NDP ACADEMY

NDP Academy® Practitioner Course

MODULE 4:

THE DATA PROTECTION OFFICER

Module 4: Overview

In this Module, we will learn about:

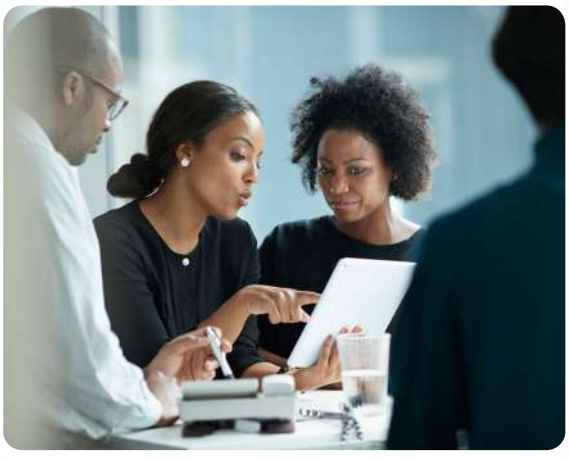
4.1. the Rationale for the Office of the DPO; and

4.2. NITDA's requirements for a DPO: Role, Duties and Obligations.

4.1 The Office of a Data Protection Officer (DPO)

4.1.1. The DPO is the cornerstone of Personal Data protection accountablity in a Data Controller's organisation. Although now a requirement of legislation, the office of the DPO gradually evolved from the Personal Data protection practices of the EU Member States in compliance with the Directive 95/46 EC that heralded the EU GDPR.[1] Thus, being a product of practice or common sense, some Data Controllers who appreciate the risks that good Personal Data protection practices seek to mitigate, still see the need to have a DPO, whether internally or outsourced, even if extant legislation does not mandatorily require it.

4.1.2. A part of the Data Controller's organisation, the DPO facilitates relevant Personal Data protection communication among the key stakeholders in the Personal Data protection regime; they are, the Data Subject, the Data Controller and the Regulator, for example NITDA. Given the objectivity of Personal Data protection requirements, the DPO naturally must be an objective institution within the Data Controller's organisation; speaking truth to power!



[1]See https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (last visited on Monday, June 22, 2020).

4.1.3. Accordingly, independence, judgement, objectivity and accountability are core features of the office of the DPO. The office is for every stakeholder in the Personal Data protection regime, and for no stakeholder in particular. This feature requires that the office of the DPO must be specially protected within the Data Controller's organisation to do its work. This fact has led some Personal Data protection regimes, for example, in the EU, to create special rules for the governance of the office.

4.1.4. Aside legislation and given the history of the role as one that evolved from good Personal Data protection practices, the Data Controller must also appreciate the essence of the office of the DPO from a risk management governance perspective. The office exists to derisk Personal Data protection practices and compliance in the Data Controller's organisation. Accordingly, the DPO may, subject to the Data Controller's organisational structure, sit within any of the risk management, internal audit, compliance, governance or functions of the Data Controller's organisation; however with a clear and direct line to the leadership of the Data Controller.

4.1.5. The DPO is expected to be independent and have the ability to work with critical business functions such as: Information Communication Technology (ICT), Human Resources (HR) Sales, Information Security Team, if different from the IT team. All importantly, the DPO is to ensure data protection is a regular feature in the discussions of the highest governance apparatus of the Data Controller.

4.1.6. More developed Data Protection regimes require that the office of the DPO should have direct access of communication to the Board of Directors' level in a bid to ensure that Personal Data protection risks are frontally handled and not stuck up in the daily functional processes of the Data Controller. Today, the office of the DPO may not be a person but an organisation to which the Data Controller outsources the function. This should not detract from the requirement that the DPO must have direct access to the Data Controller's leadership.

Think Time

Blakebank PLC is a commercial bank in Nigeria looking to implement best practices in Personal Data protection and compliance with the NDPR. On the agenda of its 54th Board of Directors' Meeting is "Engagement of a DPO". Being considered is the employment of a candidate with extensive experience in Personal Data protection in the EU. This option comes at a considerably higher cost. Dr. Malik, a Board Member and a lawyer interjects and says the Bank does not need to spend money in hiring a new DPO, seeing that the Company Secretary who is there present at the meeting, taking the Minutes, is suited for the job, with her long years of service to the Bank and understanding of its business. According to him, "no one can better protect this Bank than the Company Secretary who is a lawyer. She will protect us better than any new person. Let us add DPO to her designation and give some additional remuneration for the function". What do you consider wrong with Dr. Malik's submissions? Do you think the Bank needs an EU experienced privacy professional for its data protection compliance objective? Would your answer be different if the Company Secretary had successfully passed the NDPR Academy® Practitioners' Course?

4.1.7. A Data Controller has the obligation to provide adequate resources necessary to support the DPO to carry out his tasks, have access to Personal Data and processing operations and also maintain his expert knowledge.[2] The DPO must be prevented from undue influence in performing his tasks. The Data Controller should ensure that the DPO does not receive any instructions regarding the exercise of his tasks.[3] Accordingly, the DPO should not be dismissed or penalised by the Data Controller for performing his tasks. He should directly report to the highest management level of the Data Controller or Processor.[4]

4.2. NITDA's Requirements for a DPO: Role, Duties + Obligations

4.2.1. Similar to the EU GDPR, the NDPR has created the role of the DPO. It however makes it mandatory as it provides that every Data Controller shall designate a DPO, whether internally or outsourced, for the purpose of ensuring adherence to the NDPR, other privacy laws and the data protection directives of the Data Controller.[5]

[2]Article 38 (2) of the EU GDPR
[3]Article 38 (3) of the EU GDPR
[4]Article 38 (3) of the EU GDPR
[5]Article 4.1(2) of NDPR.

4.2.2 It is necessary to mention that the Implementation Framework provides for a category of Data Controllers who are expected to have dedicated a DPO. These category of Data Controllers include:

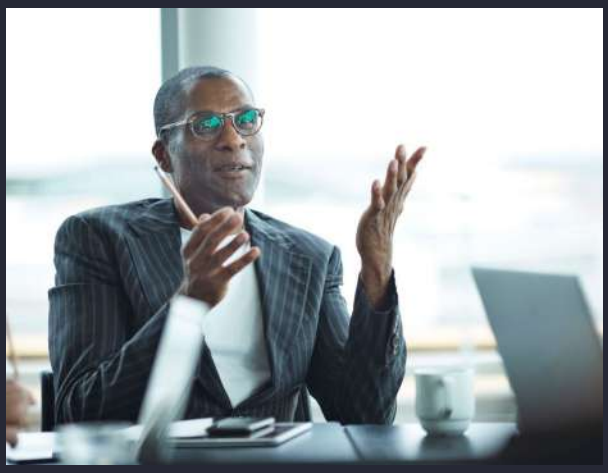
4.2.2.1 Government organ, ministry, department, institution or agency – the mandatoy requirement for Public Institutions to have DPOs has become operational;[6]

4.2.2.2 Data Controllers whose core activities require the processing of large sets of Personal Data;

4.2.2.3 Data Controllers that process Sensitive Personal Data in the regular course of their business; and

4.2.2.4 Data Controllers that process critical national databases consisting of Personal Data.[7]

4.2.3 Please note that the foregoing requirement of the Impementation Framework does not detract from the fundamental obligation under the NDPR to designate a DPO. However, Data Controllers who fall under the category listed in paragraph 4.2.4 are expected to have a dedicated DPO as opposed to Data Controllers outside that category who have the flexibility of combining the role of DPO and other job functions provided there is no conflict of interest.



4.2.4 A Data Controller may outsource the DPO function to a verifiably competent firm or person not directly in the employ of the Data Controller. Such firm or person need not be a DPCO.

4.2.5 All Public Institutions in Nigeria are required to have DPOs not later than Sunday, August 16, 2020.[9] The DPO of a Public Instituion is required to:

4.2.5.1 be a senior level officer in the Public Institution;

4.2.5.2 be trained within 90 days of his appointment in the general principles and management of Personal Data;

4.2.5.3 understand the Personal Data processing activities in the Public Institution and interpret the roles of each operational unit in Personal Data protection;

[6]Paragraph 2.6 of NPIG
[7]Paragraph 3.2 of the Implementation Framework.
[8]Article 4.1 (2) of NDPR
[9]Paragraph 2.6(a) of NPIG

4.2.5.4 develop an appropriate Personal Data implementation plan for the Public Institution and get Board and Management buy-in to it;

4.2.5.5 report directly to and advise the Public Institution's Management on the practices that could trigger Personal Data breaches;

4.2.5.6 inculcate data protection culture in the Public Institution by constantly training and developing the capacity of staff, licensees, contractors and stakeholders of the Public Institution on Personal Data protection and management;

4.2.5.7 avoid any activity which would be prejudicial to his judgement or advice to the Public Institution on Personal Data protection management; and

4.2.5.8 be assisted by other Public Officers with certification, knowledge and experience in law, data protection and privacy, information technology, cybersecurity and related fields.[10]

4.2.6 While the EU GDPR exempts courts acting in their judicial capacity from appointing a DPO,[11] NDPR however does not make any distinction between courts and other Public Institutions.

Think Time

Select whether a dedicated DPO is required or not for the following Data Controllers according to the NDPR, the NDPR Implementation Framework and the NPIG:

1. Ministry of Health
2. Kepsy (A beverage production Company)
3. Central Bank of Nigeria
4. NAFDAC
5. Independent National Electoral Commission
6. University of Nigeria, Nsukka
7. Chicken Republic
8. Christian Association of Nigeria
9. Beckers Gas Station
10. National Identity Management Commission
11. National Youth Service Corps

4.2.7 The duties of a DPO requires him or her to have expertise and sufficient knowledge of Personal Data protection issues. While these qualifications are not expressly listed by the NDPR, a DPO must be a verifiably competent person. It invariably follows that a DPO must have requisite understanding of relevant data protection legislation at every point in time in order to ensure that the Data Controller is consistently compliant.

[10]Paragraph 2.6 of NPIG
[11]https://gdpr-info.eu/issues/data-protection-officer/

4.2.8 Where appointing a DPO, it is essential that a Data Controller carries on background checks to ensure that there would be no conflict of interest on the part of the proposed DPO. Accordingly in the event where a Data Controller wishes to combine the role of the DPO with another role within its structure, it is recommended that an evaluation be carried out between the expected obligations of the DPO and the current job functions of the personnel to be appointed as DPO to ensure that such job functions would not interfere with his responsibilities as a DPO.

4.2.9 The Data Controller or Administrator has the obligation of ensuring consistent and regular training for the DPO and other employees as the NDPR expressly provides for this when it states that a Data Controller or Administrator shall ensure continuous capacity building for its DPOs and the generality of its personnel involved in any form of data processing. These regular trainings will serve to ensure that the DPO has an updated knowledge of any recent development regarding Data Protection in Nigeria in order to further advise and take steps to ensure that the Data Controller is compliant at all times with the current provisions of Data Protection legislation in Nigeria.

4.2.10 The regular training is also to sensitize both the DPO and employees who have access to Personal Data on the proper handling of such Personal Data in a bid to reduce the risk of the occurrence of a breach incident in the course of data processing as well as any liability which could arise from such breach. DPCOs are given the obligation to, among other things, carry out trainings on compliance with relevant data protection regulations which are in place at every point in time. It is recommended that Data Controllers ensure that their DPOs and relevant personnel who are responsible for the regular handling of Personal Data are exposed to these trainings.

4.2.11 Articles 37 and 38 of the EU GDPR provides for the instances where a DPO is required to be designated by an organisation and what can be described as the minimal job description of the DPO. The Data Controller or Processor is mandated to ensure that a DPO is involved in all issues relating to the protection of Personal Data in a proper and timely manner. This means that the DPO should not be left out in any business activity or plan which will involve the processing of Personal Data including data protection audits and data protection impact assessments. He is to be involved in all plans to process Personal Data as he is well versed in the provisions of relevant data protection legislation and would be in the best position to advice the Data Controller on compliance with relevant legislation before, during and after the processing of Personal Data.

[12]Article 4.1(3) of the NDPR
[13]Article 38 (1) EU GDPR

4.2.12 Data Subjects are allowed to contact the DPO with regards to all issues related to the processing of their Personal Data and to the exercise of their rights under this Regulation.[14] Although the NDPR does not expressly provide for this, this is implied as the NDPR provides that a Data Controller among other things shall provide the contact details of its DPO in its Privacy Policy.

4.2.13 While the EU GDPR provides that a group of undertakings may appoint a single DPO, the NDPR is silent on this. Therefore, it is not inconceivable that a conglomerate of organisations with a group structure in Nigeria may have a single DPO. That said, it must be borne in mind that the Implementation Framework states that a DPO based in Nigeria must be appointed within a multinational structure for the purpose of compliance with the NDPR.[15]

4.2.14 We summarise the foregoing duties and obligations[16] of the typical DPO as follows :

4.2.14.1 inform and advise the Data Controller, management, employees and third parties who undertake Personal Data processing activities of their obligations;

4.2.14.2 monitor compliance with the relevant data protection legislation and with the internal policies of the organization and ensure that these policies are drafted to guarantee the security, integrity and confidentiality of Personal Data and Data Subjects;

4.2.14.3 organize awareness sessions and training of staff generally and particularly personnel who at any point in carrying out their responsibilities have access to and handle Personal Data. Such trainings are done in order to reduce the risk of the occurrence of a data breach and even where such breach has occurred, to mitigate the impact and substantially reduce the probability of it occurring again. The trainings are also done in order to comply with the provisions of the NDPR which makes provision to the effect that employees of a Data Controller who for any reason and at any point in time have access to Personal Data are to undergo training and capacity building;[17]

[14]Article 38 (4) EU GDPR
[15]Article 3.3 of the NDPR Implementation Framework
[16]Article 15 of the Implementation Framework and Article 39 of the EU GDPR.
[17]Article 4.1 (3) of NDPR

4.2.14.4

provide guidance and direction in the event of a data breach incident and advice the Data Controller on steps to be taken to mitigate the effect of such breach and prevent any further breach in the future. Prior to the occurrence of a breach, it is essential that a Data Controller has policies in place which will guide the organisation in the event of a breach incident. It is advisable that a DPO be involved in the drafting and approval of such policies and should also be conversant with the provisions of these policies so as to properly guide the Data Controller in the event of a breach incident;

4.2.14.5

undertake internal investigation of the Personal Data breaches including assigning responsibilities to other personnel in the course of mitigating the impact of a breach. Data Controllers generally have policies which deal with data breach incidents such as Disaster Recovery Plan, Data Protection Policy, Data Breach Incident Response etc. These policies basically guide the organisation on steps to be taken in the event of a breach, particularly in the aspect of gathering a response team. In this regard, a DPO would have the responsibility of assembling a Data Breach Response Team and assigning roles and responsibilities to the members of the team based on skill set with the aim of efficiently mitigating such data breach;

4.2.14.6 facilitate the cooperation of the Data Controller with relevant stakeholders and acting as point of contact with NITDA. The DPO also acts as a liaison with the regulatory body as well as with DPCOs where necessary. In the event of a breach incident for instance, a DPO would be necessary particularly when determining whether the incident is of a degree which would warrant making a report to the regulatory authority. Furthermore, during investigations by NITDA, the DPO may be the main representative of the Data Controller in such circumstances. A DPO would also aid the Data Controller in determining whether the breach incident as well as the Personal Data involved is of a degree as would make it necessary to contact the respective Data Subjects to inform them of the breach incident; and

4.2.14.7 be the contact person in the event of a report or complaint by a Data Subject. The details of a DPO must be included in the Data Controller's Privacy Policy.[18] Due to his knowledge of the provisions of data protection legislations as well as the rights of Data Subjects provided therein, a DPO would be in the best position to respond to Data Subjects who have reports or complaints.

[18]Article 3.1 (7) (b) of NDPR

Think Time

You have just been selected to fill in the position of a DPO in your organization. What duties would you typically be required to carry out by virtue of this position?

Do you think it would be necessary to contact you in the event of a data breach incident? Yes No

Would you in your capacity as a DPO be required if there is a natural disaster and your office building collapsed? Yes No

Do you think it would be necessary for a Data Controller to include a DPO when preparing a Data Protection Impact Assessment Policy?

Yes No

4.3 Summary

4.3.1 A DPO is an essential position in the organisation of a Data Controller. He or she aids in ensuring that the organisation is consistently compliant with relevant data protection legislation in force at any given period of time.

4.3.2 The NDPR generally does not mandate all Data Controllers to have a DPO. However, it provides for instances where a DPO is required as a necessity. These instances include among others – where the Data Controller is a government body, ministry, department or agency, where it handles sensitive personal data in the ordinary course of its business activities, where it handles large sets of personal data etc.

4.3.3 It is essential that a DPO is well versed in relevant Data Protection legislation as this would enable him effectively carry out his duties and ultimately keep the Data Controller in compliance with the relevant Data Protection laws.

4.3.4 Some of the duties of a DPO includes advising the Controller on establishing internal procedures and processes in compliance with relevant data protection legislation, reviewing documents and policies to ensure that such are in line with relevant data protection provisions, acting as a contact person between the Data Controller and the

4.3.5 It is essential that a Data Controller provides adequate support to the DPO in order to carry out his obligations efficiently and effectively. Accordingly, a Data Controller is to provide sufficient access to the DPO to documentation, processes, policies and procedures of the organisation for review and assessment of the compliance level of the Data Controller in this regard. The Data Controller is also to provide adequate support and budget necessary for the DPO to carry out his functions efficiently.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[19]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007[20]
4. Data Protection Implementation Framework
5. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020[21]

[19]Available at: http://taxtech.com.ng/download/Nigeria%20Data%20Protection%20Regulation.pdf
[20]Available at: http://taxtech.com.ng/download/NITDA-act-2007.pdf
[21]Available at : https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf