

MASTERING DATA SUBJECT ACCESS REQUESTS

A step-by-step guide for handling DSARs
with confidence



Amsterdam • Dublin • London • New York • Toronto





INTRODUCTION

Handling Data Subject Access Requests (DSARs) can be daunting and requires careful attention to ensure compliance with the General Data Protection Regulation (GDPR).

Individuals have the right to access their personal data but fulfilling these requests isn't always simple. Your team must balance various obligations – safeguarding third-party privacy, maintaining confidentiality, and meeting deadlines. DSARs that involve multiple data subjects, repeat requests from the same individuals, and high volumes of sensitive data can also add further challenges.

DSARs are inherently complex and it's common for professionals to have differing views on how to approach them. If you're unsure at any point, it is important to seek advice and guidance from your Data Protection Officer (DPO) or a specialist.

This guide takes you through the key aspects of completing a Data Subject Access Request (DSAR). Though it isn't exhaustive or specifically tailored to your company or sector, we highlight the key considerations you'll need to address.

YOUR STEP-BY-STEP DSAR GUIDE

INFORMATION	PAGE
What is a DSAR	04
Time frames for responding	05
Validating the requestor	06
Receiving a request from a third party	07
Acknowledging and processing the DSAR	08
Determining what to redact	09
Responding	10
What about exemptions?	11
DSAR progress checklist	12
Why choose the DPO Centre?	13



WHAT IS A DSAR?

A Data Subject Access Request (DSAR) is a formal request by an individual (a 'data subject') to access the personal data an organisation holds about them.

DSARs can be made by email, phone call, social media, or even a third party – there is no specified format.

EU and UK data protection laws

Organisations operating across the EU and UK have a legal obligation under the General Data Protection Regulation (GDPR) to respond to a DSAR. Responses must be free of charge and include:

- Confirmation that personal data is being processed
- Clear information about how the data is used and the retention period
- A copy of their personal data, usually in electronic format

The GDPR requires organisations to conduct a 'reasonable search' for relevant data. In the UK, the Data Use and Access Act (DUAA) 2025 further defines this as 'reasonable and proportionate'.



In our experience, the average DSAR response requires around 27 hours to complete.



According to EY Law's latest survey of 2023, 60% of respondent organisations reported an increase in DSARs, with trends suggesting this rise is continuing.

TIME FRAMES FOR RESPONDING

Under the GDPR, you have one calendar month to respond to a DSAR, with the clock starting on the day you receive the request.

If the data subject hasn't provided enough information for you to identify the data, you can ask them for clarification – this will pause the response clock until you receive the necessary details.

For organisations operating in the UK, the Data Use and Access Act (DUAA), 2025 provides further clarity on when and how the clock can be paused, aiming to bring consistency in DSAR handling.



Advice: If the response deadline date falls on a weekend or a public holiday, you have until the next working day to respond.

EXTENSIONS

If a DSAR involves large volumes of data, sensitive data, or spans numerous jurisdictions, it may be considered complex and eligible for an extension of up to a **maximum of two months**.

In this instance, you must:

- ✔ Document your decision and the reasoning behind it
- ✔ Communicate your decision to the data subject as soon as possible and within the initial one-month period

From that point, you have two months to respond, regardless of how much of the original one month is left.

STEP 1: VALIDATING THE REQUESTOR

A first and crucial step in processing a DSAR is to validate the identity of the requestor. This ensures the request is legitimate and determines the rights available to the individual, including the appropriate processing approach.

How to validate an individual's identity:

- **Request formal documentation:** Encourage the individual to submit their request in writing with an official ID copy (passport, bank statement, etc), although they are not obliged to do so
- **Verify contact details:** Confirm the email address they have used to contact you aligns with the one you hold on record
- **Phone the data subject:** Call using the number listed in your database, not one provided in the request
- **Asking security questions:** Pose questions only the data subject would know the answers to



💡 **Advice:** Watch for information security threats from bad actors attempting to gain access to data. Train staff to spot red flags and always verify information against internal data.



RECEIVING A REQUEST FROM A **THIRD PARTY**

A DSAR can be submitted by a third party who is acting on behalf of the data subject, such as an agency or through a DSAR platform.

In this instance, you should:

- Confirm the identity of the data subject, either directly or via the third party
- Ensure the data subject has given explicit consent to the disclosure and they understand what the DSAR process entails
- Check that the third party is legitimate and has the authority to act on their behalf

💡 Advice: If the requestor cannot be positively identified and you believe there is no applicable right of access, the request should be refused. You may wish to seek expert advice before making any decisions.



STEP 2: ACKNOWLEDGING AND PROCESSING THE DSAR

It is important to actively manage the entire lifecycle of a DSAR.

By accurately logging and recording each action and decision, you not only demonstrate your adherence to the GDPR but also create essential documentation in the event of a dispute with the data subject. It is also vital for proving your compliance to a regulator such as the UK's Information Commissioner's Office (ICO).



ACKNOWLEDGE THE DSAR

Acknowledge the request by sending a communication to the data subject as soon as practically possible, detailing the terms of engagement and response time frame.

LOG THE DSAR

Use a DSAR log to maintain a record of all requests received, the date of receipt, tasks and responsible personnel, and timeframes.

RETRIEVE THE INFORMATION

Retrieving the requested information will require a thorough and organised approach. This will likely involve searching multiple systems, departments and data repositories.

STEP 3: DETERMINING WHAT TO REDACT



There are often occasions when providing personal data in a DSAR conflicts with other privacy rights or could prejudice legal provisions or interests.

To protect these rights, certain information should be removed or redacted from the disclosure.

HOW TO HANDLE CONFIDENTIAL CONTENT

Information is deemed confidential if it has been given in confidence or attracts a duty of confidence. Confidential information must be redacted within the DSAR disclosure, unless there is an overriding public interest.



Advice: If an individual has marked an email 'private and confidential', this does not automatically trigger the confidentiality exemption. You should assess the content and context to determine if it genuinely qualifies under the exemption.

HOW TO HANDLE THIRD PARTIES

When compiling a DSAR response, information about other individuals might also be included.

In these situations, a balance must be struck between the requestor's right to access their data and the privacy and legal rights of the third party.

STEP 4: RESPONDING

Best practices for responding to a DSAR

COVERING LETTERS

It's good practice to include a covering letter or accompanying explanatory material as part of your DSAR response. In addition to the statutory information, a cover letter should:

- Confirm the details and nature of data processing
- Be easily accessible, using clear and plain language
- Explain the rationale for any redactions and appropriate exemptions used

SECURE DELIVERY

Your delivery method should align with the requestor's preference, where possible. And regardless of the method, you should ensure delivery is safe and secure. We recommend using measures such as password protection and document watermarking.

REQUEST CLOSURE

After responding to a DSAR, close the case on any internal registers or databases. Include the response date, actions taken, and decisions made. This helps prove compliance in case of a dispute and keeps a record of what information was shared and with whom. Also, retain a copy of the data supplied, as it can save time if the data subject has further questions or complaints.



WHAT ABOUT EXEMPTIONS?



Under the GDPR, data subjects have rights, but there are situations where certain rights may be exempt.

WHEN DO EXEMPTIONS APPLY?

Exemptions typically apply to specific sections of data, not an entire DSAR. These include situations where the data included could:

- Compromise legal proceedings
- Prejudice safeguards
- Impact ongoing investigations

DOCUMENTING EXEMPTIONS

Every exemption must be clearly justified and documented, including the specific exemption applied, the reasoning behind it.

💡 Advice: If refusing the request in its entirety on excessive or manifestly unfounded grounds, you must explain your reasons for refusal, the right to complain to the local jurisdiction regulator, and the ability to enforce rights through judicial remedy.





DSAR PROGRESS CHECKLIST

Use this checklist to guide you through the key steps when processing a DSAR.

- Logged the request
- Validated the identity of the requestor
- Established the type and scope of the request
- Acknowledged the request in writing
- Performed searches and/or contacted relevant departments to undertake searches
- Considered the application of any exemptions
- Considered whether any 3rd party personal data needed redaction
- Watermarked the response
- Produced a covering letter
- Sent response securely
- Recorded our decision making and closed on the DSAR Log

You can also refer to our [DSAR white paper](#) for additional information.

WHY CHOOSE THE DPO CENTRE?



Handling Data Subject Access Requests (DSARs) can be complex, time-consuming and legally sensitive. That's where we can help.

EXPERT-LED, SCALABLE SUPPORT

With one of the largest teams of specialist data protection professionals and a dedicated DSAR team, we provide tailored support to fit your organisation's needs. Whether you need full end-to-end management or assistance with specific tasks.

CONFIDENCE IN EVERY RESPONSE

Outsourcing your DSARs to us means peace of mind.

With our expertise, you reduce risk, save time, and stay compliant, allowing your team to focus on core business priorities.



KEY BENEFITS

- ✔ Designated DPO and specialist DSAR Officers working with your team
- ✔ Stress-free compliance, with end-to-end DSAR management
- ✔ Flexible pricing options, including pay-as-you-go and retainer plans

WHO WE'VE WORKED WITH

We have delivered consultancy, interim support, EU and UK Representation, DSAR Response and Data Protection Officer services to over 1,000 organisations across a wide range of industry sectors since 2017.



Medical and Healthcare



Software and Technology



Retail and eCommerce



Finance and Insurance



Education, Schools and Colleges



Charities and Not-for-profit





OUR KEY LOCATIONS



+44 (0) 203 797 1289

hello@dpocentre.com

www.dpocentre.com



DSAR RESOURCES

Scan this QR code to access additional DSAR resources from The DPO Centre.

About The DPO Centre

The DPO Centre is a leading provider of fractional Data Protection Officer and AI governance services for organisations operating in UK and EU markets. With offices in London, Toronto, New York, Dublin, Amsterdam, and a network of representation establishments across all 27 EU Member States, the company is uniquely positioned to support organisations across multiple jurisdictions.

The DPO Centre provides access to one of the largest teams of experienced and permanently employed DPOs and AI compliance specialists. Since 2017, the company has worked with over 1,000 clients across a wide range of industry sectors, including Finance, Tech, Life Sciences, and Retail.

The DPO Centre is part of Axiom GRC, a global governance, risk and compliance platform, serving over 40,000 clients and 2 million users globally.

Amsterdam • Dublin • London • New York • Toronto

☎ +44 (0) 203 797 1289

✉ hello@dpocentre.com

www.dpocentre.com

