by a data protection professional who is not a licensed DPCO, however, due to the requirements of the NDPR, the audit report of such person cannot be filed with the regulatory authority, NITDA. This is because NITDA issues licenses to eligible organisations to act as DPCOs, which essentially confers such licensed organisations with the authority to conduct audits and file the resulting audit report with NITDA.

5.1.5

The categories of companies which are eligible to apply for a Data Protection Compliance Organisation license include – IT Service Providers, Law firms, Audit firm, Professional Service Consultancy firm and must have evidence of professional, academic certification or experiences in the following areas:

a. Data Science
b. Data Protection and Privacy
c. Information Privacy
d. Information Audit
e. Data Management
f. Information Security
g. Data Protection Legal Services
h. Information Technology Due Diligence
i. EU GDPR Implementation and Compliance
j. Cyber Security/ Cyber Security Law
k. Data Analytics
l. Data Governance

A firm, including its subsidiary or agent which engages in providing financial audit for a Data Controller is prohibited from acting as a Data Protection Compliance Organisation for such Data Controller.

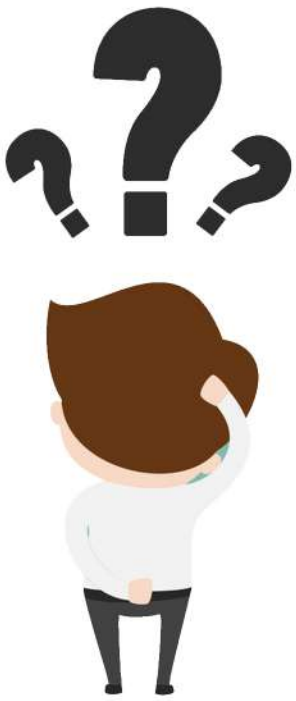
5.1.6. As you may recall, under the NDPR all Data Controllers or Administrators that processed the Personal Data of more than 1,000 Data Subjects within 6 months from January 25, 2019, must undergo and file, through their DPCO, an Initial DPCA Report with NITDA not later than July, 25, 2019. This was subsequently extended by NITDA to 25 October 2019. The Initial DPCA Report was to be filed by Data Controllers through their respective DPCOs in 2019 alone and therefore is no longer applicable. Thus, Data Controllers are required to file the Annual Data Protection Compliance Audit Report which will be discussed shortly.

[1] Article 2.4(a) of NDPR

5.1.7 Furthermore, all Data Controllers or Administrators that annually process the Personal Data of more than 2,000 Data Subjects, must undergo and file, through their DPCOs, Annual DPCA Reports with NITDA not later than March 15 of the following year. This statutory deadline is usually extended by NITDA, and currently has been extended to June 30, 2022 for the 2021 audit period. The foregoing compliance requirements are illustrated in the table below:

Number of Data Subjects	Compliance Requirements	Timeline
≥ 1,000	Filing of Initial Data Protection Audit Report	October 25 2019
≥ 2,000	Filing of Annual Data Protection Audit Report	March 15 of every year. Currently extended to June 30th 2022.

5.1.8 In addition to the statutory reports mentioned above, some practitioners have developed the concept of an Interim DPCA Report. The Interim DPCA Report is a temporary filing done by a Data Controller who is still undergoing a DPCA and wishes to apply for an extension of time for filing the Annual Data Protection Report. This report is usually filed when it is foreseeable that a Data Controller will not be able to meet up with the deadline imposed by NITDA for filing the DPCA Report.



Think Time

Black Lion Bank is a newly incorporated bank and currently controls Personal Data of about 1,600 Data Subjects. The bank wishes to comply with the provisions of the NDPR as it relates to DPCA and DPCA Report filing with NITDA for year 2020. The Bank estimates that by 1st day of March 2021, it shall have processed the Personal Data of about 1,900 Data Subjects. As a DPCO, kindly advise on the compliance issues under the NDPR.

[2] Paragraph 2.8 of NPIG
Paragraph 1.2 of NPIG

5.1.9 It is necessary to reiterate that the Interim DPCA Report is not provided for by the NDPR. It however serves as a measure of temporary compliance pending the completion of the Annual DPCA and filing of the Annual DPCA Report. The Interim DPCA is filed in order to reduce a Data Controller's risk or exposure of non-compliance with the NDPR particularly the requirement of conducting a data protection audit and filing the report therefrom with NITDA. The Interim DPCA Report among other things states a timeline within which the Annual DPCA process will be completed and the final Annual DPCA Report filed with NITDA.

5.1.10 Public Institutions are mandated to retain the services of DPCOs who will, among other Personal Data protection services, undertake the conduct of DPCAs on them. Government at all levels have been identified as one of the largest set of Data Controllers in Nigeria. NPIG was established to ensure the safety of Personal Data while undergoing processing by the Public Institutions. Accordingly, Public Institutions are also required to carry out DPCAs in compliance with the NDPR to ensure the consistent security, confidentiality and integrity of Personal Data and Data Subjects.

5.1.11 A DPCA is carried out for any or all of the following reasons, to:

5.1.11.1 comply with the provisions of the NDPR - NDPR provides for instances where a DPCA is required to be carried out and filed with NITDA. In this regard, an audit is done in order to comply with those provisions;

5.1.11.2 assess (through a Gap Analysis methodology) the Data Controller's level of compliance with the requirements of the NDPR by reviewing relevant DPCA Documentations such as policies, contracts, processes, practices and procedures of the Data Controller in order to determine its level of compliance;

5.1.11.3 further to the assessment, the conduct of a DPCA, through the recommendations, also assists the Data Controller to further its compliance with the NDPR. This is done through review and amendment of relevant documents, contracts, processes and policies to meet up with the NDPR's required standards.

5.1.11.4	discover vulnerabilities in the Data Controller's system which are susceptible to data breaches. In the course of a DPCA, the DPCO or auditor reviews and assesses the internal documentation and procedures of the Data Controller as they relate to the processing of Personal Data including the Data Controller's security systems. Policies such as Data Protection Policy, Information Security Policy etc are reviewed and where there are vulnerabilities in the processes which expose the Data Controller to risks of data breaches, such vulnerabilities are raised and recommendations on how to handle them are documented.

Think Time

Asgard Technologies, a multinational company in the telecommunications sector has approached you as a Data Protection Compliance Organisation (DPCO) in order to comply with the NDPR's requirement for the filing the Company's Annual Data Protection Audit with NITDA. However, you look at your calendar and alas, it is the 20th of June and it would be difficult to conduct and conclude the Company's Audit Report and file same with NITDA within the deadline. What would you do as a DPCO? What do you think are the objectives of a DPCA?

5.2. The DPCA Methodology: Checklist + Report

The DPCA Checklist:

5.2.1 A DPCO will typically commence the DPCA process by administering a DPCA Checklist or Questionnaire on the Data Controller. NITDA has provided a template DPCA Questionnaire for this purpose.[4] It is necessary to note that the template DPCA Questionnaire serves only as a guide and may be modified in so far as the essence of the DPCA is sufficiently achieved.

5.2.2

DPCA Questionnaires and the entire DPCA process have also been automated by some companies such as Taxaide Technologies Ltd (Taxtech)[5] and its proprietary automated DPCA platform known as iDAP®[6]. Platforms like iDAP® are designed to guarantee time and cost efficiency and effectiveness for Data Controllers and DPCOs throughout the DPCA process. Accordingly, Data Controllers as well as DPCOs may register on the iDAP® to efficiently carry out their DPCAs.

5.2.3 Based on the Data Controller's responses to the DPCA Questionnaire, the supporting documents and or other information referenced in the completed DPCA Questionnaire are provided to the DPCO for review and assessment. Interviews may be held with relevant personnel of the Data Controller in order to clarify any issues or enquiries which may arise in the course of reviewing any and all of the completed DPCA Questionnaire, the supporting documents and or other information provided by the Data Controller to the DPCO.

5.2.4 Supporting documentations and or information that are typically reviewed in the course of a DPCA include but are not limited to:

5.2.4.1

Biodata form used for collecting personal data from customers, employees and vendors

5.2.4.2

Privacy Policy

5.2.4.3

Information Security Policy

5.2.4.4

Disaster Recovery Policy

[4] Appendix A of the Draft Implementation Framework.
[5] www.taxtech.com.ng
[6] iDAP® can assessed at any of: www.idap.taxit.com.ng; www.ndpr.ng; www.ndpr.nitda.gov.ng.

5.2.4.5 Data Retention Policy

5.2.4.6 Data Breach Incident Management Policy

5.2.4.7 Data Protection Policy

5.2.4.8 Human Resource Policy

5.2.4.9 Data Breach Register Template

5.2.4.10 Data Subject Access Request Policy

5.2.4.11 Data Subject Access Request Register

5.2.5 Where software such as iDAP® are not being used,[7] other tools that could come handy in the DPCA process include a Gap Analysis Tool[8] and a Process Analysis Tool.[9]

5.2.6 A Gap Analysis Tool is used to measure the Data Controller's current compliances with the requirements of NDPR. Areas covered by a Gap Analysis Tool include:

5.2.6.1

Governance: Awareness of the need to address the NDPR within the corporate structure, DPA/NDPR compliance oversight (nomination of accountable/director/senior management member, regular update of company leadership on NDPR compliance).

5.2.6.2 Risk Management: the following questions need to be addressed under risk management:

5.2.6.2.1

Is the NDPR risk (fines and legal actions) on the corporate risk register?

5.2.6.2.1

Does the internal control framework include privacy risk?

[7] Most of the functionalities of the tools to be discussed have been programmed into a software such as iDAP®.
[8] Taxtech®'s Gap Analysis Tool can be assessed at:
[9] Taxtech®'s Process Analysis Tool can be assessed at:

5.2.6.3 The NDPR Project: the following questions are relevant under this sub-theme:

5.2.6.3.1

is there a project team in the Data Controller for its NDPR compliance efforts?

5.2.6.3.2

does the project team have necessary knowledge and training?

5.2.6.3.3

does the project team have Management Support?

5.2.6.3.4

what are the efforts towards meeting the NDPR compliance deadline?

5.2.6.4 The Data Protection Officer (DPO): with regards to the DPO, the following issues need to be addressed:

5.2.6.4.1

does the DPO have the required independence?

5.2.6.4.2

does the DPO have direct access to top Management?

5.2.6.4.3

is the DPO adequately resourced to perform his or her function?

5.2.6.4.4

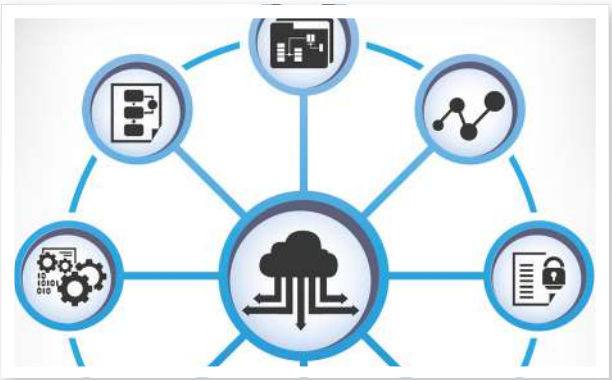
does the DPO have knowledge of the NDPR?

5.2.6.4.5

is the DPO informed and up to date with current developments regarding Personal Data protection?

5.2.6.5 The Rights of Data Subjects: this subtheme deals with how the Data Controller facilitates the exercise of Data Subject Rights and the procedure and technologies in place that enables the organization respond to the exercise of Data Subject Rights.

5.2.7 The Process Analysis Tool maps the entry and exit points of Personal Data within the Data Controller to determine the potential areas of risk and attribute the level of risk to each Personal Data processing activity. In order to ensure compliance with the NDPR, a Process Analysis Tool must detail the following:



5.2.7.1 key business processes;

5.2.7.2 type of Data Subjects;

5.2.7.3 number of departments within the Data Controller that use or access Personal Data;

5.2.7.4 Personal Data processing map;

5.2.7.5 the organisation's status (e.g. Data Controller or Data Administrator);

5.2.7.6 type of Personal Data collected and the format of collection;

5.2.7.7 access control within the Data Controller;

5.2.7.8 transfer of Personal Data within and outside the Data Controller or outside Nigeria;

5.2.7.9 automated processing;

5.2.7.10 Lawful Basis for processing Personal Data;

5.2.7.11 confirmation if the appropriate Privacy Notices have been put in place;

5.2.7.12 Data Controller's practices and process with regards to: Specificity, Adequacy, Accuracy, Storage and Security.

5.2.8 Supporting documentation and or information must be thoroughly reviewed by the DPCO as the DPCO has the obligation to ensure a professional audit process and verify the eventual DPCA Report to be filed with NITDA. A DPCO that is found to be unprofessional, for example, concealing the breaches of the NDPR by a Data Controller is liable to lose its license and prior reports made by it may be subject of investigation.[10]

In order to avoid such liability, DPCOs are required to review the Data Controller's documentation and or information and verify the DPCA Report.

5.2.9

Upon the DPCO's review and assessment of all of the completed DPCA Questionnaire, the supporting documents, other information provided by the Data Controller to the DPCO, and the internal practices and process of the Data Controller as may be established through the interview sessions, the DPCA Report will be prepared by the DPCO.

Think Time

Bronxx Company Limited, a fashion design company established in Nigeria has heard about the Nigerian Data Protection Regulation and wishes to be compliant and has approached you in this regard. Upon preliminary assessment, you discover that the Company processed the Personal Data of 995 Data Subjects in 2019. What type of report would the Company as Data Controller be required to file with NITDA?

10 www.nitda.gov.ng/data-protection-criteria/

The DPCA Report:

5.2.10 The DPCA Report details the Data Controller's Data Protection practices. NITDA's minimum requirements [11] of a DPCA Report are:

5.2.10.1

Identification of the category of Personal Data which a Data Controller processes and the relevant groups of Data Subjects that own the Personal Data;

5.2.10.2

The processing activities carried out on the Personal Data; ranging from its collection, use, transmission to eventual deletion;

5.2.10.3

The purpose for which such Personal Data are processed; in other words, the Lawful Basis for all of the categories of processing activities carried on the Personal Data. As you may recall from Module 2 of the Foundation Course (Principles of Personal Data Processing), each category of processing activities must have a Lawful Basis. Where there is no Lawful Basis, there should be no Personal Data processing. Any Personal Data processing carried on without a Lawful Basis is a breach of the NDPR.

5.2.10.4

The Privacy Notices given to Data Subjects on the processing or intended processing of their Personal Data, including the manner in which the Privacy Notices are administered. For example, the Data Controller is required to put up a notice at every point of collection of Personal Data indicating the reason for collection of such Personal Data as well as the rights of the Data Subjects on the processing of their Personal Data.

5.2.10.5

Any access given to Data Subjects to review, amend, correct, supplement, or delete their Personal Data which is in the possession of the Data Controller. You may recall in Module 3 of the Foundation Course (Rights of Data Subjects) that one of the rights of the Data Subject is the right to review, amend, correct, supplement or delete his or her Personal Data being processed by the Data Controller, assuming Consent or Contract is the basis of the processing.[12] Accordingly, DPCOs are to indicate as part of the DPCA Report, the medium through which Data Subjects are able to exercise their Data Subject Access Rights (DSAR).

[11] Article 4.1 (5) (a-j) of the NDPR
[12] Article 3.1 (7) (h) of the NDPR

5.2.10.6

Where Consent is the basis of a processing activity, details on whether or not such Consent are obtained from Data Subjects before Personal Data is collected, used, transferred or disclosed to any third party. The method by which such Consent is obtained from the Data Subject must also be stated.

5.2.10.7

Details on the internal policies and practices of the Data Controller which have been put in place for:

5.2.10.7.1	the security, confidentiality and integrity of Personal Data in the Data Controller's possession;
5.2.10.7.2	the proper use and processing of Personal Data in order to ensure that such processing activity is in compliance with the provisions of the NDPR;
5.2.10.7.3	ensuring regular and consistent monitoring and timely reporting of violations of privacy and data protection policies;
5.2.10.7.4	assessing the impact of technologies on the Data Controller's privacy and security policies.

5.2.11 As a precondition to filing a Report, a DPCO is required to attach a verification statement made under oath to the Audit report. The statement is as follows:

p µ @ã 9 À µ @ã 9 À
@ ã 9 À
µ @ ã æ µ @ã æ
@
æ µ À @
9 µ @ã æ
µ À @
9 ã @

î þb µ ¨þ9 Hµ î H µ ı ³ 8 Hæ @ üH

Upon completion of the DPCA Report, it is necessary for the DPCO to have a close-out meeting with the Data Controller in order to address the performance gaps and discuss the recommendations before filing with NITDA.

Think Time

Mr. Green, the CEO of GreenWich Hotels and Resorts, a hospitality company processing the Personal Data of over 250,000 (Two Hundred and Fifty Thousand) Data Subjects yearly has approached you. He has read about the Nigeria Data Protection Regulation and wishes to be compliant to avoid any sanctions. He desires that a Data Protection Compliance Audit be done on the Company and has requested for a step by step guide on how the audit process will be done. Advice Mr. Green in this regard.

5.3 Post-DPCA Report Issues: Audit Recommendations

5.3.1 It is good practice for a DPCO to assist the Data Controller document all the gaps, processes and documentation challenges of the Data Controller as observed by the DPCO during the DPCA process. This typically comes by way of DPCA Recommendations that the DPCO may privately share with the Data Controller.

5.3.2 The DPCA Recommendations may typically contain the gaps of the Data Controller as established from the Gap Analysis Tool and Process Analysis Tool. iDAP® also generates Recommendations as part of its output, picking out areas of non-compliance and proffering recommendations to address those areas. Ultimately, all DPCA Recommendations indicate areas of non-optimal compliance or gaps which the Data Controller, whether with or without the DPCO, should remediate.

5.3.3 Part of the engagement of a DPCO may include the DPCO assisting the Data Controller to implement the DPCA Recommendations. Accordingly, the DPCO may assist the Data Controller in revising documents – policies, contracts, plans etc. to ensure the Data Controller's compliance with the NDPR.

5.3.4

The Data Controller is to take appropriate steps in ensuring that the recommendations as proffered by the DPCO are implemented to the greatest extent possible. Where it has any difficulty, the Data Controller may reach out to the DPCO for assistance in order to ensure that it is compliant with the NDPR and other relevant data protection regulations.

5.3.5 The DPCO may also provide general advisory and implementation support to the Data Controller in order to ensure that the internal practices of the Data Controller as it relates to Data Protection are in compliance with the NDPR as well as other applicable legislation.

5.3.6

The DPCO may also assist the Data Controller in ensuring compliance by providing relevant toolkits such as DPIA Toolkit, DSAR Registers, Compliance Assessment Tools etc to the Data Controller where necessary.

5.3.7

The Data Controller may further ensure compliance by coordinating regular training sessions for its employees particularly its DPO as well as employees who by the nature of their job description are responsible for handling Personal Data.

5.3.8

It is recommended that a DPCO also regularly follows up with the Data Controller in order to monitor and assess the level of implementation of the DPCA Recommendations.

Think Time

You have filed an Annual Data Protection Audit Report for Brownstone Bank, a commercial bank who has just recently heard of the NDPR. From the audit, you identified a number of areas of non-compliance in the Bank as regards Data Protection and also proffered recommendations on how these areas of non-compliance may be addressed. After filing, what are the steps you are to take as a DPCO to ensure that the recommendations are implemented by the Data Controller?

5.4 Module Summary

5.4.1 Data Controllers are required to file their DPCA Reports for the previous year with NITDA on or before the 15th of March every year. Failure to carry out such filings would typically attract sanctions to the Data Controller.

5.4.2 It is worthy of mention that only a licensed DPCO is allowed to carry out Data Protection Compliance Audits and file same with NITDA within the required timeline.

5.4.3 A DPCA Report is required to contain certain information including but not limited to – Policies on security of Personal Data, methods of obtaining the consent of a Data Subject by the Data Controller, legal basis for the processing activities done on Personal Data by the Data Controller, access by the Data Subject to review, delete, supplement his Personal Data in the Data Controller's possession etc.

5.4.4 All DPCA Reports regardless of whether Initial, Interim or Annual are required to contain statements sworn on oath by the DPCO.

5.4.5 A Data Controller, after the DPCA Report has been filed by a DPCO is to take steps to implement the suggested recommendations proffered by the DPCO in the course of the audit in order to ensure compliance with the requirements of the NDPR as well as subsequent regulations on Data Protection in Nigeria.

Further Reading

1. 2019 Nigeria Data Protection Regulation[13]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007[14]
4. Data Protection Implementation Framework
5. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020[15]

[13] Available at: http://taxtech.com.ng/download/Nigeria%20Data%20Protection%20Regulation.pdf
[14] Available at: http://taxtech.com.ng/download/NITDA-act-2007.pdf
[15] Available at: https://ndpacademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf