NDP ACADEMY

MODULE 2:

RIGHTS OF DATA SUBJECTS: DSAR IN FOCUS

Module 2: Overview

In this Module, we will learn about:

2.1 the Data Subject's Right of Access;

2.2 the Data Subject Access Request (DSAR); and

2.3 setting up and implementing a DSAR system

2.1 The Data Subject's Right of Access

2.1.1. You may recall from the Foundation Course (Module 3), the 8 Rights of Data Subjects recognised under the NDPR. These are the rights:

[1]Regulation 3.1(7) and 2.5 of NDPR.
[2]Regulation 1.3 (xiv) and 2.3.2(c) of NDPR.
[3]Regulation 3.1 (15) of NDPR.
[4]Regulation 2.8(b) of NDPR.
[5]Regulation 3.1(7)(h) of NDPR.
[6]Regulation 3.1(11) of NDPR.
[7]Regulation 3.1(15) of NDPR
[8]Regulation 3.1(9) of NDPR

2.1.2. 2.1.2. In this Module, we shall be examining in greater detail the Data Subject's right of access and the process for exercising this right under the NDPR. To give some context, violations of the right of Data Subjects to access their Personal Data is one of the singular more popular infractions of the rights of Data Subjects globally. In other words, Data Controllers and Data Administrators easily fall prey to the infraction of Data Protection regulations such as the NDPR on account of their failure to respect and comply with Data Subjects' rights of access. The essence of this module is to extensively discuss the concept of the Data Subject Access Request, the processes involved and compliance requirements which are provided by the NDPR for Data Controllers to follow.

2.1.3. Simply put, the Data Subject's right of access is the Data Subject's right to contact the Data Controller or Data Administrator to confirm whether or not his Personal Data is being processed, what Personal Data is being processed as well as what processing activities are being conducted on such Personal Data (recall we discussed Personal Data processing in Module 2 of the Foundation Course). Where the Personal Data is being processed, the Data Subject may, particularly where consent is the lawful basis for the processing activity, exercise some of his other rights including to:

2.1.3.1.

obtain a copy of the Personal Data from the Data Controller or Data Administrator;

2.1.3.2.

verify the lawfulness or otherwise of the processing activity;

2.1.3.3.

where the lawful basis for the processing is wholly-based on consent, withdraw the consent;

2.1.3.4.

object to the processing activity especially where the Data Controller or Data Administrator has no overriding legitimate grounds to base the processing activity;

2.1.3.5.

restrict the Data Controller or Data Administrator from carrying out any further processing activity on the Personal Data;

2.1.3.6.

request the Data Controller or Data Administrator to rectify any error on the Personal Data;

2.1.3.7.

request the Data Controller or Data Administrator to transfer the Personal Data to another Data Controller; or

2.1.3.8.

request the Data Controller to delete the Personal Data.

[9]https://www.pinsentmasons.com/out-law/news/business-fined-after-data-subject-access-request-failings

2.1.4. Instances may arise where the relevant Personal Data was not provided to the Data Controller or Data Administrator by the Data Subject; in such instances, some further considerations must be had on the extent of the Data Subject's right of access to his Personal Data.

2.1.5. NDPR neither made exceptions nor created assumptions on the obligation of Data Controllers to provide information to Data Subjects on the processing of their Personal Data. The information must be provided by the Data Controller to the Data Subject, whenever requested by the Data Subject, in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[10]

2.1.6. The obligation to provide information is expressly laid on Data Controllers, in which case, it is arguable that a Data Administrator will not be laden with same obligation in the event of a request from a Data Subject. Typically, a Data Administrator holds the Personal Data of the Data Subject at the Data Controller's behest. it is recommended that a Data Administrator should appropriately, in the first instance, contact the Data Controller for relevant authorisation whenever it receives a request for information from the Data Subject. It is expected that the Data Administrator should duly remind the Data Controller of the Data Controller's statutory obligation to provide the information to the Data Subject.

2.1.7. It is noteworthy that the Data Controller and Data Administrator may ultimately both be liable if the Data Subject's right of access is breached. It is expected that both the Data Controller and Data Administrator should have settled relevant agreements between themselves on the allocation of responsibility and indemnities in the event of a breach of the rights of the Data Subject to his information.

[10]Regulation 3.1(1) of the NDPR

2.1.8. It is therefore recommended that Data Controllers, before appointing a Data Administrator should evaluate such Data Administrator, particularly on the information security measures such Administrator has in place in order to confirm that such measures meet up with globally acceptable standards and are sufficient to guarantee the safety, confidentiality, security and integrity of Personal Data. Furthermore, it is advisable that Data Controllers also ensure the general compliance of such Data Administrators before contracting with it and subsequently transferring Personal Data.

2.1.9. Upon confirmation of a Data Administrator's compliance with the requirements of the relevant data protection laws applicable, it is further recommended that the Data Controller and Data Administrator put a contract (such as a Data Processing Agreement) in place which would serve to regulate their relationship as regards the processing of Personal Data. Such Data Protection contracts serve to guide the parties in their relationship with each other. Such agreement would include clauses on the allowed processing activities which the Data Administrator is allowed to conduct – this clause is typically restricting in its language as a Data Administrator is restricted to certain processing activities, being prohibited from conducting any processing activity which is not authorised by the Data Controller. Other typical clauses in such contracts are indemnity clauses etc.

Think Time

Core Business Limited is a service provider that assists corporate businesses in developing and maintaining their corporate activities as well as the retention of clients. Among its various obligations, Core Business Limited assists in printing business cards for its clients. It obtains information such as name, phone number, email address, corporate office address of the employees of its clients and transfers them to Bodmas Printing, who designs and prepares these cards. Dele, the CEO of GenTech which is a client of Core Business Limited just got his business cards back and observed that his name, phone number and email address as indicated on the card are wrong. He intends to contact Bodmas Printing to request for his Personal Data which they hold. Advice Bodmas Printing as its DPO on how to respond to Dele.

2.2. Data Subject Access Requests

2.2.1. A Data Subject exercises his right of access through a regulated eponymous process known as the DSAR – Data Subject Access Request. DSAR is statutorily defined as a mechanism for an individual to request for a copy of their data under a formal process and payment of a fee.[11] It is simply the means by which the Data Subject's right of access is exercised. We shall in this part of this Module, examine the process in a very practical manner.

2.2.2. The Data Subject is entitled to the following information from the Data Controller or Data Administrator when requesting for access to his Personal Data; they are information on the:

2.2.2.1 *purpose of the processing activities performed on his Personal Data;*

2.2.2.2 *categories of Personal Data being processed;*

2.2.2.3 *categories of third-party recipients if any;*

2.2.2.4 *period for which such Personal Data will be stored or the criteria used to determine such period; and*

2.2.2.5 *existence of his right to rectify, erase, object, restrict the processing of his Personal Data.*

[11]Regulation 1.3(l) of NDPR

2.2.3. Upon a Data Subject making an access request, the Data Controller is mandated to provide the Personal Data to the Data Subject in a structured, concise, commonly-used, transparent, intelligible and machine-readable format using clear and plain language.[12] The information requested by the Data Subject may be provided by the Data Controller to the Data Subject in writing or by any other means including electronically.[13] Theinformation may be provided in a combination with standardized icons in order to give a meaningful overview in an easily visible, intelligible and clearly legible manner. This is particularly important where the Data Subject is a child. It is essential that when providing the requested Personal Data to the Data Subject, the Data Controller should ensure that the format by which such Personal Data is provided is easily understood by the Data Subject as the NDPR specifically provides for this requirement.[14] There is however no test specified by the NDPR to determine what standard would suffice as easily accessible but we reckon that this requirement is subject to the test of reason, as to whether an ordinary person may without difficulty access such information.

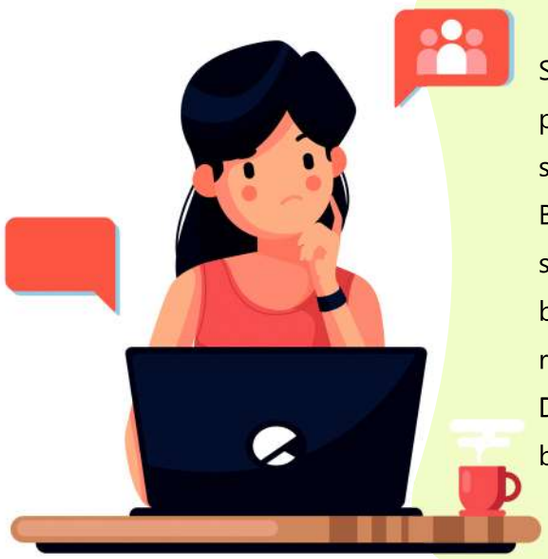
2.2.4. Only where requested by the Data Subject can the information be provided orally. The identity of the Data Subject should however be established by other verifiable means other than orally, for example, by the Data Subject providing the Data Controller with an identity card or other means of verification, including by administering security questions on the Data Subject.[15]

2.2.5. The Data Controller has the responsibility of satisfying itself of the identity of the Data Subject before responding to a DSAR. Where the Data Controller has reasonable doubts concerning the identity of the natural person making the request for information, the Data Controller will be within its right to request such person to provide such additional information as the Data Controller may require to satisfy itself that the person is the Data Subject. The identity of the Data Subject should not be proven only by the oral account of the person but should be appropriately confirmed or verified as stated above.[16]

2.2.6. The NDPR also recognizes that Data Subject Access Requests may be made by a third-party representative or agent of the Data Subject. This is provided in the questionnaire to the Implementation Framework where it asks “Do you have a procedure for dealing with subject access requests from third parties?”. The procedure for handling a Data Subject Access Request (which will be discussed subsequently) is very similar to the procedure for handling a request from a third party. It is advisable that in such event, Data Controllers should request such third party to provide a means of communication from the relevant Data Subject, this should be in a written format. Such evidence should be accompanied by a means of identification of such third party before a response to the request is made by the Data Controller. Where it is confirmed that such third party is acting on the authority of the Data Subject, the Data Controller may then proceed to initiate its process for addressing a Data Subject Access Request as discussed below.

[12]Regulation 3.1(1) of NDPR
[13]Regulation 2.13.1 of NDPR
[14]Regulation 3.1(1) of NDPR
[15]Regulation 3.1(1) of NDPR
[16]Regulation 3.1(4) of NDPR

Think Time



Stephanie is trying to register on an online financial platform in order to easily transfer money online. However, she requires information such as her account number and BVN in order to complete the registration. Unfortunately, she does not have this information. She places a call to her bank and requests for her details telling the officer to just read out the details to her while she writes it out. As the DPCO or DPO to the bank, what will be your advice to the bank on how to treat Stephanie's request?

2.2.7. **The Data Controller or Data Administrator is obligated to respond to a DSAR within one month of receipt of the DSAR. Such response includes acceding to the Data Subject's request or giving reasons why the request may not be attended to. Where the Data Controller's response is the notification of the reason why the request cannot be attended to, the Data Controller must inform the Data Subject of the possibility of the Data Subject lodging a complaint with NITDA, that is, in the event that the Data Subject does not agree with the reasons given by the Data Controller.**[18]

2.2.8. **Where the Data Controller does not take action on the request of the Data Subject, it should appropriately inform the Data Subject without delay, and not more than one month of the receipt of the DSAR, the reasons for not taking action as well as on the possibility of lodging a complaint with NITDA.**

Think Time

Adibas Hotels and Resorts is a 5 Star hotel in Lagos, Nigeria. It attracts about 1 million customers yearly. In order to further promote and provide for ease of access to its services, the Hotel has established an online platform where intending customers can register and make bookings in advance. In the process of booking, information such as name, email address, date of birth, phone number, details of next of kin etc is entered on the platform. On the 14th of February, Kunle went to spend the valentine weekend at the hotel with his wife, having made reservations in advance. On the 1st of March, Kunle wrote an email to the Hotel requesting for his information as provided when he was making the reservation. On the 10th of April, there was still no response from the Hotel. What would you advice Kunle? Would your answer be different if the Hotel had responded to his request by telling him he could not have access to the requested information?

[17]Regulation 3.1(2) of NDPR
[18]Regulation 3.1(3) of NDPR
[19]Regulation 3.1(3)(a) and (b) of NDPR
[20]Regulation 3.1(4) of NDPR

2.2.9. Unless NITDA states otherwise, a Data Controller cannot charge the Data Subject for responding to a DSAR. NDPR however recognizes the possibility of vexatious, excessive and or repetitive requests. In such instances, the Data Controller is allowed to charge a reasonable fee commensurate to its administrative costs for providing the Data Subject with the required information. Alternatively, the Data Controller can write the Data Subject, stating its refusal to act on the DSAR. Such a letter or communication should be copied to NITDA.[20] NITDA is required to have a communication channel in place for the purpose of this communication.

2.2.10. The Data Controller has the burden of establishing that the Data Subject's DSAR is unfounded or excessive.[21]

2.2.11. There may be instances where a DSAR is made by a Data Subject to a Data Administrator who comes into possession of such Personal Data by virtue of his position as a third-party service provider to the Data Controller. The Data Controller is seen as a middleman between the Data Administrator and the Data Subject. Accordingly, in such instances, it is recommended that the Data Administrator redirects the Data Subject to the Data Controller, as the information requested by the Data Subject will be transferred to him by the Data Controller. Furthermore, the Data Administrator is to provide such requested information to the Data Controller for onward transmission to the Data Subject and also work with the Data Controller to ensure that the Personal Data requested is provided to him properly and timeously in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by the NDPR.

Think Time

Mr. Gerald has been looking for an efficient insurance company with which to insure his house and car. Subsequently, he decided to contract with Peaky Insurance and in January 2019, the company provided insurance cover for his house and car for a duration of one year. Typically, his information was obtained by the company in the course of registering him. On February 14, Mr. Gerald requested that the company provide him with his information in their possession, which they did. Two weeks after, Mr. Gerald made the same request again and was obliged. On the 7th of March, Mr. Gerald again requested for the information. What would you advise that Peaky Insurance should do?

2.3. Setting up and Implementing a DSAR Process

2.3.1. Common-sense will dictate that a Data Controller should put in place an inventory system by which the Data Controller can easily identify where all Personal Data are located within its superstructure in order to guarantee easy and timely retrieval of Personal Data upon an access request being made by a Data Subject. This is reflective of the Personal Data processing principle of Security, specifically the sub-principle of Availability or Accessibility. The use of such a DSAR system may prove helpful in reducing the time and effort required by a Data Controller to respond to an access request.

2.3.2. Further, Data Controllers and Data Administrators should put measures in place to ensure that employees who are responsible for handling DSARs are appropriately and regularly trained on the organisation's DSARs processes. This is important in order to reduce the risk of non-compliance with the NDPR.

2.3.3. We set out below, some practical considerations in setting up and implementing an effective DSAR process:

2.3.3.1.

One of the essential factors a Data Controller would consider when confronted with a DSAR is to confirm the identity of the Data Subject making the request before going ahead to consider whether or not to provide the requested information. Personal Data is only to be transferred where the Data Controller is satisfied with the identity of the Data Subject making the request. The Data Controller is to ensure that the DSAR made is in relation to the Personal Data of the Data Subject who is a living person and that such Personal Data was actually given by the Data Subject to the Data Controller. The Data Controller needs to verify the identity of the person making the DSAR. Although NDPR states that the Data Controller is to request for identification where the Data Subject asks for an oral presentation of his Personal Data , it is recommended that in every occasion of a DSAR, the identity of the Data Subject making the request is first confirmed.

2.3.3.2.

For ease of compliance and response, the Data Controller may establish different categories of DSARs as well as criteria for each category in order to easily classify such request as well as the necessary actions to be taken. For instance, a Data Controller may have categories for simple and straight-forward DSARs and 'Sensitive DSAR', to differentiate between a DSAR for ordinary Personal Data and Sensitive Personal Data, respectively. This is just an example of the groupings of DSARs in order to have an efficient DSAR process.

2.3.3.3.

In the event that the Personal Data requested for is in a written document which also contains other information not requested, the Data Controller is advised to take steps to modify such document to reflect only the Personal Data that is requested. This will aid in ensuring that no extra data is released thus reflective of the Personal Data processing principle of Security, specifically the sub-principles of Confidentiality and Integrity.

[22]Regulation 3.1(1) of NDPR

2.3.3.4.

Where Personal Data is released by a Data Controller in response to a DSAR, such release must be recorded. Information to be recorded include details such as name, address and identification of the Data Subject making the request as well as the date such request was made; the Personal Data requested for and released to the Data Subject; response given where the request could not be met; fees charged (if applicable); and any issues or concerns raised and the date such response to the request was provided by the Data Controller.

2.3.3.5.

In the event that a Data Controller is unable to provide the Personal Data requested by the Data Subject, it is to respond to the Data Subject explaining why the Personal Data requested cannot be provided and also advise on any course of action such as extension of time within which to provide the Personal Data.

2.3.3.6.

In the event that the Data Controller is able to establish[23] that the Data Subject is making unfounded and excessive request of the Personal Data, the Data Controller may communicate a charge of a reasonable amount to the Data Subject or otherwise communicate the option of lodging a complaint with NITDA to the Data Subject.

2.3.3.7. In summary and giving the NDPR requirement that a DSAR must be responded to immediately and not later than one month from the date of the DSAR, we recommend the following simple processes for dealing with a DSAR:

1

Upon receiving the DSAR, immediately record the details of the request in the DSAR Register[24] and confirm/acknowledge receipt of the request to the Requester and notify the Requester that the Data Controller will, as soon as possible, revert to the Data Subject upon compliance with the Data Controller's DSAR Process. Details of the request will include: the time of the request; the contact details/ means of identification of the Requester; and the particular request. Where the Requester is not the Data Subject himself but a representative, a letter authorizing such Requester to make the request for Personal Data.

2

Implement the Data Controller's DSAR Process by:

- Verifying the identity of the Requester to ascertain that he is the Data Subject;
- If yes:
  - Gather the relevant information requested by the Data Subject and send to the Data Subject.
  - Update the DSAR Register with the record of the information sent to the Data Subject and the time of the response.
- If no:
  - Notify the Requester that:
    - *the Data Controller's DSAR Process will not allow the Data Controller grant the DSAR as the relevant Data Subject's identity could not be verified; and*
    - *the Requester can lodge any complaint on the response to NITDA.*
  - Update the DSAR Register with the record of the information sent to the Requester and the time of the response.

[23]Regulation 3.1(4) of NDPR
[24]A template DSAR Register is available at: https://ndpacademy.ng/DSAR-Registertemplate

2.3.4. It is important to ensure that the Personal Data to be provided to the Data Subject in response to the DSAR must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[25] The Data Controller must also ensure that the Personal Data is provided in writing or by any other means including electronically, for example, by email. The information may also be provided orally. In such circumstances however, it is mandatory that the Data Controller takes steps to confirm the identity of the Data Subject.

2.4 Module 2: Summary

2.4.1. The right of access is one of the 8 rights of Data Subjects under the NDPR. The exercise of the right often enables the Data Subject to exercise his other rights under the NDPR.

2.4.2. The right of access is primarily the Data Subject's right to confirm from the Data Controller if any processing activity is being carried on in respect of the Data Subject's Personal Data.

2.4.3. The Data Controller or Data Administrator must respond to a DSAR in a structured, concise, commonly-used, transparent, intelligible and machine-readable format using clear and plain language.

2.4.4. Data Controller or Data Administrator must respond to a DSAR in writing unless the Data Subject elects to obtain the information orally.

2.4.5. The Data Controller or Data Administrator will be right to insist that a person establish that he is the Data Subject or his representative, by a means other than the oral account of that person.

2.4.6. The Data Controller or Data Administrator has a month to respond to a DSAR. The response could be that of declining a positive response to the DSAR and informing the Requester of his right to file a complaint or report with NITDA as regards the refusal by the Data Controller to carry out the request.

2.4.7. A Data Controller or Data Administrator should ensure that it has a good and implemented DSAR System or Process within its organisation.

Further Reading:

1. 2019 Nigeria Data Protection Regulation[26]
2. European Union's General Data Protection Regulation
3. National Information Technology Development Act 2007[27]
4. Data Protection Implementation Framework

[25]A template DSAR Response (email) is available at: https://ndpacademy.ng/resources.php
[26]Available at: http://taxtech.com.ng/download/Nigeria%20Data%20Protection%20Regulation.pdf
[27]Available at: http://taxtech.com.ng/download/NITDA-act-2007.pdf