NORTON ROSE FULBRIGHT

UK Pensions Briefing: Dealing with a Data Subject Access Request

May 2022

Introduction

We have recently seen an increase in pension scheme members using Data Subject Access Requests (**DSARs**) to extract information from scheme trustees and sponsoring employers. This is linked both to members becoming more aware of their right to their personal data and Claims Management Companies (**CMCs**) encouraging members to use a DSAR to fish for information.

Members may make such requests for various reasons, from simply wanting to know what information the data controller holds to trying to obtain information in the context of a dispute with the data controller.

Responding to a DSAR can be a significant endeavour in terms of time and costs, however failure to comply could result in enforcement action from the Information Commissioner's Office (**ICO**).

In this briefing, we offer some practical tips for dealing with a DSAR in a pensions context. Our Norton Rose Fulbright Pensions and Data Protection teams are available to assist if you need help responding to a DSAR or would like to explore training or a health check in this area.

What is a DSAR?

Under data protection laws, an individual has a right to request access to all of their personal data held by a data controller (such as pension scheme trustees or their current or previous employer) or on its behalf by its processor. A request of this kind is known as a Data Subject Access Request (or DSAR).

The individual will need to be provided with a copy of their personal data (or access to this) as well as certain other supplementary information which largely aligns with the information that should be provided in a privacy notice.

Can a Data Controller refuse to comply with a DSAR?

A data controller can refuse to comply with all or part of a DSAR where the request is manifestly unfounded or manifestly excessive.

These thresholds are interpreted very narrowly but examples include where a request:

- Is manifestly intended to cause disruption such as being sent once a week.
- Targets a particular individual against whom the data subject has a grudge, making unsubstantiated allegations.
- Includes a request for something in return for withdrawing it.
- Repeats the contents of a previous DSAR within a very short time-frame where the personal data is unlikely to have altered in the interim.

Care must be taken as unjustified rejections can be regarded as infringements of a data subject's rights

and can be subject to the exercise of the corrective powers of the ICO as described below.

What are the risks of not complying with a DSAR?

You should take great care when receiving and responding to DSARs. If a data controller does not comply with the relevant legislation then the ICO can take action against them including levying substantial fines. Failure to comply with a DSAR can also lead to the data subject applying for a court order requiring compliance or seeking compensation.

Can we charge a fee?

Usually, you will be unable to charge a fee for responding to the DSAR. However, if a DSAR is manifestly unfounded or manifestly excessive, you can charge a 'reasonable fee,' for the administrative costs of complying with the request – you should think carefully before imposing this.

Do we need to provide all the personal data requested?

A data subject does not have an automatic right to a copy of **all** the data that is held about them by that controller. Certain exemptions may apply and will need to be considered. The principal exemptions are:

- Where there is third party personal data mixed with the data subject's personal data – there may be a need to get that third party's consent to disclose the personal data.
- Where the disclosure of the personal data could prejudice the prevention and detection of crime.
- Where the personal data is subject to legal professional privilege.
- Where the personal data records intentions in relation to negotiations with the data subject, which would be likely to prejudice those negotiations if disclosed.
- Where the personal data consists of material which is processed for management forecasting or planning and disclosure would be likely to prejudice such activity.
- Where personal data is processed for the purpose of providing a confidential reference (for example, an employee reference).

How can pension schemes deal with a DSAR?

When a DSAR is received from a current or former scheme member, trustees and / or sponsoring employers will have a lot to work through under immense pressure. Action points include:

Step 1: Review your readiness

Rather than waiting for a DSAR to land, consider proactively putting in place a policy for dealing with DSARs and drafting a template response letter in readiness. This should assist you with running an efficient review and response process if required.

You could also consider obtaining training on DSARs to ensure that the relevant individuals are well-prepared to respond to the request within the tight timeframe afforded.

Step 2: Identify the DSAR

This is the first challenge and an area where training can be very helpful. DSARs can come in all shapes and sizes – including via social media - as there is no specific request format required by law. The DSAR also need not be in writing as an oral request is sufficient. So they are not always easy to spot!

Step 3: Watch the clock!

Unless you can classify the DSAR as complex, you will usually only have one month to provide a response. Take care to plan your review process around this deadline.

Whether you can regard a request as complex will depend on the circumstances of your internal resources and the contents of each DSAR. Potential factors include technical difficulties in retrieving the information (e.g. electronically archived data) or large volumes of particularly sensitive information.

Step 4: Check identities

Before you disclose any personal data, especially any special category data, you need to make sure you know the identity of the person making the request. If you are uncertain about the identity of the requester then you can ask for reasonable additional information to verify this, but this should not be more than the information initially needed for the verification of the data subject's identity (such as authentication). You should make sure that you do this promptly.

This is particularly important where a third party (such as a CMC) makes a DSAR on behalf of another individual. You must be satisfied that the third party has the authority to act on behalf of the individual.

The clock will not start ticking on your response to the DSAR until you have received the ID documents.

Step 5: What help do I need?

Consider who you will need to involve in your DSAR response. For trustees, it is likely that the scheme's administrator will manage the process but trustees should ensure they understand the administrator's process and that their contract includes appropriate obligations on the administrator and protections for the trustee. Employers should consider whether they need assistance from HR or IT teams.

You may also consider it prudent to obtain legal advice on how to deal with the DSAR, particularly where the request or the circumstances surrounding it are complex or where you believe the DSAR may be manifestly unfounded or manifestly excessive.

Step 6: Identify the search parameters

Review the DSAR, decide what it is requesting and set reasonable search parameters including:

- What potential person identifiers to search for (such as names, email addresses, telephone number, NI number, and date of birth).
- What the start and end dates for the search should be.
- Where the information might be held (i.e. hard copy files, back-up servers for deleted items etc.).
- What types of data are within scope (e.g. hard-copy documents, emails etc.)

You are not required to conduct exhaustive searches that would be unreasonable or disproportionate but you should be able to justify this conclusion. Keep a record of the search parameters selected and the reasons behind these selections.

Step 7: Review the potential material

Review the material which your searches have generated and consider:

- Are you the data controller for this material and if not, can / should you disclose it? This may be particularly acute for company-nominated trustees who will need to take some care to decide which data was generated in their company capacity versus their trustee capacity. Trustees in this situation should ensure their correspondence and documents are stored separately for their different roles where possible.
- Can or should the data be redacted or withheld, e.g. because of legal professional privilege, third-party personal data or confidential references (see above for more detail on exemptions)?

Keep an audit trail of the decisions you make and your reasons for making them. You may also like to engage legal assistance to conduct a second-line review, particularly in applying the exemptions.

Step 8: Provide a response

The final step is to respond to the data subject with a copy of any findings or materials identified after following the steps above.

Remember that you do not always have to actually provide copies of documents or emails. For example, if you find emails which the data subject is copied into as a recipient which contain no information or personal data relating to the individual other than their name and email address, then it is sufficient to advise the data subject that you identified their name and email address within a

specified number of emails and disclose to them the name and email address associated with those emails. You do not need to provide each email.

You should include a covering letter which includes points such as, a brief explanation of the searches conducted and any exemptions applied and enclose a copy of your privacy notice. You should make the requestor aware of their right to complain to the ICO or to seek to enforce their rights through the courts.

What's next?

In the autumn of 2021, the Government consulted on plans to reform the DSAR process as part of wider data protection reforms following the UK's exit from the European Union.

The Government has proposed allowing data controllers to charge a fee for responding to a DSAR over a certain cost limit and to make it easier to refuse to deal with all or part of a DSAR if it is vexatious.

The consultation closed on November 19, 2021, and we now await the Government's response to the feedback received. While the proposed reforms are welcome from a trustee and employer point of view, we expect to continue to see a steady stream of DSARs as members become increasingly aware of their data protection rights.

Contacts

Lesley Browning

Partner
+44 20 7444 2448
lesley.browning@nortonrosefulbright.com

Shane O’Reilly

Partner
+44 20 7444 3895
shane.o’reilly@nortonrosefulbright.com

Law around the world

nortonrosefulbright.com