SQUIRE PATTON BOGGS

Pensions Quick Guide

Data Subject Access Requests

What Is a Data Subject Access Request (DSAR)?

Under both the UK's post-Brexit law relating to personal data protection (UK GDPR) and the EU General Data Protection Regulation (EU GDPR) ("Data Protection Laws"), an individual has the right to be informed, on request, whether personal data relating to that individual is being processed by or on behalf of a data controller — such as the trustees of a pension scheme (this right is subject to very limited exceptions). A DSAR is a request made by an individual for access to this personal data. UK pension trustees might be required to comply with both UK GDPR and EU GDPR, depending on individuals' location.

There is no prescribed format for making a DSAR. It can be made verbally, or in writing on paper or in electronic form. A request does not have to include the phrase "subject access request", as long as it is clear that the individual is asking for access to their own personal data. A simple letter/email stating "Please supply to me all personal information that you hold about me" would be sufficient. This does not prevent a body or organisation from having a prescribed form for submitting DSARs, but it is not permitted to make compliance with the DSAR conditional on the form being completed.

What Is Personal Data?

The Data Protection Laws only give individuals access to personal data held about themselves. On this basis, nothing else needs to be provided under a DSAR other than the individual's personal data. "Personal data" refers to any information relating to a living individual who can be identified from that information, or from that information combined with other information that might be sought out from other reasonably available sources by a "motivated inquirer" to identify an individual.

Whether information constitutes personal data is context specific, and whether a particular item is personal data is not always immediately obvious. Information or documents that do not provide information about the person making the request and that do not have that person as their subject matter will generally not constitute personal data. An example of when they might is if the DSAR stems from the fact that the individual was not aware of something and the document shows they were/were not sent the information.

Similarly, if another email in the chain is needed to give context to an email containing personal data, then this should be included. For example, if an email says "Please let me know who received an overpayment" and the next email in the chain says "[NAME]", both emails would likely constitute personal data.

How Long Do Trustees Have to Respond to a DSAR?

The information requested in the DSAR has to be supplied to the individual promptly and within one month of receipt of the request. If the DSAR is particularly complex or there are numerous requests, this period is extendable by a further two months (if necessary) subject to informing the individual of the extension within one month of receipt of their request and explaining why the extension is necessary. The one-month period runs from the day the request is received until the corresponding calendar date in the next month, irrespective of whether the day the request is received is a working or non-working day. If the next month is shorter and there is no corresponding calendar date, trustees have until the last day of that month to respond.

According to the guidance published by the Information Commissioner's Office (ICO), if the corresponding date in the following month falls on a weekend or a public holiday, trustees have until the next working day to respond.

If evidence is needed to confirm the individual's identity, then the time limit for responding to the DSAR will start when this additional information is provided. Note, the trustees should only request identification if they have reasonable doubt about the identity of the person making a request. If the trustees need to ask for identification, they should only request necessary information and it should be requested as soon as possible.

What Data Must Trustees Provide?

Trustees should provide personal data held electronically (on servers and other devices, including laptops, phones and tablets) or in hard copy form to the extent that it is within a "filing system" as defined in the Data Protection Laws. Hard copy information will form part of a "filing system" if such information is readily accessible/indexed so that specific information about a specific individual can be easily found (e.g. A to Z filing allowing quick retrieval of an individual's information, such as personnel files).

If personal data held in hard copy format does not form part of a "filing system", the Data Protection Laws do not apply to that data and trustees do not have to provide access to such information.

Remember that electronically stored personal data might be held in more than one way. This could include email boxes, documents held on servers, CCTV footage, phone call recordings, messages sent through SMS, WhatsApp, instant messenger, etc., where the controller or processor provides or controls the device or account and other electronic information held on behalf of trustees by third parties. Multiple copies of the same data do not have to be provided.

Where the trustees process a large quantity of information about the data subject, the trustees may wish to enter into a dialogue with the individual and request that individual to specify the information or processing activities to which the request relates. We recommend seeking legal advice before entering into such a dialogue.

What Actions Should Trustees Take?

Step 1 – Acknowledge receipt of the DSAR promptly and request any further information that is required in order to complete the request or verify the individual's identity.

Step 2 – Determine the search parameters. When working out what to search for and where, consider the wording and context of the request and specifically:

- The appropriate identifiers for the individual, i.e. "first name" or "surname" or "initials" or "job title". You should also consider whether other identifiers are appropriate, e.g. abbreviated names or nicknames, maiden name, member ID, etc.
- The nature or subject matter of the information sought
- The time period in respect of which the information sought relates
- Which mailboxes/devices/accounts should be included in the search
- Which categories of documents should be searched, e.g. emails, documents, member files, text messages, call recordings or even CCTV footage, etc.

Step 3 – Filter out non-relevant material. For example, if the request was "all data relating to my transfer value request", it may not be necessary to provide all data relating to membership.

Step 4 – Assess the relevant material. Are there any reasons why the contents should be redacted or withheld entirely? For example, documents might contain the personal data of other persons, or they might be subject to legal privilege. The Data Protection Laws contain a number of exceptions to the right to access personal data. Seek legal advice if you are unsure what information to disclose.

Step 5 – Print off and review a hard copy file so that you can check it does not contain anything unexpected that is not visible on screen (having already reviewed on screen).

Step 6 – Provide the material with covering correspondence, which should describe the scope of the search undertaken and why some documents have been redacted or withheld.

What Other Information Should Be Provided to the Requester?

Certain additional information must always be provided to the requester, including:

- The purposes of the processing
- The categories of the personal data concerned
- The recipients or categories of recipients to whom the personal data has been or will be disclosed
- Any disclosures of or access to personal data outside of the European Economic Area, including the safeguards in place relating to the disclosure
- The period for which the personal data is to be retained or, if not possible, the criteria used to determine the period

Much of this information may already be provided in the trustees' privacy notice. It may be appropriate to include a further copy of the notice with the response. If it contains all the necessary information, it is sufficient simply to provide the notice.

How Must the Data Be Provided?

According to ICO guidance, if an individual makes a request electronically, trustees should provide the information in a commonly used electronic format, unless the individual requests otherwise. Dispatch should always be carried out in a secure manner (e.g. using encryption if sent by email or if you allow the individual to access it electronically). Documentation sent by post should be sent by courier or recorded delivery with acknowledgement of receipt.

Should Trustees Rely on Their Administrators to Deal with Subject Access Requests?

It is the trustees, as controllers, who have the responsibility to respond to subject access requests, and who will be held responsible if they are not responded to or are dealt with incorrectly. Trustees need, therefore, to work closely with their administrators in dealing with such requests. The data protection agreement with an administrator should contain assurances that the administrator will cooperate with the trustees in relation to any subject access request. While the administrators will have a key role in collating documents for provision to the individual, it is recommended that they be received by or for the trustees and the response letter is sent from the trustees.

Some Practical Points

Do	Don't
Do take legal advice if you are unsure which documents, records and/or information to disclose.	**Don't** assume every request for information is a DSAR. If it seems likely that an individual is simply looking for access to a specific piece of information, clarify that with the individual and deal with the request informally if the individual is happy with that approach. This is likely to save both time and costs!
Do verify the identity of the person making the DSAR.	**Don't** charge a fee for complying with the DSAR (although there is limited scope to levy reasonable fees if requests are "manifestly unfounded" or "excessive").
Do deal with every DSAR. The motive behind a DSAR is irrelevant, even if the trustees think that the request has been made in connection with potential or future litigation or as a fishing expedition.	**Don't** delay contacting scheme administrators and other trustees to ensure that assistance is available to carry out the search quickly and efficiently in order to meet the statutory deadline.
Do keep a detailed audit trail setting out the reasons behind any decision to clarify the scope of a DSAR and/or to withhold information, as well as the search parameters employed.	**Don't** make responding to a DSAR conditional on completion of specific documentation or forms.
Do consider whether to provide additional documentation that might assist a member with their query even if it does not contain personal data, such as a relevant policy.	**Don't** supply documents without checking them first – make sure to redact personal data relating to other persons. If the person can still be identified, consider taking legal advice as to whether you can withhold the document.

What Are the Consequences of Failing to Comply?

If the trustees fail to comply with the data subject access requirements of the Data Protection Laws, the ICO has the power to take enforcement action, including, for the most serious breaches, issuing a fine of up to £17.5 million (or up to 4% of the total annual worldwide turnover of an organisation in the preceding financial year, if higher) under UK GDPR or €20 million (or up to 4% of the total annual worldwide turnover of an organisation in the preceding financial year, if higher) under EU GDPR.

Contact

Philip Sutton
Partner, Birmingham
T +44 121 222 3541
E philip.sutton@squirepb.com