SQUIRE PATTON BOGGS

LOCAL GOVERNMENT ASSOCIATION

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

1. This guidance 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 guidance 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 guidance 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 guidance 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 guidance note.
3. This guidance 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 guidance 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 gives us written instructions to do so.
4. This guidance note (which forms part of a series of documentation on dealing with DSARs, including a Procedure 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 guidance on 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 council in that capacity) are not covered by this guidance 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 guidance note.

Squire Patton Boggs (UK) LLP

February 2022

Version 1: valid from **11 May 2022**

GUIDANCE FOR HANDLING DATA SUBJECT ACCESS REQUESTS

INTRODUCTION

This guidance note has been specifically designed to assist Administering Authorities with handling a data subject access request (a 'SAR' or 'DSAR' – referred to as a "DSAR" for the purposes of this note) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Its purpose is to allow Administering Authorities to recognise a DSAR and carry out their own assessment of the documentation and further information that is required to be disclosed in response to a DSAR. For full guidance, please see the Information Commissioner's Office's (ICO) guidance or seek further legal advice.

THE DSAR

WHAT IS A DATA SUBJECT ACCESS REQUEST?

Under Article 15 of the UK GDPR, an individual (**data subject**) is entitled to be informed that their personal data is being processed, have access to their personal data, be provided with a copy of their personal data and be given specific 'supplementary information' about their personal data. A DSAR is the exercising of this right by or on behalf of a data subject. Any data subject, or their representative, can submit a DSAR to any data controller, therefore as Administering Authorities are data controllers, they may receive a DSAR.

There is no prescribed format for making a DSAR. A DSAR can be made verbally or in writing. 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 the data subject's representative, is asking for their personal data. A simple email stating "*please supply a copy of all my personal data that you hold*" would be sufficient. Please note – a DSAR is distinct from a Freedom of Information Act request, which is outside the scope of this guidance note.

There may be circumstances where all that the data subject, or the data subject's representative, is looking for is access to a specific piece of information or specific document, for example, they may simply have mislaid this information or document. In such cases, the recommendation is to supply the requested information or document and deal with the request informally.

In some cases, Administering Authorities may receive multiple DSARs from or on behalf of the same data subject. The UK GDPR does not limit the number of DSARs that a data subject can make (either directly or through a representative) to any

organisation, although it does provide an exception where a request is 'manifestly unfounded' or 'manifestly excessive' (see below).

Unless the DSAR is limited to a response from the Administering Authority in its capacity as administering authority (in which case, the Administering Authority can respond on that basis), 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. Please note that dealing with a DSAR which 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 which it is responsible for, is outside the scope of this guidance note.

WHAT IS PERSONAL DATA?

"Personal Data" means any information relating to a **living** individual who can be identified from that information, or from that information combined with other information in the possession of the data controller. For example, a person's contact details, employment status, bank details and even the opinion that somebody holds about a person are all Personal Data.

In the context of Personal Data in relation to the Local Government Pension Scheme fund for which the Administering Authority is responsible for and in addition to the data subject's member file in the pensions administration system, this could include information contained in emails, electronic messaging services, Word documents and any other method of recording information. Administering Authorities are only required to provide personal data in respect of which they are the data controller (please note that Administering Authorities may hold personal data in respect of the data subject in more than one capacity which is outside the scope of this guidance note). This means that it is not necessary to supply personal data stored on someone else's computer, mobile device or database unless they are a data processor acting on behalf of the Administering Authority. Examples of a data processor would include IT service providers and payroll service providers. In practice, we would expect the vast majority (if not all) of the personal data that Administering Authorities hold in that capacity to be contained within the data subject's member file in the pensions administration system.

There are certain types of personal data, known as 'special category personal data', which are particularly sensitive and therefore need additional protection. Special category personal data includes personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs and/or trade union membership, genetic data, biometric data (where used for identification purposes) and data concerning health, as person's sex life and/or a person's sexual orientation. Administering Authorities must take extra caution to redact any third party special category personal data within DSAR documentation.

TIMESCALES

HOW LONG DO ADMINISTERING AUTHORITIES HAVE TO RESPOND TO A DSAR?

Administering Authorities have one month from either the date that the DSAR is received, or, if it is necessary to verify the identity of the data subject or the third party submitting the DSAR on behalf of the data subject (see below), from the date that identification is provided.

The time limit for responding starts from the day of receipt of the DSAR (or identification), whether or not that day is a working day and regardless of the time of receipt. The time limit runs until the corresponding day of the next month. If that date falls on a bank holiday or on a weekend, the deadline for responding is the next working day. If there is no corresponding date in the following month, i.e. because the next month is shorter, it should be the last day of that month.

Examples:

- The DSAR/identification is received on Tuesday 31 May 2022. The deadline for responding is Thursday 30 June 2022.
- The DSAR/identification is received on Thursday 23 June 2022. The corresponding day of the next month is Saturday 23 July 2022, so the deadline for responding is Monday 25 July 2022.

CAN THE TIMESCALE FOR RESPONDING BE EXTENDED?

Yes, in two circumstances:

1. 'Stopping the Clock'
   If the Administering Authority processes a large amount of information about a data subject, they can ask the data subject / data subject's representative to clarify the scope of their request. The time limit for responding to the request is paused until the data controller receives clarification and no information needs to be provided to or in respect of the data subject until such clarification is received. This is referred to as 'stopping the clock'. There is no obligation to seek clarification and so unless data cannot be searched for without the

clarification, the Administering Authority can carry out a reasonable search and so should not normally seek to pause the time limit in this manner. There is no express guidance on what is a reasonable search although there is a high expectation placed upon data controllers to find the information requested through a DSAR. A reasonable search would be one that is not unreasonable or disproportionate to providing the information; the Administering Authority would have to justify why a search is unreasonable or disproportionate.

2. 'Complex' requests
   The timescale for responding can be extended by a further two months (i.e. to three months from the date of receipt of the DSAR/identification) where the request is complex. Whether or not a request is complex depends on the specific circumstances of each DSAR and the data controller in question. The size and resources of an organisation are normally relevant factors.
   The Information Commissioner's Office's (ICO) guidance sets out some examples of factors that may, in certain circumstances, increase the complexity of a request, such as technical difficulties in retrieving the information, the need to apply a particular legal exemption to a large volume of particularly sensitive information, needing to obtain specialist legal advice beyond that routinely required or requested. Note that the volume of data requested or reviewed as part of handling a DSAR is not likely to result in a DSAR being considered 'complex'. An Administering Authority should seek legal advice before exercising its right to extend the timescale for responding on the basis that a request is complex. Typically, however, an Administering Authority is likely to be considered to have the resources to process the majority of DSARs they will receive within the normal one month timescale.

THE DATA

WHAT DATA MUST ADMINISTERING AUTHORITIES PROVIDE IN RESPONSE TO A DSAR?

Administering Authorities must provide a **copy** of the Personal Data requested and that is in existence at the time that the DSAR is made to the data subject or the data subject's representative. If Personal Data relating to the data subject has been 'filleted' in accordance with UK GDPR prior to the DSAR (by deleting Personal Data that is no longer required, for example following a transfer-out of the Local Government Pension Scheme fund), only the remaining Personal Data can be provided to the data subject / the data subject's representative.

It is normally easiest to provide copies of the documents containing the Personal Data, with appropriate redactions applied. However, data subjects are entitled to a copy of their Personal Data, and not the document itself, so this can be provided in another form, such as copying the applicable data into a separate schedule. The approach taken will depend upon the amount of data requested and the resources of the Administering Authority.

WHERE MUST ADMINISTERING AUTHORITIES SEARCH FOR THE DATA?

Administering Authorities should provide Personal Data held electronically (on servers and electronic devices including laptops, phones and tablets) or held in hard copy form, to the extent that it constitutes a 'relevant filing system'. Information will form part of a 'relevant filing system' if it is readily accessible/indexed in such a way that specific information about a specific data subject can be easily found, e.g. an A to Z filing system allowing quick retrieval of a data subject's information.

If Personal Data held in electronic or hard copy form does not form part of a relevant filing system, then it does not fall within the scope of a DSAR, and an Administering Authority does not have to provide access to it. A common example would be where Personal Data is contained in an unorganised notebook, included as part of general and mixed notes.

Electronically stored Personal Data relating to the pension fund will usually be held in:

- member files/records held electronically in the administration system;
- documents and emails held in email mailboxes or any other electronic messaging service used;
- documents and information held on servers, such as minutes of meetings, timesheets, etc. (whether in Word, Excel, PowerPoint or any other format);
- phone-call recordings; and/or
- information falling in the above categories but held by third parties on the Administering Authority's behalf.

Administering Authorities are only obliged to provide Personal Data in respect of which they are the data controller. Administering Authorities are not expected to ask employees to search their private emails or personal devices, unless they have good reason to believe that the relevant employee(s) are holding relevant personal data.

IS THERE DATA THAT IS NOT RELEVANT AND/OR SHOULD NOT BE INCLUDED?

Whether or not information constitutes Personal Data will need to be assessed on a case-by-case basis. For example, if a data subject is copied into an email but the subject matter of the email is not them and does not contain any information about them, this would not be their Personal Data.

The Information Commissioner's Office's (ICO) guidance contains details on determining whether information is Personal Data. If another document or email in an email chain is needed to give context to the email containing the Personal Data, then this should also be included. For example, if there is an email which says "*please let me know who has complained about their ill health pension*" and the next email in the chain includes the data subject's name, both emails should be included.

UK data protection law (the UK GDPR and Data Protection Act 2018) also sets out certain exceptions to when Personal Data must be provided. The most common exceptions are:

- **Confidential references** given or received by the data controller for educational, training or employment purposes.
- Personal data processed for the purposes of **management forecasting or management planning** in relation to a business or other activity, but only to the extent that complying with the DSAR would prejudice that conduct of the business or activity.
- Documents containing **third party personal data** (in certain cases).
- Documents that are subject to **legal professional privilege**.
- Personal data that consists of records of the intentions of the data controller in relation to any **future negotiations** with the data subject, but only to the extent that complying with the DSAR would be likely to prejudice those negotiations.

The most common form of data that needs to be redacted or withheld is **third party personal data**. Under data protection law, there is no obligation to comply with a DSAR if it would mean disclosing information relating to another individual who can be identified from that information unless: (a) the other individual has consented; or (b) it is reasonable to disclose the information without their consent.

With regard to (b) above, whether or not it is reasonable to disclose the information will need to be assessed on the basis of a 'reasonableness test'. As part of this test, Administering Authorities should consider:

- The type of information that would be disclosed (how personal it is (e.g. salary details), whether it constitutes 'special category personal data' (e.g. health data) etc.)
- Any duty of confidentiality owed to the other individual.
- Any steps taken to get the consent of the other individual.
- Whether the other individual is capable of giving consent.
- Any express refusal of consent by the other individual.
- Whether the data subject has previously received the information e.g. they were originally included in the email chain.

There is a continuous balancing act that must be performed between the data subject's right to access their personal data, and the third party's right to privacy. It may be possible to redact the third party data in question, but if this is not sufficient to anonymise the data in question then it may be necessary to withhold the information.

MUST ANY OTHER INFORMATION BE PROVIDED?

Yes. The following supplementary information must be provided:

- the purpose for which the data subject's personal data is being processed;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been disclosed;
- 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;
- the period for which the data subject's personal data is to be retained, or if not possible, the criteria used to determine that period;
- where the data subject's personal data was not collected from themselves, information about the origin of the personal data; and
- 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.

The above supplementary information, which incorporates that set out in Article 15 UK GDPR, should be contained in the privacy notice that the Administering Authority has provided to the data subject.

In addition, Administering Authorities also need to inform the data subject / data subject's representative of: (a) the data subject's right to lodge a complaint with the

Information Commissioners Office (ICO); and (b) the existence of the data subject's rights to rectification, erasure or restriction of personal data or to object to the processing of their personal data. This information is contained in the template covering response letter, which should be tailored and provided to data subjects / data subjects' representatives with their DSAR documentation.

ACTION

WHAT ACTION SHOULD ADMINISTERING AUTHORITIES TAKE IN RESPONSE TO A DSAR?

Please see the Procedure Note for detailed information on the actions that need to be taken in response to a DSAR.

SHOULD AN ACKNOWLEDGEMENT LETTER BE SENT?

Yes. Transparency is key, so the data subject / data subject's representative should be sent a letter or email to confirm receipt of the DSAR and confirm that it is receiving attention from the Administering Authority in question. Please see the Template Acknowledgement Letter.

If more information and/or an extension to the deadline for responding to the DSAR is required, these requests can be built into the acknowledgement letter. Please see the Template Acknowledgement Letter Requesting More Information and the Template Acknowledgement and Deadline Extension Letter.

SHOULD COVERING LETTERS BE PROVIDED?

Yes. Please see the Template Response Letter.

WHAT ABOUT GOVERNANCE/AUDIT TRAILS?

Administering Authorities should ensure that all employees know how to identify a DSAR and that there is a single point of contact for handling DSARs that solely relate to the Administering Authority, in capacity as administering authority and being the controller of Personal Data relating to the Local Government Pension Scheme fund to which they are responsible (e.g. a DSAR relating to the data subject's transfer out of the fund or the data subject's application for an ill health early retirement pension). Records of correspondence with the data subject / data subject's representative, the searches performed, decision making and the final response should be maintained in order to provide a record of handling the DSAR should the data subject / the data subject's representative subsequently complain to the ICO.

HOW

HOW MUST ADMINISTERING AUTHORITIES PROVIDE THE DATA?

The data should be provided in writing or, if appropriate, by electronic means. If the DSAR was originally made by electronic means, e.g. in an email, then the data should be provided in a commonly used electronic form unless otherwise requested by the data subject. In practice, this will normally be a PDF file.

The electronic documents should be password protected and where possible, sent via a secure link. The password to access the documents should be sent separately in a different form, e.g. by SMS message.

If either the data subject or the data subject's representative requests it, the data can be provided verbally provided the Administering Authority in question is satisfied as to the identity of the data subject and/or authority of the data subject's representative to act on behalf of the data subject; a written record of the information provided verbally should be kept.

Remember that the response needs to include not only the data, but the supplementary information required under Article 15 UK GDPR (refer to section headed "Must any other information be provided" above).

LEGAL CONSIDERATIONS

WHAT AUTHORITY IS NEEDED TO SUBMIT A DSAR ON BEHALF OF SOMEONE?

A data subject may prefer a third party, such as a relative, a claims management company or a solicitor, to make a DSAR on their behalf. This is permitted, but before proceeding to action the DSAR, Administering Authorities need to ensure they are satisfied that the third party who submits the DSAR has the authority to act on behalf of the data subject. It is the third party's responsibility to provide evidence of this.

If a third party submits a DSAR on behalf of a data subject, Administering Authorities should ask for the third party to submit evidence that they have the right to act on behalf of the data subject. Appropriate evidence may include written authority signed by the data subject, stating that they give the third party permission to make a DSAR on their behalf, a valid power of attorney, or written evidence that they have been instructed to submit the DSAR as the data subject's relative/solicitor/claims management company.

SHOULD THE DATA SUBJECT / DATA SUBJECT'S REPRESENTATIVE BE VERIFIED? IF SO, HOW?

If a third party submits a DSAR on behalf of a data subject, the evidence described above should be requested if the Administering Authority is not satisfied that the third party has the authority to act on behalf of the data subject and to submit a DSAR.

Where a data subject submits a DSAR on their own behalf, and Administering Authorities are unsure of the data subject's identity, appropriate evidence of identity should be requested. This may be the case where a data subject submits a DSAR via email, from an email address that the Administering Authority does not have on file for that data subject. In order to verify the identity of the person making the request, the Administering Authority should request a copy of the data subject's driver's license, passport, member number or other form of ID. However, this should only be requested where there is reasonable uncertainty as to the identity of the data subject / data subject's representative. For example, if the data subject is a current employee and they submit the DSAR from their work email address, it would be unreasonable to ask that they verify their identity.

CAN ADMINISTERING AUTHORITIES REFUSE TO COMPLY WITH A DSAR? IF SO, IN WHAT CIRCUMSTANCES?

Yes. If a DSAR is 'manifestly unfounded' or 'manifestly excessive' then an Administering Authority may either charge a reasonable fee or refuse to act on the request. This is subject to providing the data subject / data subject's representative with reasons as to why the DSAR is either manifestly unfounded or excessive, and informing them of the data subject's right to complain to the ICO or apply to the Courts. There is currently minimal guidance on what would constitute a manifestly unfounded or excessive request, but the inclusion of the word 'manifestly' means there must be an obvious or clear quality to the unfoundedness or excessiveness of the DSAR.

A DSAR may be manifestly unfounded if:

- the data subject / data subject's representative clearly has no intention to exercise the data subject's right of access, e.g. if they submit a DSAR but then offer to withdraw it in return for some form of benefit (please note this would likely not include an offer to withdraw a DSAR as part of an overall settlement in relation to a pension benefit claim raised by or on behalf of a data subject); or
- the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption, e.g. if the data subject /

data subject's representative explicitly states that they intend to cause disruption, makes unsubstantiated accusations against specific employees that are clearly prompted by malice, systematically sends different DSARs to an organisation on a regular basis with the intention of causing disruption, or targets a particular individual (such as an employee and/or another pension scheme member) against whom they have a personal grudge.

The Administering Authority must consider each request in the context of which it is made. There is no tick box exercise that can be performed to decide whether a DSAR is manifestly unfounded.

A DSAR may be *manifestly excessive* if it is clearly or obviously unreasonable, taking into account all of the circumstances of the DSAR including:

- the nature of the information requested;
- the context of the request, and the relationship between the Administering Authority and the data subject;
- whether a refusal to provide the information or even acknowledge whether the Administering Authority holds it, may cause substantive damage to the data subject;
- resources available to the Administering Authority;
- whether the request largely repeats previous requests and a reasonable interval has not elapsed; or
- whether the request overlaps with other requests and does not relate to a completely separate set of information.

A DSAR is not likely to be excessive simply because the data subject / data subject's representative requests a large amount of information, or the Administering Authority holds a large amount of information about the data subject. Each DSAR must be considered individually to determine whether it is proportionate when balanced with the burden or costs involved in deadline with it.

The burden lies on the Administering Authority to demonstrate that the request is in fact manifestly unfounded or excessive. The Administering Authority should therefore only use such grounds for refusing to comply with a DSAR in very exceptional circumstances, where there are strong justifications for considering the request to be manifestly unfounded or excessive that can be clearly demonstrated to the data subject / data subject's representative and to the ICO. The Administering Authority should instead seek to provide what it can and/or seek to clarify the scope of the DSAR, rather than refuse to comply with the request altogether.

MUST THE DATA SUBJECT BE INFORMED THAT A DSAR HAS BEEN ISSUED ON THEIR BEHALF?

A DSAR can only be issued on behalf of a data subject by a third party who has the authority to do so. If a third party issues a DSAR on behalf of a data subject, the Administering Authority should request the evidence described above to satisfy itself that the data subject has authorised that third party to do so.

WHAT IS THE RELEVANT LEGISLATION?

The legislation governing DSARs is the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

INTERNAL DISPUTE RESOLUTION PROCEDURE (IDRP)

HOW (IF AT ALL) DOES THE LGPS IDRP FIT INTO THE DSAR PROCEDURE?

A DSAR is separate and distinct to a complaint made under the LGPS IDRP, as explained below.

- A DSAR is where an individual exercises their rights under Article 15 of the UK GDPR to be informed that their personal data is being processed, have access to their personal data, be provided with a copy of their personal data and be given specific 'supplementary information' about their personal data. A DSAR is made to a data controller and need not relate to pension matters. Should the data subject have a complaint about the way in which a DSAR has been dealt with, a complaint can be made to the ICO. The data subject may also wish to raise a complaint under the LGPS IDRP should the DSAR reveal information regarding their LGPS pension (see further below).
- The IDRP is a formal two stage procedure which is in place to resolve disagreements about decisions taken regarding LGPS pension matters. The requirements are set out in regulations 74 – 79 of the Local Government Pension Scheme Regulations 2013 (**LGPS Regs 2013**) and regulations 69 – 74 of the Local Government Pension Scheme (Scotland) Regulations 2018 (**LGPS (Scotland) Regs 2018**). Administering Authorities will also have their own IDRP policy document which will set out who will look at a 'Stage 1 IDRP' and confirm who will look at a 'Stage 2 IDRP' (we note that in Scotland a 'Stage 2' IDRP is determined by Scottish Ministers). Should the individual not be content with the outcome of the Stage 2 LGPS IDRP, a complaint can be made to the Pensions Ombudsman. The individual may also wish to submit a DSAR during or following conclusion of their LGPS IDRP.

- Raising a DSAR does not prevent a data subject from raising a LGPS IDRP (assuming that the data subject is eligible to do so in accordance with the applicable legislation and Administering Authority's IDRP) and vice versa.
- A DSAR and LGPS IDRP can be run in parallel or separately; care will need to be taken to ensure that the timescales applying to the respective DSAR and LGPS IDRP are complied with.

SOME ADMINISTERING AUTHORITIES HAVE RECEIVED STAGE 1 IDRP COMPLAINTS IN RELATION TO PAST TRANSFERS. THE COMPLAINTS ARE WELL OUTSIDE OF THE TIME LIMITS LAID DOWN IN REGULATION 74(2) OF THE LGPS REGS 2013 AND REGULATION 69(2) OF THE LGPS SCOTLAND REGS – ARE THEY ADMISSIBLE?

The time limits applicable to bringing a Stage 1 IDRP is within six months of the date of the notification of the decision or the act or omission about which you are complaining **or such longer period as the adjudicator considers reasonable.**

It is therefore for the Administering Authority to make a decision on what may be a reasonable longer period. In reaching that decision, the Administering Authority may wish to take into account of the date of the individual's knowledge about the act or omission which the complaint relates to; for example if the individual only recently became aware of the issue being complained of:

- despite the act or omission that led to the issue arising, occurring more than 6 months before the Stage 1 IDRP being raised;
- as a result of a DSAR.

WHEN PAYING A TRANSFER (AFTER RECEIVING THE MEMBER'S ELECTION TO TRANSFER UNDER SECTION 95 OF THE PENSION SCHEMES ACT 1993) SHOULD ADMINISTERING AUTHORITIES ADVISE THE MEMBER OF THEIR RIGHT TO APPEAL THE PAYMENT OF THE TRANSFER UNDER REGULATION 73 OF THE LGPS REGS 2013 AND REGULATION 68 OF THE LGPS (SCOTLAND) REGS 2018?

There is no obligation for Administering Authorities to inform a member of their right to appeal the payment of a transfer, as set out in regulation 73 of the LGPS Regs 2013 and regulation 68 of the LGPS Scotland Regs; however, there is nothing to prevent the Administering Authority from providing this information to the member should it wish to do so.

The Administering Authority should ensure that processes are in place to comply with the requirements to pay a transfer under The Occupational and Personal Pension Schemes (Conditions for Transfers) Regulations 2021.

ADDENDUM – FOLLOW UP QUESTIONS

WHY DOES CONFIDENTIALITY NEEDS TO BE PRESERVED WITHIN THE DATA CONTROLLER IF INFORMATION IS ONLY SHARED BETWEEN PEOPLE WHO WORK FOR THE DATA CONTROLLER?

There are several reasons as to why confidentiality needs to be preserved, including accountability.

Accountability is one of the data protection principles and an area the ICO is particularly hot on at the moment. This principle makes controllers take accountability for what is done with personal data, including taking demonstrable steps to protect data subject's rights (one of which is the right of access). This links in with the key principle of security, i.e. controllers process personal data securely by means of 'appropriate technical and organisational measures' that must ensure the 'confidentiality, integrity and availability' of controller systems, services and the personal data processed within them.

The fact that a data subject has made the DSAR (either directly or through a CMC / solicitor) is in itself that data subject's personal data. Individuals submit DSARs for all sorts of reasons, not all of which are clear and some of which can be particularly sensitive. Further, the action of searching for and collecting personal data in order to respond to a DSAR is all processing of that personal data, which should be done in a secure and confidential manner. As such, from a security perspective: (a) the existence of a DSAR should only be notified to those members of staff who actually need to be aware of it in order to respond; and (b) processing of personal data to respond should be undertaken in a manner that limits access to that data where possible (e.g. automatic searches are performed remotely by an IT team, who do not review the data in question but simply provide the results to those members of staff who will be reviewing the search results and preparing the response to the DSAR).

From a practical perspective, the more people who know about and may discuss the DSAR on email etc., then the more personal data being created about the data subject. There is nothing to stop the data subject / data subject's representative submitting a later DSAR requesting this information. We know from previous experience that sometimes employees put unhelpful comments in writing on the assumption it will never be seen by the individual in question, only to have it later disclosed in response to a DSAR. The best way to counter this risk is to keep the existence and handling of the DSAR limited to specific individuals who are trained on the process and aware this could happen.

Finally, the UK GDPR requires controllers to ensure that anyone acting under their authority and with access to personal data do not process that data unless the controller has instructed them to do so. There is a risk that staff may delete emails they would prefer not to be disclosed if they know that an individual has made a DSAR, which is an offence under the Data Protection Act 2018.

HOW MUCH INFORMATION SHOULD BE PROVIDED WHERE A THIRD PARTY REQUESTS COPIES OF ALL THE DATA RELATING TO A MEMBER WHEN IT IS OBVIOUS THE REQUEST RELATES TO A PREVIOUS TRANSFER OUT. IN THESE CASES, CAN THE FUND JUST SEND THE INFORMATION THEY THINK IS RELEVANT TO THE TRANSFER OUT OR SHOULD THEY INCLUDE ALL THE DATA THEY HOLD FOR THE MEMBER INCLUDING, NEW STARTER DETAILS, SALARY DETAILS, DEFERRED BENEFIT CALCULATIONS, DIVORCE CALCULATIONS ETC.

Strictly speaking, no, but in practice it would depend on the circumstances of the request.

If the request explicitly says that the data subject / data subject's representative wants all personal data then the first step should be to search for all personal data; this is a request that the data subject is entitled to make, even if the Fund has additional context suggesting what they are really after is data relating to a previous transfer out.

The Administering Authority could write to the data subject / data subject's representative acknowledging the request and clarifying whether the data subject / data subject's representative is looking for something specific, such as personal data related to a previous transfer out.

- If the data subject / data subject's representative replies stating that they do want all of their personal data and there aren't a high number of results returned by the preliminary search, the Administering Authority should disclose all of the personal data returned (following a review and redaction process).
- If the data subject / data subject's representative replies stating that there are only specific items they would like, then the Administering Authority can disclose those (rather than all personal data).

If the results of the initial search are large enough and potentially include such a large amount of third party personal data that reviewing all of the items would arguably constitute a disproportionate invasion of third party rights (e.g. the results include thousands of emails), then the Administering Authority should then consider options for focusing the search on what the data subject / data subject's

representative is actually concerned about; we understand from the scope of DSAR requests covered by the sample documentation we have provided to date, this is unlikely to be an issue in practice.

The key is that the Administering Authority performs the wider search first to: (a) confirm this is actually the case; and (b) have a figure for the number of items returned by the wider search to support an argument that it processes a large amount of personal data about the data subject (and can therefore clarify the request in accordance with ICO guidance) and demonstrate that the number is so high that it would be disproportionately invasive on third parties to review all of the results. In these circumstances, we would recommend one of the following approaches:

1. If the request included a list of items under the wording “including but not limited to”, such as in the example letter, the Administering Authority may consider it reasonable to perform a further, more focused search for only those items. If this option is taken, it may not be necessary to write to the data subject / data subject’s representative first as we advise in option 2 below, but there is nothing to prevent the Administering Authority from doing so. That said, tactically if a list was provided already then writing to just confirm that list gives the data subject / data subject’s representative the opportunity to object, which puts the Administering Authority in a difficult position if the wider search leaves it with an unmanageable number of items to review. Assuming the Administering Authority does not write to the data subject / data subject’s representative using the Template Acknowledgement and Request Letter, it nevertheless needs to ensure that it includes the appropriate wording in the response letter to explain what it has done (see drafting note 9 (DN9) in the Template Response Letter).

2. If no specific items were included in the request, but the Administering Authority has context to indicate what the data subject / data subject’s representative is after, again it might be reasonable to search for just that data. In this instance, it is more appropriate for the Administering Authority to write to the data subject / data subject’s representative using the Template Acknowledgement and Request Letter and ensure that letter is worded to clarify the Administering Authority’s understanding (drafting note 8 (DN8) in the Template Acknowledgement and Request Letter). Again, this will not always be the appropriate approach, but will depend on each individual case. Whether or not the Administering Authority writes to the data subject / data subject’s representative to clarify its understanding, when providing the final response to the data subject / data subject’s representative the Administering Authority needs to ensure it includes the appropriate wording in the response letter to explain what it has done i.e. if no clarification is sought, drafting note 9 (DN9) in

the Template Response Letter, or if clarification is sought, drafting notes 6 (DN6) and 7 (DN7), as well as 8 (DN8) if applicable).

3. If no specific items were included in the request and there is nothing to indicate exactly what the data subject data subject's representative wants, the Administering Authority should write to the data subject / data subject's representative using the Template Acknowledgement and Request Letter with the wording for requesting information (see drafting notes 6 (DN6) and 7 (DN7) in the Template Acknowledgement and Request Letter). Again, when responding with documentation and drafting the response letter, the appropriate explanation of steps taken needs to be included (drafting notes 6 (DN6) and 7 (DN7), as well as 8 (DN8) if applicable of the Template Response Letter).

Notwithstanding the above, it is impossible to avoid a data subject / data subject's representative eventually complaining about the approach taken to handling the DSAR and the decision to only search for certain data, if they are / it is dissatisfied with the response. There is also no guarantee that the ICO will agree with the approach that the Administering Authority takes, although even if they disagree they would usually tend to direct the Administering Authority as to how they wish a further search to be performed. However, the Administering Authority needs to ensure that if it is limiting a response to only certain personal data, it acts in a manner that is reasonable, proportionate and transparent and that it is accountable. The Administering Authority should keep records of all decisions made, as well as copies of all correspondence with the data subject / data subject's representative, and ensure it is comfortable that it can present an arguable approach to the ICO if a complaint is subsequently made. The above options are intended to support an arguable approach for focusing the search for data.