Data Access Request Handling Guide for UK SMEs

Why data access requests matter

- A Data Subject Access Request (DSAR) is when an individual wants to see the information that a business has regarding them. The request can come from: A customer, An employee, Anyone who has had any contact with the business
- Under UK GDPR (General Data Protection Regulation), individuals have a legal right to see what data businesses hold on them. They can also ask the business for the reason why the data is being retained and who it has shared the data with.
- Small to medium businesses will find that they have far more of these requests than they will have anticipated, and the way in which DSAR's are dealt with will demonstrate a business's commitment to data protection.
- Poorly managed DSAR's will result in complaints being made to the Information Commissioner's Office (ICO).
- Many SMEs believe that DSAR's are complicated and particularly challenging to deal with. However, in most cases, you will be able to handle these requests in a timely manner and using a straightforward process.
- There are clear processes and checklists with templates available to enable businesses to respond quickly with confidence and comply with the law.

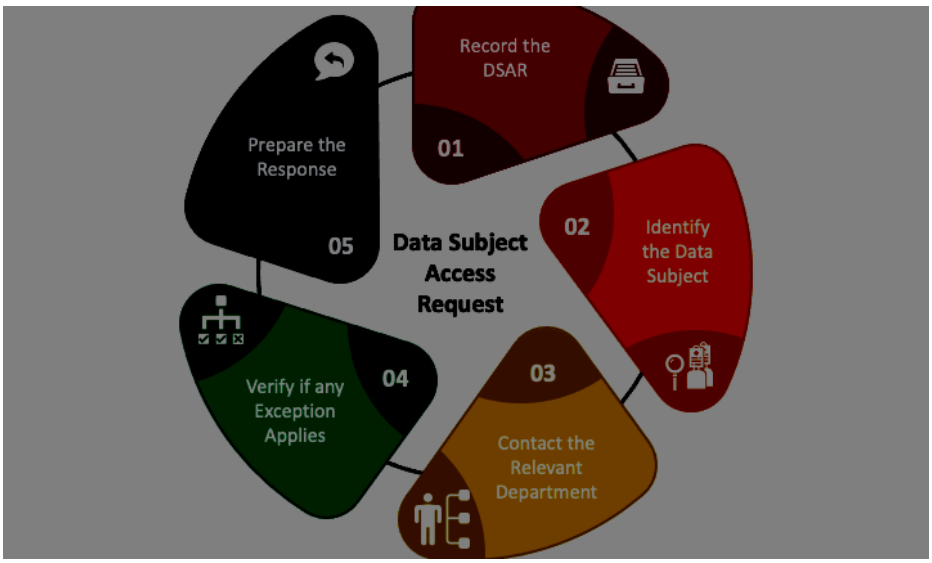
What a Data Subject Access Request (DSAR) is

A data subject access request (DSAR) is an individual (or the "data subject") making a request of a business for (accessing) any personal data that is being possessed by the business. Personal data may include any type of information that can uniquely identify a person .

Requests for accessing personal data can be made verbally or in writing (for example, using email, letters, or social media). They do not have to specifically state "data subject access request" or "subject access request" to be a valid request for access to personal data as long as the requester is making the request in a clear manner.

Once a DSAR has been received by the business, the organisation needs to respond to the request without delay and generally speaking within one month. The response to the request must provide information in an easy to understand format (usually in an electronic format) and include the following information:

- details of the personal information held by the business,
- the reason(s) the personal data is being held (i.e. the purpose),
- who the personal data has been shared with,
- the length of time the business intends to retain the personal information, and
- the rights of the individual (e.g. to change their information or have the information deleted).



Who can submit a data access request

- People who are currently or in the past a customer
- People who are currently or in the past a worker or contractor
- People or businesses you have a relationship with (holding personal data)
- Anyone your organisation processes personal information for (e.g., job candidate, website visitor)

A request can be made on behalf of a child by a parent/guardian and by a person with the Power of Attorney.

Examples of common DSAR situations

- A customer requesting "Please provide any and all information you have about me?"
- A former employee requesting "Please provide me with all of my HR record and all emails that were directed at me."
- A person who requested information last year requesting the notes made on that request.
- A candidate requesting feedback from the interview.

Step-by-step process for handling DSARs

Use these guidelines to process virtually all types of requests in an efficient manner.

Recognise the request.

- Log the request as soon as you receive it (include the date received, who requested it and what it is they requested). Log every request, even if it is not a formal request.

Confirm the requester’s identity.

- If you are unsure of who the requester is, you should ask them for proof of their identity (e.g., their driving licence, passport, utility bill, etc.). This protects you from processing requests made by fraudulent individuals.

Document the request internally.

- Enter the request onto an internal DSAR record (a simple spreadsheet is acceptable): date, name of requester, deadline, and the name of the person assigned to process the request.

Identify systems that may contain applicable data.

- Consider where personal data could reside: for example, in emails, within HR records, in the CRM, in accounting systems, in CCTV footage, on web forms, in loyalty programs, etc.

Search for personal data across many different systems.

- When searching for a person's personal data use their name, email, phone number or reference number when performing your searches. You should also conduct the same searches against any archival or backup systems that may apply.

Review and redact

- Removing data for any other person is prohibited. If you know that the requester is a person and you would expect them to be an adult, all information related to someone other will remain private.

Package the response properly.

- The information must be in a clear document that provides adequate explanation as to what has been sent back and what rights have been afforded to that request.

Securely transmit the response.

- You must send this document either by encrypted email or via secure file sharing link with a password. If you require confirmation of receipt, it is advisable to obtain confirmation.

Keep a record of completion

- You must keep a log of the completion of requests with you documenting the date of completion, method of sending, any redactions of data and/or any other data that you had withheld.

Time limits and response expectations

- Businesses must respond within one month after receiving a request. If a request is complicated or if there are multiple requests from one person, an extension may be granted; however, the business must advise the requester of the status during the first month, indicating the reason for the delay.
- The clock will begin once the business receives a clear request for action and verifies the requester's identity.

What information businesses must provide

The business must provide individuals with:

1. Their personal data,
2. The reasons the data is being processed,
3. Categories of the data shared with other parties (not names),
4. Time frames for retention of the data,
5. Individuals have a right to have their data corrected, deleted, objected to, etc.,
6. Where the data was received from,
7. Whether automated decision-making has occurred.

The requirements for providing this information in an electronic format and in as understandable a manner as possible.

Situations where data may be withheld or redacted

You can withhold/redact information at times if:

- It includes another person’s personal data (to protect their privacy)
- Disclosing it will negatively affect another person’s rights/freedoms
- It is legally privileged (i.e. legal advice)
- National security or criminal prevention applies (only applies to very few SMEs)

Record-keeping and documentation

You should also maintain a basic DSAR log that indicates:

- Date request made
- Name of the requester
- What the requester wanted
- The date you must respond to the requester
- Who was the contact point
- The date of your reply

- Any redactions or withholdings made and your reasons for same

This log will assist you in answering questions from the ICO and demonstrate that you have a process in place.

DSAR handling checklist

- ✓ Confirm request was logged with date and details?
- ✓ Confirmed that identity of requester was verified?
- ✓ Conducted search on all known relevant systems?
- ✓ Provided a copy of the third-party records with necessary redactions?
- ✓ Prepared a response to the requester in a clear format?
- ✓ Sent the response securely and within one month of making your request (or extended with an explanation)?
- ✓ Documented completion of the request in your DSAR log?
- ✓ Reviewed any lessons learned from the request for future requests?

Personal data search checklist

- ✓ Email (includes both archived and deleted emails)
- ✓ Human Resources / Personnel Files
- ✓ Relationship Management (CRM) System
- ✓ Accounts payable / Accounts Receivable
- ✓ Documents stored electronically (SharePoint, one drive, or local hard drives)
- ✓ Security video (CCTV) footage
- ✓ Loyalty programs / marketing email lists
- ✓ Web forms and/or contact submissions from your website

Data protection readiness checklist

- ✓ Privacy Notice Is Up To Date & Available To The Public
- ✓ Staff Has Been Briefed & Trained On The DSAR Process
- ✓ Simple DSAR logging has been implemented
- ✓ Retention Policy Has Been Written And Implemented
- ✓ Has A Secure Method Of Responding (Encrypted email or link)

FAQs

1. What is a data subject access request?

Someone requests access to their personal data that your company possesses. This is possible through either a verbal or written request and does not require stating "data subject access request."

2. **How long does a company have to respond to a data subject access request?**

A data subject access request must be responded to within 30 days from receipt of the request and upon successful completion of identity verification. If the request is complex, it may take up to an additional 2 months to provide a response to the data subject access request. An explanation of why the time has been extended must be provided to the data subject within the first 30 days.

3. **Is it permissible for a company to charge a fee for processing a data subject access request?**

In general, a company will not charge a fee for processing a data subject access request, unless the request is manifestly frivolous or excessive.

4. **What if the data subject access request is large?**

You may request further clarification from the data subject to limit the scope of the request. If the data subject access request is still large, you may extend the time to respond for up to 2 months; however, the data subject must be notified that the time has been extended.

5. **Can a company refuse a data subject access request?**

A company can only refuse to fulfil a data subject access request for certain limited reasons. The company must provide the individual requesting the data with an explanation of why the data subject access request was denied and inform the individual of their right to file a complaint with the ICO.

6. **What is personal data?**

All information that may be used to identify an individual who has not died.

7. **Who should handle a DSAR?**

Typically, a request of this kind will be dealt with by the owner, office manager or someone designated for this purpose. In larger SMEs, it will usually be handled by either the HR or compliance lead.

8. **What if someone else's personal data is part of the request?**

In such cases, you will need to either redact or withhold third party information to protect their privacy, so be sure to document that you have taken this action.

About This Guide

The **Computer Support Centre** developed this guide to assist small or medium-sized UK companies with how to appropriately respond to Data Subject Access Requests (DSAR). Many businesses have customer, employee and partner personal data, therefore individuals hold rights to obtain access to this information.

This guide intends to clearly and simply explain what a Data Subject Access Request is and how a business should respond, as well as to provide practical steps, examples and checklists for non-technical users to effectively manage requests with confidence, and to avoid making common mistakes. In addition, it has been produced with regard to the general responsibilities businesses have under UK GDPR.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

As individuals are increasingly aware of their data rights, Data Subject Access Requests (DSARs) are becoming increasingly common. For small and medium-sized enterprises (SMEs) in the UK, the need to respond correctly is not only important for ensuring legal compliance but also for maintaining trust with your employees and customers.

Businesses will be able to meet the response time frames set out in legislation by implementing a clear DSAR process, having organised records, and training staff members to identify DSARs, thereby reducing the risk of confusion.

Being prepared for handling DSARs will simplify the process for companies.

An organisation will be able to efficiently manage data subject access requests via the establishment of basic procedures and appropriate documentation. This practice will assist in protecting the individual's personal information, while demonstrating sound data management practices.