PRIVACY & DATA PROTECTION
23rd October 2025



Maryam Abdulsalam[1]

AN EVALUATION OF DATA SUBJECT ACCESS REQUESTS IN ORGANIZATIONS

1. Introduction

In ensuring the effective protection of personal information, data subjects have a range of rights over their personal data that are recognized by privacy laws[2] and regulations.[3] Some of the rights of a data subject include the right of access, the right to rectification, the right to erasure, and the right to object, among others. Data controllers and data processors are obligated to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data in their possession and control. An essential right conferred on a data subject is the right to access the personal data in question. Data subjects can request access to their information and obtain a copy of their personal data from the organization that is in possession of the data. This right promotes the principle of transparency and gives room to other rights such as rectification, withdrawal, erasure, or objection to further processing. Data subjects can exercise this right through a Data Subject Access Request (DSAR).

This article aims to examine the procedure for initiating a DSAR and the procedure for handling DSAR in organizations.

---

1 **Maryam Abdulsalam, Associate, Intellectual Property Department, SPA Ajibade & Co. Lagos, Nigeria.**

2 See, section 34 of *Nigeria Data Protection Act* (NDPA) 2023, available at <https://ndpc.gov.ng/resources/#> accessed on 14th September 2025.

3 See, Articles 15 - 22 of *General Data Protection Regulation* (GDPR) 2019, available at <https://gdpr-info.eu/art-15-gdpr/> accessed on 14th September 2025.

2. Data Subject Rights

These are legal rights created by privacy laws and regulations that confer authority on individuals regarding the use and process of their personal information. The rights guarantee protection and control of the data subject's information processed in an organization. In Nigeria, the rights of data subjects are recognized under Part VI of the Nigeria Data Protection Act.[4] These rights align with the international standards provided in the General Data Protection Regulation (GDPR).[5]

- **Right to Access** – Data Subjects are conferred with the right to demand for their information collected and processed in an organization. This right ensures that data subjects are aware of their personal data collected and stored in an organization.
- **Right to rectification** – This relates to a data subject's right to correct or rectify personal data utilized by the data controller. In other words, it implies a data subject's right to have incorrect or outdated data about him/her corrected or rectified.
- **Right to object and/or restrict** – In exercising this right, a data subject may object to the processing and/or restrict the continued processing of his/her personal data. This right ensures the data subject determines the extent to which a data controller or data processor utilizes his/her information.
- **Right to withdraw consent** – Data subjects have the right to withdraw consent, and a controller must inform data subjects of this right, but such withdrawal shall not prejudice the lawfulness of previous processing. Any further processing of the data subject's data amounts to an infringement of his right, the breach of which could be remedied by approaching a court of law for redress.
- **Right to erasure** – This right grants the data subject to request for the erasure or deletion of his/her personal data from a data controller. However, this right can only be exercisable if the personal data is no longer necessary to the purpose for which it was initially collected, or if consent has been withdrawn by the data subject, or the data controller is processing without lawful basis, and the personal data is not subjected to any legal claim, and investigation by legal authorities.

[4] Sections 34 – 38 of NDPA 2023.
[5] See, Chapter 3 (Article 12- 23) of GDPR, 2019 available at <https://gdpr-info.eu/> accessed on 23rd October 2025.

- **Right to data portability** - This right relates to the transfer of personal data from one data controller to another controller or processors. Data subjects are entitled to collect a copy of their personal data controlled or stored by a controller in a compact, structured, commonly used, and machine-readable format or to have the data transferred to another controller.

3. What is a Data Subject Access Request (DSAR)?

A DSAR is a request made by a data subject in the exercise of his/her right of access to their personal data held by an organization. The request allows the data subject to obtain a copy of their personal data, and other supplementary information from an organization processing the personal data, which may or may not include payment of a fee depending on the circumstances of the case, provided such access will not infringe on the rights of others.

DSAR grants the data subject control over their personal data and ensures transparency on how the organization processes their data. It enhances accountability in the organization's processing activities and ensures that the personal data is processed in a lawful, specific, fair, and legitimate manner. Typically, DSAR is generated in written or electronic format, containing the relevant information to process the request, and submitted physically or electronically (including via social media) to the organization.[6]

4. Effective Management of DSAR in an Organization.

For effective management of DSAR, organizations should consider the following in handling requests received from data subjects:

4.1 Designated personnel to handle DSAR

Appointing designated personnel or a team, usually a Data Protection Officer (DPO) or Compliance team in an organization, to handle DSAR is crucial for compliance and operational efficiency. The DPO or Compliance team is required to be trained to effectively handle DSAR within the appropriate timeframe and provide accurate responses to the request. The designated contact person's details should be communicated to Data Subjects.

4.2 DSAR Policy and Data Mapping

[6] See, Information Commission Officer, *How do we recognise a subject access request (SAR)?* Available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-recognise-a-subject-access-request-sar/?q=register&utm_source=chatgpt.com#whatis> accessed on 16th September 2025.

A DSAR policy should be developed and enforced in an organization. The policy which should be comprehensive and easily operational, must contain the process for handling requests and clear procedures for identifying, retrieving, and reviewing personal data. Conducting a data-mapping exercise to highlight the organization's processing activities can enable the DSAR response team easily contact appropriate team members or person upon the receipt of DSAR and to coordinate swift capture of personal data and respond to the request.[7]

4.3 **Awareness and Training**

Continuous training sessions are essential for new and existing personnel responsible for attending to data subjects' requests on the obligations of the organization and the rights of the data subjects. An organization can develop a privacy checklist as a guide to persons engaged in data processing activities to enable them to understand their duties and responsibilities.[8] The guide should contain the procedures for handling DSAR and the appropriate timeframe in responding to the requests from data subjects.

4.4 **Communication and Clarity**

Where an access request is made, the organization should acknowledge the request with a holding response. Further clarifications may be required in processing the request. The organization can liaise with the data subject to understand the scope of the request, the mode of responding to the request, and streamlining resources to specific and relevant information. This is an integral part of effectively managing a DSAR.

4.5 **Duration**

An organization is obligated to respond within one month upon receiving a DSAR. However, when the DSAR is complex and requires extensive details, the timeframe might be adjusted and payment of a fee required, depending on the circumstances surrounding the DSAR. It is essential that organisations respond to these requests effectively and within the set timeframe in order to meet requirements and avoid the impact of potential fines or reprimands from the regulatory authorities.[9]

---

7 See, Nicola McCrudden & 4 ors, 'Navigating The Rise In Data Subject Access Requests', available at <https://www.mondaq.com/uk/data-protection/1620206/navigating-the-rise-in-data-subject-access-requests> accessed on 16th September 2025.

8 See, Article 30 (7) *NDP Act General Application and Implementation Directive (*GAID) 2025, available at

9 See, S. Dehsheykhi and A. Strickland, Data And Cyber School: Top Tips On Dealing With Data Subject Access Requests, available at <https://www.mondaq.com/canada/data-

4.6 **Providing Specific and Accurate Information**

The response to a DSAR should be specific to the information requested. Organizations should employ data minimization in providing responses to DSAR. Irrelevant information not requested can expose the organization to potential data breaches. Also, accurate, complete, and non-misleading information should be provided in the response. Where a request is made electronically, data controllers should provide the required information in a commonly used electronic format, unless the individual requests otherwise.

5. Limitations to DSAR

Certain restrictions can hinder an organization from providing the information requested on DSAR. A data controller can restrict some information or documents in responding to a DSAR. Where such information or documents are subject to legal obligations, organizations are required to comply with the legal obligations and withhold the information or documents. Hence, data controllers may not provide data that is processed in certain conditions such as in relation to a legal claim, contemplation of litigation, criminal investigation, public or government interest, or confidential communication between a lawyer and their client.[10]

Additionally, organizations are obligated to restrict access to a data subject's personal data if complying with their DSAR will impact the rights of others. Responses to DSAR should not contain personal data of another data subject as this can lead to possible risk and personal data exposure. Organizations must conduct comprehensive due diligence and verify the identity of the data subject prior to responding to the DSAR.

6. Conclusion

With the increase of data rights awareness and the rise of DSAR activity, it is imperative for organizations to establish a comprehensive and efficient method for responding to DSAR, while taking into consideration the relevant legal restrictions on data privacy.

In addition, organizations should, by proportionate means and technological tools, verify the identity of the data subject submitting a DSAR, assess whether the request gives rise to ancillary obligations necessitating notification of other internal functions, and ensure that the data subject is duly informed of his or her rights under applicable data protection law.

---

protection/1526076/data-and-cyber-school-top-tips-on-dealing-with-data-subject-access-requests> accessed 16th September 2025.

[10] See,<https://www.mondaq.com/ireland/data-protection/1404836/how-to-respond-to-a-data-subject-access-request> accessed 30th September 2025.

A thorough evaluation of an organization's existing methods and processes for handling data subject requests should be conducted for the adoption of additional new and effective processes. This assessment is crucial to ensure that they can promptly identify requests as they are submitted.

It is essential for organizations to stay aware of and adhere to all relevant legal deadlines related to these requests, ensuring they respond in a timely manner and maintain compliance with regulations and data protection laws. By doing so, organizations can better protect individual rights and uphold their legal obligations.

For further information on this article and the area of law,
please contact **Maryam Abdulsalam**
at S. P. A. Ajibade & Co., Lagos, by
Telephone +234.1.270.3009; +234.1.4605091; +234.1.460.5092
Mobile +234.908.819.3288, +234.903.967.5389
Email: mabdulsalam@spaajibade.com
www.spaajibade.com