NDP ACADEMY

NDP Academy® Practitioner Course

MODULE 6:

DATA PROTECTION IMPACT ASSESSMENTS

Module 6: Overview

In this Module, we will learn about:

6.1. the nature and objectives of DPIAs;

6.2. NITDA's DPIA requirements;

6.3. DPIA Methodology: Checklist and Report; and

6.4. implementing your DPIA Report.

6.1 Nature and Objectives of a DPIA:

6.1.1 6.1.1. Personal Data protection is a risk-based subject, meaning that amongst its other objectives, its primary focus is on the security and integrity of the Personal Data of Data Subjects, with particular focus on mitigating any risks that may arise from the daily processing of this Personal Data by Data Controllers. Data Controllers have an overarching responsibility to protect the Personal Data that they process. Where they are not adequately protected, especially in accordance with standards, guidelines, regulations or laws set up for such purpose, the Data Controller becomes liable not only under the extant standards, guidelines, regulations or laws, but also to the Data Subject, especially where the rights of the Data Subject are thereby breached or the security of the Personal Data is thereby compromised. To avoid or mitigate such risks is the crux of Personal Data protection.

6.1.2 It is within the context of the statements above that, concepts such as identifying the risks – the threats to and likely impact of such threats – to Personal Data, becomes highly relevant to Data Controllers. This is the foundation of DPIAs – to assess the risks to Data Subjects and the Personal Data being processed by Data Controllers.

6.1.3 A DPIA is a risk assessment carried out by a Data Controller to evaluate and discover the possible risks associated with its processing activities on the Personal Data of its Data Subjects. It is a systematic analysis of a Data Controller's data processing activities and processes in a bid to discover and minimise to the greatest extent possible, any risk associated or arising from such processing activity. It is an assessment done to ascertain the possible implication of the proposed processing activity on the Personal Data protection compliance obligations of the Data Controller.[1]

[1]Paragraph 7.2 of the Draft Implementation Framework.

6.1.4 There is no limit to the type of risks a DPIA is designed to identify and minimise. Accordingly, risks should not be limited to a data breach incident which may lead to loss or exposure of Personal Data. The risks envisaged by a DPIA extends to cover risks associated with non-compliance with relevant data protection legislation as well as any risk which is likely to affect the Data Subjects and the public in general.

6.1.5 Accordingly, where a Personal Data processing activity has a likely high risk to the rights of Data Subjects being breached or the security of Personal Data being compromised, the Data Controller should, prior to undertaking the processing activity, carry out an assessment of the impact of the proposed processing activity on the rights of Data Subjects and the security of their Personal Data.

6.1.6 The examples of such high risk Personal Data processing activities are not closed and include the following:

6.1.6.1 processing of Sensitive Personal Data;

6.1.6.2 processing of the Personal Data of children or other vulnerable individuals for marketing purposes;

6.1.6.3 processing of Personal Data that expose the Data Subject to harm in the event of a breach;

6.1.6.4 using new technologies (especially the intrusive ones) to process Personal Data;

6.1.6.5 tracing, tracking or systematic monitoring of Data Subject's locations or behaviour;

6.1.6.6 profiling Data Subjects in order to decide their rights to services;

6.1.6.7 profiling a large scale of Data Subjects;

6.1.6.8 embarking on new projects that would involve the intense use of Personal Data;[2] and

6.1.6.9 processing by Public Institutions of Personal Data that are validly with another statutory body.[3]

6.1.7 Generally, it is recommended that DPIAs are conducted for proposed processing activities that have not been risk-assessed. This is particularly important for processing activities with attendant high risk to Data Subject Rights and or Personal Data Security. Relatedly, where there is a proposed change in the nature or scope of a processing activity that a DPIA has been conducted on, a new DPIA on the processing activity should again be carried out on the proposed new nature and scope of processing activity.

[2]Paragraphs 4.2(vii) and 7.2 of the Draft Implementation Framework.
[3]Paragraph 3.2.(a) of NPIG.

Think Time

Asger Technologies Limited is a software development company. Due to the COVID 19 pandemic, the Company is working on a software application which will allow users to communicate online with other users of similar religious orientation. The application will also allow for video conferencing of up to 100 persons. When registering for the application, information obtained include – name, address, location, religion, email address and phone number. The application is made such that it automatically categorizes users according to their religious orientation as indicated during registration. As the DPO to Asger Tech, do you think the Company will need to carry out a DPIA for this new application? Why?

6.2 NITDA's DPIA Requirements:

6.2.1 You may recall from the Foundation Course (Module 6) that NITDA, under the NDPR, has certain compliance requirements of Data Controllers. The conduct of a DPIA is not one of those set out under the NDPR as the NDPR itself does not expressly provide for the instances where a DPIA is required.

6.2.2 The Implementation Framework however states that DPIA is not compulsory although it may be required for the processing activities earlier discussed.[4] In other words, and under the Implementation Framework, a DPIA may be required by NITDA from a Data Controller as it sees fit.

6.2.3 It is noteworthy however that the template Data Protection Compliance Audit Questionnaire at Appendix A of the Implementation Framework highlights the requirement of Data Controllers having a DPIA Policy in place.[5] While such a DPIA Policy may require a Data Controller to conduct DPIA in appropriate circumstances, this differs from saying it is a mandatory compliance requirement by NITDA.

[4]Paragraph 7.2 of the Draft Implementation Framework.
[5]Questions 1.17 and 1.18 in the Data Protection Compliance Audit Questionnaire at Appendix A of the Draft Implementation Framework.

6.2.4 This is not the case with Public Institutions who are mandatorily required to undertake DPIAs where they intend to process Personal Data with another Data Controller. Such other Data Controller may be another Public Institution, a private entity, an international organisation or another statutory body.[6]

6.2.5 The DPIA by a Public Institution is required to be undertaken through a DPCO. The DPCO will after undertaking the DPIA and generating the DPIA Report file the DPIA Report with NITDA. NITDA has 15 working days from the date of submission of the DPIA Report to give its feedback on it.[7]

6.2.6 Save for the NPIG which lays the statutory requirement for Public Institutions to undertake DPIAs, the DPIA Policy would be the fallback document that basically sets out the policy statements of the Data Controller on the circumstances that it will conduct DPIAs and how it will conduct them. Accordingly, a Data Controller is expected to have a DPIA Policy.[8]

6.2.7 It is accordingly safe to conclude that while only Public Institutions are statutorily required to conduct DPIAs, it is advisable for non-Public Institutions to still form the habit of undertaking DPIAs seeing, the:

6.2.7.1
underlying positive risks management philosophy that forms the bedrock of DPIAs; and

6.2.7.2
possibility that NITDA may still require that a DPIA be conducted.[9]

6.3 DPIA Methodology: Checklist + Report:

The DPIA Checklist:

6.3.1 A DPO or DPCO will typically commence its DPIA process by administering a DPIA Questionnaire or Checklist on the Data Controller or the relevant functions of the Data Controller's organization that will be embarking on the processing activity which is the object of the DPIA.

[6]Paragraphs 2.6(c) and 3.2.(a) of NPIG.
[7]Paragraph 3.2.(a) of NPIG.
[8]Questions 1.17 and 1.18 in the Data Protection Compliance Audit Questionnaire at Appendix A of the Draft Implementation Framework.
[9]Paragraph 7.2 of the Draft Implementation Framework.

6.3.2 The DPIA Questionnaire or Checklist will broadly contain request for information and documents such as those bordering on, the:

6.3.2.1

description (name, nature, scope, size, context, necessity, Lawful Basis and proportionality) of the proposed Personal Data processing activity;

6.3.2.2

nature of the threats, vulnerabilities, likelihood and impact of identified risks on the proposed Personal Data processing activity; and

6.3.2.3

control or security measures (if any), designed in the project as to mitigate the identified risks – including the level of awareness of the leadership of the Data Controller and direct project stakeholders of the issues in 6.3.2.2.

6.3.3 On receiving the duly filled Questionnaire, the DPO or DPCO is to carefully vet the responses given with the supporting documentations provided so to ensure consistency in documented processes and the reality of the project. Where there are inconsistencies, they must be highlighted, and due clarifications from the Data Controller must be sought and recorded. It is this analyses and verification process that ultimately leads to the generation of the DPIA Report.

The DPIA Report:

6.3.4 The DPIA Report is a formal document prepared by the Data Controller or its DPCO. A Public Institution that intends to process Personal Data that is being processed by a statutory organization is required to prepare a DPIA Report, through a DPCO, and submit with NITDA.[10]

6.3.5 The DPIA Report[11] will essentially contain the following headers and contents:

6.3.5.1 **Processing Activities:** which details the purpose, nature, context and Lawful Basis of the Personal Data processing activities;

[10]Paragraph 3.2(a) of NPIG.
[11]A DPIA template is available at https://ndpracademy.ng/resources/DPIA-template

6.3.5.2 **Risks:** which is a detailed assessment of the Risks (Threats and Vulnerabilities) that the processing activities will pose to Data Subjects Rights and Personal Data Security;

6.3.5.3 **Comparative Assessment:** which is a necessity and proportionality assessment of the processing activities and the inherent Risks of such processing.

6.3.5.4 **Controls:** which states the measures, safeguards, security and mechanisms to mitigate and or avoid the Risks and to demonstrate compliance with the NDPR and other relevant Personal Data protection laws.

6.3.6 The DPIA Report will after adequately describing the processing activities determine the risks which may arise as a result of the processing activities. The risks should be considered in relation to the likelihood of occurrence as well as the impact such risks may have on the Data Controller, the Data Subject and even the public. The impact could range from inability to exercise rights or to access services, loss of control over use of Personal Data, theft, loss (unavailability), or loss of Personal Data confidentiality or integrity (accuracy) etc.

6.3.7 Such impact may be categorized using numbers to determine severity

(1 - Low, 2 - Medium, 3 - High, 4 - Very High).

Also, the likelihood of the occurrence may be characterized using numbers to determine the probability of occurrence

(1- Very Unlikely, 2 – Unlikely, 3 – Likely, 4 – Very Likely).

6.3.8 The numbers are used in order to measure and determine the risk level associated with a type of Personal Data alongside the processing activities to be carried out on it. Risk acceptance is calculated by multiplying Likelihood and Impact:

Likelihood x Impact = Risk.

6.3.9 To assess and determine instances of high risk, it is recommended that both the likelihood and severity of the impact of such possible risk be considered. Upon this assessment by the Data Controller, it is recommended that the outcomes be recorded and risks which are necessary for the project are recorded as well.

6.3.10 Where a risk is discovered in the course of the assessment, the source of such risk should be recorded before considering which options may be best suited to mitigate the risk. Measures that may be established include implementation of further security measures, limiting the collection of Personal Data, training staff for appropriate handling of Personal Data, anonymisation, pseudonymization, encryption, change in technology, change of internal policies, increase in Personal Data protection awareness, etc.

6.3.11 The DPO or DPCO should take note of issues such as:

6.3.11.1 additional control or security measures for the safeguard of Data Subjects Rights and Personal Data Security;

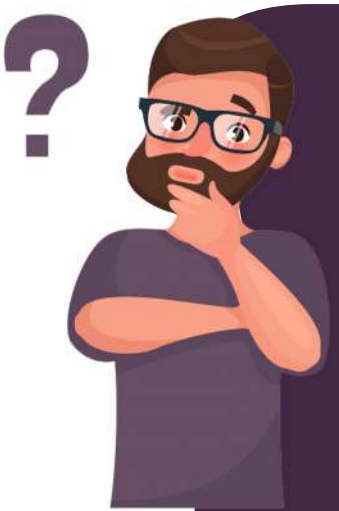
6.3.11.2 residual risks after implementation of the additional control or security measures;

6.3.11.3 where risks were eliminated, reduced or accepted, it becomes important to know what exactly it is that the measures to be implemented will achieve.

6.3.12 Where there is a high-risk project, it is recommended that the Data Controller gets appropriate additional advice from its DPO or DPCO before implementing the project. DPOs or DPCOs are to advice where it is possible to continue with the high-risk project and give recommendations on additional control or security measures where necessary. Where it is not advisable to proceed with the project, especially where the risks outweigh the benefits or necessity for the project, they should advice accordingly.

6.3.13 Public Institutions are required to submit their DPIA Reports to NITDA through their DPCOs. Accordingly, the DPIA Report process of a Public Institution is incomplete until its DPCO files the DPIA Report with NITDA.[12]

Think Time



OneWorld Foundation (the Foundation) is a charity organisation which caters to homeless children as well as the mentally-challenged. The Foundation is working with its parent Company, OneWorld Technologies Ltd (OTL) to develop an application which will be linked to a trust account for all its beneficiaries in order to efficiently and timeously cater for their housing, clothing, education and feeding. You have just recently been appointed OTL's DPO. Do you think a DPIA is required for this new application? Why? In the event that you consider that a DPIA is required, what steps will you take in conducting the DPIA? What would be the content of the resulting DPIA Report?

[12]Paragraph 3.2(a) of NPIG.

6.4 Implementing your DPIA Report

6.4.1 The aim of a DPIA is not always the total elimination of risk but its mitigation and management. The aim of a DPIA is mainly to reduce the level and likelihood of the occurrence of such risk to a level which is acceptable to the Data Controller while still allowing for the implementation and execution of a lawful project.

6.4.2 When implementing the project for which the DPIA was conducted, it is advisable that the Data Controller takes steps to:

6.4.2.1 integrate the outcomes of the DPIA as well as recommended measures (altogether, the DPIA Report) into the project plan; and

6.4.2.12 monitor the progress of the project in relation to the results of the DPIA.

6.4.3 There should be a periodic review of the DPIA Report to ensure that it is still relevant to the processing activities of the Data Controller. As stated earlier, where there are any changes to the nature, scope, purpose and Lawful Basis of the Personal Data processing activity, a new DPIA be conducted by the Data Controller.

6.4.4 In the case of Public Institutions, NITDA has an obligation to consider the Public Institution's DPIA Report, submitted through a DPCO, and provide a feedback within 15 (*fifteen*) days of NITDA receiving the DPIA Report.[13] It is expected that NITDA's feedback will give further insights on the post-DPIA Report processes that the Public Institution will undertake.

[13]Paragraph 3.2(a) of NPIG.

Think Time

Deluxe Interactive Limited (DIL) won the contract from Nigeria's National Communications Commission (NCC) and the Office of the National Security Adviser (ONSA) to provide a robust application (GodHears®) for the monitoring of the voice and data communications of some persons within Nigeria. DIL requested both NCC and ONSA to commission a DPIA for the GodHears® project. Only the NCC agreed to the DPIA and instructed DIL to commission a DPCO for the purpose. DIL retained the services of your Company (a DPCO) to undertake the DPIA. You now have the final DPIA Report in your hands. The Report majorly highlights the following:

a. GodHears® is a high-risk project as the application will be collecting, monitoring and analysing the private communications of an estimated 10 million persons, most of whom have no prior record of wrongdoing.

b. GodsHears® has become necessary in view of the rise in organized terrorism in Nigeria.

c. GodsHears® will be hosted on a cloud server owned by a service provider that is based in Athens, Greece.

d. The operatives who will be working with GodsHears® will be seconded to DIL from both the NCC and ONSA.

What will be your next steps?

6.5 Summary

6.5.1 A DPIA is a risk mitigation process that Data Controllers are encouraged to embrace as part of their overall risk management framework.

6.5.2 The aim of a DPIA is not the total elimination of a risk, rather it is the mitigation of a risk to the greatest extent possible while allowing for the implementation of a lawful project.

6.5.3 While other Data Controllers are advised to have a DPIA Policy in place and conduct DPIAs, Public Institutions have an obligation to undertake DPIAs where they intend to process Personal Data that are in the possession of another Data Controller.

6.5.4 The DPIA process involves, the:

6.5.4.1 administration of Checklists or Questionnaires on the Data Controller or relevant stakeholders of the proposed project to elicit information and documentation;

6.5.4.2 vetting of all information and documentation to ensure consistency;

6.5.4.3 generation of the DPIA Report which essentially is the DPO or DPCO's assessment of the risks (the likelihood and impact of Threats and Vulnerabilities), given the analyses of the responses from the Checklists and the vetted information and documentation.

6.5.5 Upon conclusion of the DPIA, where the project is assessed to be a high-risk project, the DPO or DPCO should advise on the measures to be put in place to mitigate the risks. A DPO or DPCO should also advise where it is unadvisable to proceed with the project.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[14]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007[15]
4. Draft NDPR Implementation Framework
5. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[16]

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