# DATA SUBJECT ACCESS REQUEST PROCEDURE

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version:</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>

Commented [EUGDPR1]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [EUGDPR2]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd.mm.yyyy</td>
<td>0.1</td>
<td>EUGDPRAcademy</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

Table of contents

1. SCOPE, PURPOSE AND USERS .................................................................................3
2. REFERENCE DOCUMENTS .........................................................................................3
3. DATA SUBJECT ACCESS REQUEST ("DSAR")...............................................................3
4. THE RIGHTS OF A DATA SUBJECT ........................................................................3
5. REQUIREMENTS FOR A VALID DSAR .......................................................................4
6. DSAR PROCESS ........................................................................................................4
   6.1. REQUEST........................................................................................................5
   6.2. IDENTITY VERIFICATION .................................................................................5
   6.3. INFORMATION FOR DATA SUBJECT ACCESS REQUEST ..................................5
   6.4. REVIEW OF INFORMATION ............................................................................5
   6.5. RESPONSE TO ACCESS REQUESTS ...............................................................5
   6.6. ARCHIVING.....................................................................................................6
7. EXEMPTIONS ............................................................................................................6
8. DATA SUBJECT ACCESS REQUEST REFUSALS ......................................................6
9. RESPONSIBILITIES .................................................................................................7
10. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT ......................7
11. VALIDITY AND DOCUMENT MANAGEMENT ......................................................7
ANNEX: DATA SUBJECT ACCESS REQUEST FLOWCHART ..........................................9
1. Scope, Purpose and Users

This procedure sets out the key features regarding handling or responding to requests for access to personal data made by data subjects, their representatives or other interested parties. This procedure will enable [Company name] (further: “Company”) to comply with legal obligations, provide better customer care, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them.

This procedure applies broadly across all entities or subsidiaries owned or operated by the Company but does not affect any state or local laws or regulations which may otherwise be applicable.

This procedure applies to employees that handle data subject access requests such as the Data Protection Officer.

2. Reference Documents

- Personal Data Protection Policy
- [relevant local legislation]

3. Data Subject Access Request (“DSAR”)

A Data Subject Access Request (DSAR) is any request made by an individual or an individual’s legal representative to the Company for access or information about personal data held by the Company. A Data Subject Access Request is a common mechanism that allows individuals to request copies of the data.

A Data Subject Access Request must be made in writing. In general, verbal requests for information will not be considered. The Data Protection Officer, who will consider and approve all Data Subject Access Request applications.

A Data Subject Access Request can be made via any of the following methods: email, fax, post, telephone or in person.

4. The Rights of a Data Subject

The rights to data subject access include the following:

Commented [GDPR3]: Insert your company name here.

Commented [GDPR4]: If you didn’t nominate the Data Protection Officer, then specify who is responsible for personal data protection.

Commented [EUGDPR5]: A Data Subject Access Request can be made verbally in Germany. Hence it is necessary to ensure that verbal requests are treated with the same level of care as with written requests.

Commented [GDPR6]: In case you do not have such job title, then specify who is responsible for handling DSARs.
5. Requirements for a valid DSAR

In order to be able to respond to the Data Subject Access Requests in a timely manner, the data subject should:

- Submit his/her request using a Data Subject Access Request Form.
- 

Subject to the exemptions referred to in this document, the Company will provide information to

However, Company will not provide data where the resources required to identify and retrieve it

Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the

6. DSAR Process
6.1. Request

Upon receipt of a DSAR, the [job title] will acknowledge the request. The requestor may be asked to verify their identity and provide a written confirmation that they are the correct individual to whom the request pertains.

6.2. Identity verification

The [job title] needs to check the identity of anyone making a DSAR to ensure information is only provided to the individual who is the subject of the request. This is done for the purposes of protecting the individual’s personal data and to prevent unauthorized individuals from accessing the information. A sample method of identification can be a photo identity and the other confirmation of address. If the requestor is not the data subject, written confirmation that the requestor is authorized to act on behalf of the data subject is required.

6.3. Information for Data Subject Access Request

Upon receipt of the required documents, the person receiving the request will provide the Data Protection Officer with all the information necessary to respond to the request. The Data Protection Officer will then notify the requestor that his/her DSAR will be responded to within 30 days of receipt of the request. Any deviation from the 30 day timeframe due to other intervening events will be communicated to the requestor.

6.4. Review of Information

The Data Protection Officer will contact and ask the relevant department(s) for the required information. The department must return the required information by the deadline imposed by the Data Protection Officer and/or if consent is required to be provided from a third party.

The Data Protection Officer must ensure that the information is reviewed/received by the imposed deadline. If not received or if the information is not correct, the department(s) responsible for providing the information must provide a reason for non-compliance. The Data Protection Officer will then document compliance with the 30 day requirement.

6.5. Response to Access Requests

The Data Protection Officer will provide the finalized response together with the information written response will be sent back to the requestor. This will be via email, unless the requestor has requested another method of communication.
only provide information via channels that are secure. When hard copies of information are posted,
[organization name] [confidentiality level]

6.6. Archiving

After the response has been sent to the requestor, the DSAR will be considered closed and archived
by the Data Protection Officer.

[organization name] [confidentiality level]

7. Exemptions

An individual does not have the right to access information recorded about someone else, unless

The Company is not required to respond to requests for information unless it is provided with

In principle, the Company will not normally disclose the following types of information in response to
a Data Subject Access Request:

- will not be granted, unless the individuals involved consent to the disclosure of their data.
- Repeat requests – Where a similar or identical request in relation to the same data subject
  made within a six month period of the original request will be considered a repeat request,
  and the Company will not normally provide a further copy of the same data

- Opinions given in confidence or protected by copyright law – The Company does not have to

- Privileged documents – Any privileged information held by Company need not be disclosed in
  response to a DSAR. In general, privileged information includes any document which is

8. Data Subject Access Request Refusals

There are situations where individuals do not have a right to see information relating to them. For
instance:

Commented [EU GDPR12]: This period is only a suggestion. The Company could decide to shorten the period.

Commented [GDPR13]: For example, a description of a living data subject which is described in artistic manner in a book.

Commented [GDPR14]: E.g. doctor-patient privilege, act of confessing to a priest, etc.
9. Responsibilities

The overall responsibility for ensuring compliance with a DSAR rests with the Data Protection Officer. If the Company acts as a data processor the Data Protection Officer will forward the request to the data controller (the person responsible for ensuring data protection compliance). The Data Protection Officer is available to offer guidance to the data controller as well as to the Data Protection Officer as appropriate.

If the responsible person refuses a Data Subject Access Request on behalf of the Company, the Data Protection Officer is required to make a report to the Data Protection Commissioner.

10. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Subject Access Request Forms</td>
<td>[specify folder on the company Intranet]</td>
<td>Data Protection Officer</td>
<td>Only authorized persons may access the folder</td>
<td>10 years</td>
</tr>
<tr>
<td>Data Subject Disclosure Form</td>
<td>[specify folder on the company Intranet]</td>
<td>Data Protection Officer</td>
<td>Only authorized persons may access the folder</td>
<td>10 years</td>
</tr>
</tbody>
</table>

11. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.
Commented [GDPR15]: There is no legal obligation to print the documents, the company needs to have a proof that it has made the documents available to the relevant employees.

If the company decides to print the document, it can also decide whether the document needs to be signed or not.