SQUIRE PATTON BOGGS

LOCAL GOVERNMENT ASSOCIATION

PROCEDURE FOR HANDLING DATA SUBJECT ACCESS REQUESTS (DSARS) FOR ADMINISTERING AUTHORITIES

1. This procedure note has been prepared for the Local Government Association. We understand that copies will be provided to Local Government Pension Scheme administering authorities in England and Wales and Scotland. **This procedure note will need to be interpreted by administering authorities in accordance with its specific circumstances.** Accordingly we accept no liability to administering authorities unless we provide formal advice specific to that authority.
2. This procedure note is not advice to other connected or stakeholder parties, their auditors or other advisers, or other third parties ("**Third Parties**"). Other than as noted in paragraph 1 above, no part of this procedure note may be passed on to Third Parties without our written agreement but, if it is so passed, we accept no responsibility, and will have no liability in contract, tort or otherwise, to those Third Parties in relation to this procedure note.
3. This procedure note has been prepared based on an understanding of the law (including taking into account the data sharing guidance issued by the Information Commissioner) as at the date of issue. In particular, the Information Commissioner may issue further guidance which may be relevant and case law is still developing in this area. Accordingly, it is possible that this procedure note will need to be updated if the law changes or guidance is revised. However, we will only do so if the Local Government Association specifically give us written instructions to do so.
4. This procedure note (which forms part of a series of documentation on dealing with DSARs, including a Guidance Note and template letters) has been prepared for administering authorities, solely in their capacity as:
   a. administering authorities; and
   b. controller of personal data relating to the Local Government Pension Scheme fund for which they are responsible;

   to set out the procedure for handling a DSAR received directly from a data subject or via a claims management company or legal firm. DSARs that are wider in scope than the parameters in (a) and (b) above (for example, if the administering authority is also the current or former employer of the data subject and the DSAR also relates to information held by the

administering authority in that capacity) are not covered by this procedure note.

5. We have not considered or advised on any tax or commercial implications that administering authorities may wish to consider in conjunction with this procedure note.

Squire Patton Boggs (UK) LLP

February 2022

PROCEDURE FOR HANDLING DATA SUBJECT ACCESS REQUESTS

INTRODUCTION

This procedure has been specifically designed for use by Administering Authorities, solely in their capacity as administering authority, when responding to a data subject access request (DSAR) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. References in this procedure note to "you" include the individual at the Administering Authority responding to the DSAR and references to "Administering Authority" are to the administering authority acting solely in its capacity as administering authority.

It should be noted that unless the DSAR is limited to a response from the Administering Authority in its capacity as an administering authority (in which case, the Administering Authority can respond on that basis), then the Administering Authority would need to respond to the DSAR in all of the capacities in which it processes personal data relating to the data subject and to which the DSAR relates; if the council also processes personal data relating to the data subject in another capacity, the DSAR will need to be referred to other departments where necessary. For full guidance, please see the Information Commissioner's Office's (ICO) guidance on handling a DSAR or seek further legal advice.

The template letters referred to in this procedure note are designed to allow Administering Authorities to respond to DSARs addressed to the Administering Authority in its capacity as administering authority, provided the template letters are adapted as required based on the complexity and scope of the DSAR. Please note that dealing with a DSAR that is sent to the Administering Authority in more than one capacity and / or relates to personal data other than that in respect of the Local Government Pension Scheme fund for which it is responsible for, is outside the scope of this procedure note. The template letters have different wording that can be selected depending upon whether the DSAR has been received directly from an individual or via a claims management company or legal firm. The template letters will however not be suitable for all DSARs (for example DSARs addressed to the administering authority in its capacity as a council, which are outside the scope of this procedure note) and specific advice should be sought where an Administering Authority has any queries or concerns.

The **Template Acknowledgement Letter** is a straightforward acknowledgement of the DSAR, with optional wording if it is necessary to verify the identity of the data subject or whether the data subject's representative has authority to submit the DSAR on behalf of the data subject.

The **Template Acknowledgement and Request Letter** incorporates a request for further information to clarify the scope of the DSAR, should this be permitted (i.e. where an Administering Authority processes a large amount of data regarding the data subject) and necessary based on how wide the scope of the request is.

The **Template Acknowledgement and Extension Letter** informs the data subject / the data subject's representative that the Administering Authority is exercising its right to extend the timeframe for responding by a further 2 months on the basis that the DSAR is complex, and the reasons as to why it is complex. In practice, most DSARs within the scope of this Procedure Note and the Guidance Note will not be complex.

The **Template Response Letter** includes the supplementary information that is required to be given in response to a DSAR, in addition to a copy of the data subject's personal data, as well as a description of the searches performed in order to provide the personal data.

STEP 1 - DSAR RECEIVED

The first step is receiving a DSAR. There is no prescribed format for making a DSAR. It can be made verbally or in writing by or on behalf of the data subject, to any individual at the Administering Authority. The request does not have to include the phrase 'subject access request' or reference the UK GDPR, as long as it is clear that the data subject or data subject's representative is asking for their / the data subject's personal data. A simple email from a data subject (or on behalf of a data subject) stating "*please supply a copy of all personal data that you hold in relation to me / [NAME]*" would be sufficient.

If the DSAR references the Freedom of Information Act (FOIA), but in fact relates to the data subject's personal data, you must still treat the request as a DSAR. It is not uncommon for a DSAR to mistakenly request that it is a FOIA request. If it is clear that the data subject / the data subject's representative is asking for the data subject's personal data, but they have cited the FOIA, you should follow certain actions:

- Deal with the request as a DSAR in the normal way. The data subject / data subject's representative does not need to make a new request.
- Clarify within 20 working days (the time limit for responding to a FOIA request) that the Administering Authority is dealing with the request as a DSAR under the UK GDPR and that the one month time limit for

responding applies. There is sample wording set out in the Template Acknowledgement Letter to include this information in such cases.

If the request relates to both the data subject's personal data and to other information, you should treat it as two requests: one for the data subject's personal data, made under the UK GDPR, and another for the remaining information, made under the FOIA. Please note that dealing with a FOIA request is outside the scope of this procedure document and the documentation referenced within it.

KEY ACTIONS AT STEP 1

1. Where a DSAR is made verbally by the data subject, you should record details of the data subject's request in writing by way of an internal memo as soon as possible, together with the date of the request. If the request is made verbally on behalf of the data subject, you should make a written request for evidence of the representative's authority to act on behalf of the data subject (as set out below) and include details of the verbal request in that correspondence, to ensure there is a written record of it.
2. Where the DSAR is purportedly made from the data subject (rather than via a claims management company or a legal firm) it is also important to ensure that you are satisfied that the data subject is who he / she says they are before you send them any information or documents. For example, if you receive a DSAR by email from a personal email address that you do not recognise, this may cause reasonable doubts about the identity of the data subject making the request. Under the UK GDPR, if you have reasonable doubts, you should request additional information necessary to confirm the data subject's identity, e.g. copy of a passport or driving licence. However, you should only request ID information where it is not obvious that the data subject is who they say they are. The Template Acknowledgement Letter includes optional wording asking for ID.
3. If you receive a DSAR from a third party on behalf of the data subject (including from a solicitor or a claims management company), you should always ask for evidence that the third party has authority to make such a request on the data subject's behalf. The evidence may be a simple written authority signed by the data subject, an email from the data subject's known email account, or something more formal, such as a power of attorney. The Template Acknowledgement Letter includes optional wording to incorporate such a request.
4. Check whether any further information is required in order to locate the information requested. Where the Administering Authority processes a large

amount of information about the data subject, you can ask the data subject / the data subject's representative for more information to clarify the scope of the DSAR. You should consider the scope of the request and the extent to which you may need to ask the data subject / data subject's representative to specify the information to which the request relates. You may want to instruct the fund's administrators to carry out an initial search against the parameters set out in the DSAR and confirm how many emails / documents this search generates. The higher the number, the more reasonable it will be for you to seek clarification; you may wish to clarify with the data subject / the data subject's representative to which capacity (or capacities) of the council the DSAR relates, if it is not clear (although as noted above, DSARs that are wider in scope than those solely relating to the Administering Authority acting in its capacity as administering authority, are outside the scope of this procedure note).

5. Send a response to the data subject / data subject's representative stating that their request is being dealt with and verifying their identity / authority if necessary (Template Acknowledgement Letter), or, where it is necessary and permitted, a response requesting further clarification (Template Acknowledgement and Request Letter), promptly on receipt of the DSAR. Where the DSAR has been received via a claims management company or a legal firm, the template letters will need to be adjusted accordingly.

STEP 2 – DETERMINE THE SEARCH PARAMETERS

By this stage, you will have either determined that the request will generate a low number of results or that it may generate a high number of results but have further clarification in order to prepare more focused search parameters. If the DSAR was limited to specific named documents, it may not be necessary to carry out an electronic search at all.

KEY ACTIONS AT STEP 2

1. On receipt of any additional relevant information requested from or on behalf of the data subject about their DSAR, you should consider whether you will need the assistance of other business departments (IT, HR, Legal etc.) to comply with the DSAR.
2. You should now prepare the search parameters you will use to conduct the search. When assessing your search parameters, you should consider the wording and context of the request, and specifically:
   a. the appropriate identifiers for the data subject, which unless told otherwise would usually consist of: "first name" OR "surname" and

National Insurance number. Consider whether other identifiers are appropriate, e.g. abbreviated names or nicknames, maiden name, employee ID, role, member number etc. Please note that the more name identifiers you input, the higher the number of hits that will be returned;

b. the nature or subject matter of the information sought;
c. the time-period in respect of which the information sought relates;
d. the individuals whose mailboxes should be included in the search (note that where the data subject has transferred-out of the fund there may not be any appropriate individuals);
e. what categories of documents should be searched, e.g. emails, letters, documents, etc. This would also include any searches for hard copy documents stored in a manual filing system (please see the DSAR Guidance for further details);
f. if necessary, keyword search terms. For example, if the request is to obtain documents relevant to a transfer out of pension benefits, you could include keywords such as "transfer", "CETV", "cash equivalent" etc.

Electronic documents should be searched, as far as possible, automatically by the fund's administrators. We anticipate that in the majority of cases all the information for responding to the DSAR will be contained in the pensions administration system. If there is any relevant information held elsewhere then additional searches should be conducted as appropriate (e.g. by the council's IT team). This is to ensure that where items are retrieved from individual mailboxes (rather than from a central electronic database like the pensions administration system), those individuals are not able to filter the items that they send to the person responding to the DSAR for review. Unless there are good reasons as to why an automated search cannot be performed, the mailbox custodians should not be asked to assist with identifying and searching for relevant electronic documents / emails. This is also important in order to preserve the confidentiality of the fact that a DSAR has been submitted by the data subject.

3. Once the parameters have been prepared, the fund administrators (or council's IT team where appropriate) will need to extract the data and assess how many unique 'hits' have been identified. If the number of 'hits' exceeds 4,000 items, you should look to focus the parameters of the search further.

4. You should always keep a detailed audit trail setting out the reasons behind the decision to focus the scope of a request, as well as the search parameters used.

STEP 3 – PERFORM THE REVIEW

Once you have carried out the search, taking into account any clarified scope to result in a figure that you consider to be a reasonable starting point, you will need to perform a review of the items for the data subject's personal data. The number of items that may be considered reasonable will depend on a number of factors, including the Administering Authority's resources, but around 4,000 items is estimated to be a reasonable number for most businesses.

KEY ACTIONS AT STEP 3

1. STAGE 1 REVIEW: FILTER OUT NON-RELEVANT RESULTS

a. The first step of the review will be to identify which information/documents fall within the definition of personal data, as identified in the Guidance Note. Depending on the scope of the DSAR and the search terms used, it is possible that some of the emails / documents returned may not contain the data subject's personal data. For example, they may relate to a different individual sharing the same first or last name; if documents held outside the pensions administration system require searching, they may simply be a day-to-day work email that refers to the data subject's name in an address field or in passing. The first sift may involve categorising the documents into those that do contain the data subject's personal data and those that do not.

b. The Administering Authority is not required to provide information that does not constitute the data subject's personal data.

2. STAGE 2 REVIEW: ASSESS THE RELEVANT RESULTS

a. Once the stage 1 review has narrowed down the search results to only those items containing the data subject's personal data, the second sift will usually be a deeper dive into the results, to assess whether there are any reasons why the results should be redacted or withheld entirely. This may be for a number of reasons, such as:

   i. **Items including third party personal data:** in this case, unless the third party has consented, you should carry out a balancing exercise assessing the rights of the data subject against the third party's right to privacy. See the 'reasonableness test' set out in the Guidance Note.

Before taking any decision to withhold the information, you should consider whether it is appropriate to provide the information in redacted form, deleting all references to the third party if necessary. If the identity of the third party is still obvious, you may consider withholding the entire document. Note that whilst the third party may consider the information about them to be confidential and its disclosure to be sensitive / damaging, it may still fall under the scope of the UK GDPR and may therefore need to be disclosed to the data subject or their representative. You also need to bear in mind that should the subject matter of the information be subject to potential litigation in the future, it may be disclosable at a future date and in unredacted form as part of those proceedings. If this occurs, the data subject / data subject's representative will likely question why the information was withheld from the DSAR response, so you need to ensure there are valid grounds for any redactions applied and / or information being withheld.

ii. **Personal data subject to legal privilege:** information constituting either legal advice privilege (i.e. confidential communications between an internal or external lawyer and the Administrating Authority for the purpose of giving or receiving legal advice), or litigation privilege (i.e. communications once litigation has commenced, or concerning contemplated litigation, where the dominant purpose is for it to be used in respect of the litigation or to obtain legal advice about the litigation), should be removed.

b. Redactions can be made electronically (if the software in use permits) or on hard copy. When redacting, the editing or deletion of information in the document needs to be permanent, i.e. the individual receiving the information should not be able to scratch correction fluid off or read through information that has been deleted with a marker pen.

c. You should always keep a detailed audit trail setting out the reasons behind the decision to disclose or not disclose any particularly sensitive data (e.g. special category personal data).

3. STAGE 3 REVIEW: PERFORMING A QUALITY CHECK OF THE RELEVANT RESULTS

By way of a quality control check, you should carry out a third stage review of the disclosable, redacted items. This should be performed by a different person to the one who performed stages 1 and 2 above.

STEP 4 – PROVIDE THE DOCUMENTATION, WITH A COVER LETTER

Once you have completed the review, you should prepare a cover letter to accompany the documents that will be disclosed to the data subject / data subject's representative. In particular, the letter should briefly describe the scope of the search undertaken and describe why some of the documents have been redacted (i.e. because they contain third party personal data). Wording is provided in this respect in the Template Response Letter.

KEY ACTIONS AT STEP 4

1. Prepare the cover letter using the Template Response Letter, which contains wording informing the data subject / data subject's representative of the data subject's right to lodge a complaint with the ICO, and the existence of the data subject's rights to rectification, erasure or restriction of personal data or to object to the processing of the data subject's personal data.
2. Check the applicable Administering Authority's privacy notice to ensure that it covers the following information:
    a. the purpose of the processing;
    b. the categories of personal data concerned;
    c. the recipients or categories of recipients to whom the personal data has been disclosed;
    d. any disclosures of or access to the personal data outside of the UK / European Economic Area, including the safeguards in place relating to the transfer;
    e. the period for which the personal data is to be preserved or, if not possible, the criteria used to determine the period;
    f. where the personal data was not collected from the data subject, information about the origin of the personal data; and
    g. details of any automated decision-making using the data subject's personal data, including meaningful information about the logic involved, as well as the significance of and the envisaged consequences of such processing for the data subject.

If any of the above information is not provided in the privacy notice, add wording covering these details to the cover letter. If you have engaged third party assistance with the DSAR, then you should also ensure that a copy of the privacy notice of the relevant third party is also provided to the data subject / data subject's representative.

3. Include with the finalised covering letter a copy of all disclosable data. As the right is a right to personal data (rather than raw documents / emails), you may choose to lift the disclosable information from the item and collate it in a separate document, rather than providing the data subject / data subject's representative with whole email chains / documents. This can, however, sometimes be more time consuming and / or costly than simply providing the data subject / data subject's representative with the items, redacted as appropriate. You should ensure that you keep copies of all the information that has been disclosed to the data subject / data subject's representative (both the redacted and non-redacted versions).
4. If the data subject / data subject's representative makes a request electronically, you should provide the information in a commonly used electronic format, unless the data subject / data subject's representative requests otherwise. Where electronic copies are to be provided, a password should be applied to the documentation and supplied to the data subject / data subject's representative by another means (e.g. by SMS message). Documentation sent by post should be sent by courier or recorded delivery, with acknowledgement of receipt.
5. As indicated above, you should keep a detailed audit trail of any decision-making process, in case there is ever a complaint or investigation by the ICO. It is important that you are able to justify any decisions not to disclose any particular type of information and the parameters used in the search.

This procedure has been provided as an indication of the steps that should be taken by Administering Authorities upon receiving a DSAR. What is required to be disclosed or withheld will significantly vary depending on the specific circumstances and the context and nature of each request. If you are in any doubt over whether or not to disclose any specific type of information, we recommend that you seek legal advice to ensure you remain compliant with your obligations under the UK GDPR and Data Protection Act 2018.

DSAR PROCEDURE FLOWCHART [DIAGRAM IS NOT ACCESSIBLE CONTENT]