SQUIRE PATTON BOGGS

LOCAL GOVERNMENT PENSION SCHEME (LGPS)

GENERAL DATA PROTECTION REGULATION - THE IMPLICATIONS FOR THE LGPS

INTRODUCTION

Thank you for providing us with a list of questions and background information in relation to the General Data Protection Regulation ("**GDPR**"), which is due to come into force on 25 May 2018.

We have been asked to provide a report setting out our response to these questions to the Local Government Association, ultimately for distribution to the administering authorities of the LGPS. For ease of reference, a copy of the list of questions as well as the additional questions raised in your email dated 17 October 2017 are appended at Appendix 1. This report sets out our response to those questions. When answering your questions we have considered the provisions of the draft Data Protection Bill which was published on 14 September 2017. That legislation could be amended during its progress through Parliament and so the position under UK law could ultimately be different to that set out in this report (although we are not anticipating any significant changes). We have not been instructed to consider any other issues in relation to the impact of the GDPR on the LGPS or any of the administering authorities. We would draw your attention to Appendix 2, which sets out the scope of our advice.

I note that you raised two additional questions in relation to additional voluntary contributions ("**AVCs**") and the general concern regarding the ability of the AVC provider to propose AVCs to scheme members under the GDPR. We have dealt with these questions under 2 below.

We have set out each of your questions and answered them in turn below.

CONSENT

1 In your view, is member consent (either explicit or otherwise) needed for administering authorities to process members' personal data for the below purposes:

As a general point we recommend that reliance on consent as a justification for processing of data by administering authorities be avoided where another lawful basis for processing can be relied on. This is because consent has to be freely given and individuals have to be free to withdraw consent at any time. If consent is withdrawn, the administering authority would then have to cease processing the data concerned and this is unlikely to be practical in many cases.

1.1 **For the fulfilment of administering authorities' obligations under scheme regulations and overriding legislation (i.e. the basic administration of the scheme)?**

(a) Article 6 of the GDPR provides that the processing of personal data is lawful only if:

(i) the data subject (i.e. the member or beneficiary) has given his consent to the processing of his personal data;

(ii) processing is necessary for the performance of a contract to which the data subject is a party or to take steps to enter into a contract at the request of the data subject;

(iii) processing is necessary for compliance with a legal obligation on the controller;

(iv) processing is necessary to protect the vital interests of an individual;

(v) processing is necessary for the performance of a task carried out in the public interest; and/or

(vi) processing is necessary for the purpose of a legitimate interest.

(b) Trustees of private sector schemes typically rely on point (vi) - i.e. they need to hold and process personal data to fulfil the purposes of the pension trust. However, having considered Article 6 and the recitals of the GDPR, point (vi) does not apply to processing carried out by public authorities. Therefore, we do not think administering authorities can rely on point (vi).

(c) However, we do not consider that consent for the processing of personal data to carry out basic administration of the LGPS is required, as the processing by the administering authority will be necessary for compliance with a legal obligation. This is because administering authorities in England and Wales are required to comply with the LGPS Regulations 2013 and administering authorities in Scotland are required to comply with the LGPS (Scotland) Regulations 2014 (the "**LGPS Regulations**").

1.2 **To process special categories of member personal data?**

(a) Generally under Article 9 of the GDPR the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited subject to a number of exceptions.

(b) Article 9(2) provides these exceptions. Two of which are explicit consent or that the processing is necessary for carrying out obligations under employment, social security or social protection law (including pensions), or a collective agreement pursuant to Member State Law (i.e. the LGPS Regulations).

(c) Therefore there is a strong argument that the processing by an administering authority of special categories of member personal data will not require specific consent, on the basis that it is necessary to perform obligations under social protection law.

(d) However, in relation to health data, because consent is needed under the Access to Medical Reports Act 1988 we would typically recommend that administering authorities nonetheless seek explicit member consent when dealing with ill health early retirement applications.

1.3 **To process personal data relating to children?**

(a) As with 1.1, the processing of personal data in relation to children is required under the LGPS Regulations and therefore, where survivor benefits are payable to the child of a member, such processing would be lawful processing of personal data and the child's consent would not be needed.

(b) It should be noted that the GDPR contains provisions that are intended to enhance the protection of children's personal data, in particular in relation to privacy notices for children where services are offered directly to a child. We do not believe that consent will be needed if a beneficiary is a child. However, if privacy notices are provided to children then they would need to be drafted as simply as possible so that children are able to understand them.

(c) We are expecting guidance from the Information Commissioner's Office (**ICO**) in relation to the processing of children's data.

1.4 **To provide information about AVCs, including information sent to a) all scheme members, and b) targeted groups of members?**

(a) Regulation 17 provides that an active member may enter into an arrangement to pay AVCs. These arrangements must be a scheme established under an agreement between an administering authority and an AVC provider. Consequently, an administering authority must provide access to AVCs if an active member requests. Therefore, the provision of information to a member (or all scheme members) in relation to AVCs is required by Regulation 17 of the LGPS Regulations 2013 and Regulation 17 of the LGPS (Scotland) Regulations 2014. It would therefore be lawful processing of personal data to provide information about AVCs to the extent it is needed to satisfy these requirements.

(b) Providing information to targeted groups of members may amount to profiling under the GDPR. There are additional requirements that may need to be satisfied where an automated process is used to profile or market to groups of individuals - for example, to remind members who have just received a pay rise or whose benefits are below a certain threshold about the ability to pay AVCs.

(c) Article 22 of the GDPR protects individuals where an automated decision could result in a potentially damaging decision. Generally, Recital 71 provides that a member has the right not to be subject to an automated decision when it is based on automatic processing and produces legal effects concerning him or her, or similarly significantly affects him or her (for example an automatic refusal of an online credit application). If this is the case, the administering authorities would need to make sure that safeguards are in place, which include specific information to the member and allow the member to obtain human intervention, express his point of view and obtain an explanation of the decision and challenge the decision.

(d) This right does not apply to all decisions and, in particular, when a decision does not have a legal or similarly significant effect on a member. Given that the payment of AVCs is statutory, we do not anticipate that this additional protection would prevent targeted communications about AVCs to groups of LGPS members.

2 What is the legal basis for passing member data to the AVC provider and does the AVC provider need to obtain member consent?

(a) Article 6(1)(b) of the GDPR provides that processing is lawful if it is necessary for the performance of a contract with the data subject or to take steps to enter into a contract at the request of the data subject. The contractual form of particular AVC arrangements may provide a legitimate basis for processing personal data, but only where both the member and the administering authority are parties to that contract. Individual analysis will be required. In any event the administering authority can still rely on the grounds for lawful processing noted in 1.4 above.

(b) It should be noted that, unless the administering authority has provided the member with the required information under Article 14 (Information to be provided where personal data have not been obtained from the data subject), the AVC provider, when contacting the member on the basis of the above, will be required to provide this information to the member. Examples of this information includes the identity and contact details of the controller, the contact details of the data protection officer, the categories of the data concerned and a right to lodge a complaint. This is, however, more of an issue for AVC providers than administering authorities.

(c) We believe that it is likely that consent from the member would be required should the AVC provider contact the member direct to advertise and inform members of the product without the member first contacting the administering authority to request information about paying an AVC. This is because the legal obligation under the LGPS Regulations to provide access to AVC arrangements applies to the administering authority, not to the AVC provider. Therefore, administering authorities should not automatically provide AVC providers with members' personal data for these purposes.

(d) We do not consider it necessary in order to comply with the GDPR for the member to contact the AVC provider direct, based on the analysis above and the current practice of marketing AVCs. Provided the member has indicated to the administering authority that he or she wishes to pay AVCs, we are comfortable that the administering authority can rely on its obligation under the LGPS Regulations to provide access to AVC arrangements to justify passing the member's personal data to the AVC provider.

3 Where an LGPS fund already holds a member's email address for the purposes of disclosing information to them under the Disclosure Regulations 2013, does any action need to be taken by the administering authority to ensure the member consents to the holding of that email address from 25 May 2018 onwards?

3.1 We suggest that members are informed by way of the relevant administering authority's privacy notice setting out that they hold email addresses, the purpose for which they hold the email address and the other information that Articles 13 and 14 of the GDPR require to be provided to data subjects. Much of this information is likely to already be included in existing privacy notices, but we would recommend that they are reviewed as the GDPR does extend the amount of information that has to be given.

3.2 There is no special protection given to email addresses so no specific consent is required where there is a general justification for processing personal data (i.e. a legal obligation).

4 Where an LGPS fund no longer has a liability for a member (for example, because they opted out and received a refund), do administering authorities have the right to hold the personal data of that individual, on what grounds and for how long? In asking this, we draw attention to circumstances like GMP reconciliation and the tracing of lost pensions, where long term records of individuals' scheme membership can be beneficial to both the authority and the individual.

4.1 Recital 39 of the GDPR provides that personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Article 5(e) of the GDPR also provides that data must not be kept in a form that is capable of identifying an individual for longer than is necessary. In addition, the GDPR requires data controllers to inform individuals how long their data will be kept or (if that is not possible) at least the criteria that it will use when determining retention periods. It is therefore clear that personal data should not be kept any longer than necessary and time limits should be established by the controller (i.e. the administering authority of a LGPS fund) for erasure or for periodic review. However, the GDPR does not itself specify particular time periods after which personal data must be deleted.

4.2 As you have mentioned in your example, after a member has left the scheme there may be circumstances where they need to be contacted or traced or the scheme needs to be able to demonstrate how the liability was settled. For example, GMP reconciliation requires the administering authority to be able to demonstrate if and when liability was discharged; or to help a former member with tracing a pension liability.

4.3 It will be a question of fact as to the personal data that is retained under data retention policies in line with the GDPR and as pensions are very long term liabilities we are aware of a number of trustees who take the view they are justified keeping data for ex-members indefinitely and think that is arguable/defensible. We do not envisage a problem with that approach, provided that it results from some genuine analysis and appropriate steps are taken to keep the data secure. However, given the data should be held only for as long as is needed and only essential data should be retained we would encourage administering authorities to think hard about what is really needed. For example, after a member has transferred out it may be felt unnecessary to retain the salary and service data that was used to calculate the transfer value or their bank account details. Where it is possible to "fillet" the retained data to the bare essentials we think this would be helpful to comply with the GDPR.

4.4 Market practice in relation to the above will develop over time and this should be kept under review. Further, the use of approved codes of practice and certification mechanisms are endorsed by the GDPR. Whilst no such codes or certification schemes have currently been published or approved it is expected that they will be produced in due course and this may include codes of practice on the retention of data.

4.5 Each administering authority will therefore need to review the data it collects and weigh up whether or not to keep any personal data in relation to members who have left the scheme in line with the principles under Article 5 of the GDPR. Article 5 requires the administering authorities to show how they will comply with the GDPR. In particular Article 5(1) requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay. Article 5(2) of the GDPR sets out that the controller (i.e. the administering authorities) shall

be responsible for, and be able to demonstrate compliance with Article 5(1). We suggest policies are put in place/updated regarding the review, retention and deletion of personal data under the GDPR.

RIGHT TO ERASURE/RIGHT TO RESTRICT PROCESSING/PRIVACY BY DESIGN

5 Do members have a right to erasure in respect of personal data held by administering authorities for the purposes of the administration of the scheme? Does the position differ where the LGPS administering authority no longer has a liability for the individual?

5.1 Members have a right of erasure under the GDPR. However, it only applies in certain limited circumstances, such as where the data is no longer needed for the purposes for which it was being processed (see Article 17(2) of the GDPR).

5.2 We therefore do not consider that the administering authority would be obliged to erase data that is needed to be processed for the purposes of the administration of the scheme.

5.3 As discussed above, on the basis that the administering authorities keep under review the information they retain and can justify why they are retaining such information in respect of a former member for whom the LGPS fund no longer has a liability, they should be able to rely on the fact that the data needs to be retained for the purposes of administering the scheme and for archive purposes in the public interest.

6 Can a member utilise the 'right to restrict processing' to prevent an LGPS administering authority from processing their personal data and in what circumstances?

6.1 Article 18 provides that a data subject (i.e. a member) has a right to obtain a restriction on processing in the following circumstances:

(a) Where a member contests the accuracy of the personal data. In this case, the administering authority should restrict the processing until the accuracy of the personal data has been verified.

(b) Where processing is unlawful. This should not be relevant here as the administering authority should not be carrying out unlawful processing in any event.

(c) Where an administering authority no longer needs the personal data, but such data are required by the member in relation to legal claims. Again, this should not be relevant here as the administering authority would, by definition, not need to process the data.

(d) Where the data controller is processing the data on the basis that it is necessary to perform a public task or is in its legitimate interests, the data subject can require use to be restricted until the justification is verified. As noted previously, we consider that LGPS administering authorities will generally be able to rely on other justifications to process personal data.

6.2 The member must be informed when the administering authority decides to lift a restriction on processing.

7 What does 'privacy by design' mean for how administering authorities should approach data protection in their administration of the scheme? For example, would the adoption of a privacy by design approach mean that funds should not include personal data in communications sent to members even where there is a reasonable justification for doing so (such as including information so that members have the opportunity to correct inaccuracies)?

7.1 As part of the accountability principle, Article 25 of the GDPR requires controllers (i.e. the administering authorities) to incorporate data protection by design and by default into their systems and processes. This is to ensure that members are not exposed to unnecessary risks and that the administering authorities are only collecting the data that they need.

7.2 As regards privacy by design, Article 25.1 requires the administering authorities, both at the time of the determination of the means of processing and at the time of the processing itself, to implement appropriate technical and organisational measures designed to implement data protection principles in an effective manner, to integrate the necessary safeguards into the processing of personal data to meet the requirements of the GDPR and protect data subjects. This Article specifically contemplates that the decision as to what measures need to be taken should take into account the cost of implementation, the nature, scope, context and purposes of processing, and the risks to the rights of individuals posed by the processing.

7.3 Article 25.2 requires the controller to implement appropriate technical and organisational measures to ensure that, by default only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of storage and accessibility.

7.4 The ICO has provided guidance on "privacy by design", which is currently not codified under the Data Protection Act 1998 ("**DPA 1998**"). This guidance includes encouraging data controllers to carry out a privacy impact assessment, which is a tool that data controllers can use to identify the most effective way to comply with their data protection obligations. This will allow data controllers to identify and fix problems at an early stage and reduce any damage to reputation and any costs.

7.5 The administering authorities will need to design and implement compliant policies, procedures and systems to meet these requirements.

7.6 We would not expect 'privacy by design' to impact on the communications sent to members where there is a reasonable justification for including personal data in those communications.

THE ROLE OF THE ADMINISTERING AUTHORITY

8 Is the administering authority a data controller for the purposes of the administration of the LGPS, a joint data controller with the scheme employer or a data processor (with the scheme employer as data controller)?

8.1 In view of the amount of discretion that the administering authority has in administering their relevant LGPS fund, we consider that the administering authority will be a controller and not a data processor in relation to scheme data.

8.2 It is less clear whether there may be circumstances in which the administering authorities and the scheme employers are likely to be joint controllers, as the GDPR

itself gives very little guidance on the matter other than to state that there will be joint controllers 'where two or more controllers jointly determine the purposes and means of processing' of personal data. Our view is that if administering authorities and employers operate a joint database of pooled data then they would be joint controllers in relation to that data. However, simply providing a copy of an existing database to another party for them to then use for their own purposes will not be enough to create a "joint" database where the two copies are then held and processed separately.

8.3 Consequently, we anticipate it is most likely that scheme employers will be controllers of the personal data they pass to administering authorities. Those authorities will then assume responsibility as controllers of that data for the purposes of the scheme. In its capacity as administering authority and an employer in the scheme, the administering authority will have a dual role but the same legal responsibility.

8.4 We understand some administering authorities operate a practice whereby scheme employers are given access to parts of the pension administration system in order to view or update their members' records. In these circumstances the position is less clear and it would be necessary to analyse which party (i.e. the employer or the administering authority or both jointly) has the responsibility and whether there are data processing agreements in place setting out which party is a controller and which party is a processor. The outcome would be a question of fact based on each individual situation. We would be happy to advise on this point should an administering authority require further information.

9 What are the considerations that need to be borne in mind regarding data protection where the same legal entity has more than one role in respect of employee/scheme member personal data? How should any issues arising from this be managed?

9.1 The entity would need to have in place appropriate protocols and record in writing/document the different circumstances in which the entity is processing personal data. It would also need to be careful to ensure that where it holds personal data that it has obtained in one capacity, that it does not inadvertently use that data to perform its other roles.

9.2 Finally as a public body, each administering authority will be required to appoint a data protection officer. This should be a standalone function in order to avoid any conflict of interest. In other words, the data protection officer should not also have responsibility for an authority's use of personal data (for example, by being responsible for its role as administering authority of the LGPS fund).

10 Is the fund actuary appointed to provide services to an administering authority under the LGPS Regulations a data controller in respect of the personal data they have access to in fulfilling this role, a joint data controller with the administering authority or a data processor?

10.1 Whether the fund actuary is a data controller or processor will generally be a question of fact. The ICO and the Institute and the Faculty of Actuaries (**IFOA**) have published guidance in relation to processing of personal data. Although these guidance papers were published in 2014, we understand that the same principles will apply in relation to the GDPR.

10.2 Our view is that, if the fund actuary is personally appointed as fund actuary to the administering authority and is carrying out a specialist service, he will be acting as a data controller in relation to the processing of data in his role as fund actuary. This is

because the fund actuary will be exercising his professional judgement and consequently exercising a sufficient degree of control in processing the data to be categorised as a data controller and not a processor. This position should be distinguished from the situation where the fund actuary is acting on behalf of his firm as an employee where it is the firm that is providing actuarial services to the LGPS fund. In that case, the actuarial firm may be data processor and not a controller.

10.3 The IFOA sought confirmation from the ICO in relation to its view of scheme actuaries. The ICO confirmed that scheme actuaries are likely to be data controllers and will therefore have to comply with the DPA 1998 and have personal liability as a data controller.

10.4 Agreements should therefore be put in place between the fund actuary, his firm and the relevant administering authority setting out the actuary, the firm and the administering authority's classifications under the GDPR. The actuarial firm will however need to assess how data is processed in relation to its own contractual obligations and professional obligations as well as the obligations of the fund actuary. As mentioned above, this will be a question of fact as to how the data is processed as to whether the actuarial firm will be acting as a data controller or as a data processor. The classification will need to be assessed on an individual basis.

If you have any questions or would like to discuss this in any more detail then please contact Kirsty Bartlett or Stuart James.

Squire Patton Boggs (UK) LLP
27 October 2017

APPENDIX 1

The implications of GDPR for the LGPS

We would be grateful for a legal view on the below questions in respect of the implications for the Local Government Pension Scheme (LGPS) of the General Data Protection Regulation (GDPR), coming into force on 25 May 2018.

The questions asked are in respect of the LGPS in both England and Wales and in Scotland. Both schemes are occupational pension schemes registered under s153 of the Finance Act 2004 with scheme rules set out in statute. The scheme regulations for the LGPS in England and Wales are the LGPS Regulations 2013 (SI2013/2356) issued under the Superannuation Act 1972. The scheme regulations for the LGPS in Scotland are the LGPS (Scotland) Regulations 2014 (SSI2014/164) issued under the Public Service Pensions Act 2013. These two statutory instruments are referred to in this document as 'the LGPS Regulations'.

The schemes are administered locally by 'administering authorities', which are mainly local authorities and are listed in part 1 of schedule 3 of the LGPS Regulations 2013 and schedule 3 of the LGPS (Scotland) Regulations 2014.

Consent

Under the LGPS Regulations, administering authorities are required to provide their members with pensions in accordance with the provisions of the scheme and with overriding legislation. This requires the processing of scheme members' personal data.

In addition to providing members with a pension upon their retirement, the LGPS Regulations provide a range of other benefits on the meeting of certain conditions, including ill-health benefits and survivor pensions payable to members' spouses, civil partners and co-habiting partners. These aspects of the schemes' rules mean that administering authorities will sometimes hold information on the health and the sexual orientation of their members. (Administering authorities will know the sexual orientation of their members by virtue of knowing their marital status as well as the gender of their spouse and/ or partner.)

The LGPS Regulations also provide, in specified circumstances, for the payment of children's pensions upon the death of a member, requiring LGPS administering authorities to process personal data relating to children.

LGPS Regulations require administering authorities to offer scheme members the option of paying in-house additional voluntary contributions (IHAVC) to one or more providers with which the authority has entered into a contract. Administering authorities may issue information to scheme members about this option, including marketing products from their providers. Such information may be sent to all scheme members or to targeted groups (for example, those nearing retirement).

Q1. In your view, is member consent (either explicit or otherwise) needed for administering authorities to process members' personal data for the below purposes:

- **a) For the fulfilment of administering authorities' obligations under scheme regulations and overriding legislation (i.e. the basic administration of the scheme)?**
- **b) To process special categories of member personal data?**
- **c) To process personal data relating to children?**
- **d) To provide information about AVCs, including information sent to a) all scheme members, and b) targeted groups of members?**

Under the Occupational Pensions Schemes (Disclosure of Information) Regulations 2013 (SI2014/2734) (the Disclosure Regulations 2013), occupational pension schemes like the LGPS can disclose certain information to scheme members electronically, including via email. There is no requirement for occupational pension schemes to hold email addresses for their members or communicate with their members via email but many LGPS funds choose to do so and hold their members' email addresses for this purpose.

Q2. Where an LGPS fund already holds a member's email address for the purposes of disclosing information to them under the Disclosure Regulations 2013, does any action need to be taken by the administering authority to ensure the member consents to the holding of that email address from 25 May 2018 onwards?

In a variety of circumstances, LGPS administering authorities may have no further obligation to an individual in respect of rights they have previously had in the scheme. This can occur for example where an individual leaves and receives a refund of contributions or where a member transfers to another pension scheme. In such cases, records are often retained on systems for completeness and can be of use in future situations, such as:

- GMP reconciliation - this has required LGPS funds to be able to demonstrate if and when they have discharged a liability 20+ years after the event
- Tracing a pensions liability - if a member has lost track of their pension, they may approach the administering authority for details about when and where this has been transferred many years after the transfer took place.

Q3. Where an LGPS fund no longer has a liability for a member (for example, because they opted out and received a refund), do administering authorities have the right to hold the personal data of that individual, on what grounds and for how long? In asking this, we draw attention to circumstances like those noted above, where long term records of individuals' scheme membership can be beneficial to both the authority and the individual.

Right to erasure / right to restrict processing / privacy by design

Q4. Do members have a right to erasure in respect of personal data held by administering authorities for the purposes of the administration of the scheme? Does the position differ where the LGPS administering authority no longer has a liability for the individual?

Q5. Can a member utilise the 'right to restrict processing' to prevent an LGPS administering authority from processing their personal data and in what circumstances?

Q6. What does 'privacy by design' mean for how administering authorities should approach data protection in their administration of the scheme? For example, would the adoption of a privacy by design approach mean that funds should not include personal data in communications sent to members even where there is a reasonable justification for doing so (such as including information so that members have the opportunity to correct inaccuracies)?

The role of the administering authority

By virtue of regulation 53 of the LGPS Regulations 2013 and regulation 51 of the LGPS (Scotland) Regulations 2014, LGPS administering authorities in England and Wales and in Scotland are responsible for the management and administration of the LGPS as well as the maintenance of a pension fund for the payment of pensions.

Scheme employers play a vital role in the administration of the LGPS and are required to provide regular pay and contributions data to the administering authority for their scheme members. In particular, the LGPS regulations provide that annually scheme employers must provide specified items of personal data to the administering authority in respect of their scheme members including name, gender, date of birth and national insurance number (reg 80 of the LGPS Regulations 2013 and reg 78 of the LGPS (Scotland) Regulations 2014).

Q7. Is the administering authority a data controller for the purposes of the administration of the LGPS, a joint data controller with the scheme employer or a data processor (with the scheme employer as data controller)?

Administering authorities are also scheme employers in relation to their own employees who will, in most cases, also have access to the LGPS. Usually different parts of the organisation will be responsible for the different roles in relation to the LGPS but there will be crossover in some situations.

Q8. What are the considerations that need to be borne in mind regarding data protection where the same legal entity has more than one role in respect of employee/scheme member personal data? How should any issues arising from this be managed?

Additional questions raised in email dated 17 October 2017

Q8 – We are aware that some funds operate a practice whereby scheme employers are given access to parts of LGPS funds' pensions administration systems in order to be able to view or update their members' records. This can be useful so that the employer can identify and /or correct inaccuracies in data that's held on the system or so that the employer can run benefit estimates without needing to ask the administering authority to do this. Given that we have established the administering authority and the scheme employer are not joint data controllers but are each data controllers in respect of the data they each have a legal obligation to hold, does GDPR have any implications for the continued operation of such practices? I assume the precise answer in any given case will depend on the specific data that employers are given access to and the range of actions they can undertake, but any general comments you can provide would be very helpful.

New question – This may need a new question, but we have been asked to seek a view on the status of fund actuaries under GDPR and whether they would be a data controller, a joint data controller with the administering authority or a data processor. The context to this question is that we understand one of the four actuarial firms operating in the LGPS has issued a contract variation to its LGPS clients to define it as a joint data controller with the administering authority in the provision of its services. Our understanding, however, would actually be that fund actuaries are data processors in the sense that they are appointed by LGPS administering authorities to provide various services – however, fundamentally, actuaries process data on behalf of their clients and it is not their data. Would you agree? This question could perhaps be summarised as 'Is a fund actuary, appointed to provide services to an administering authority under the LGPS Regulations, a data controller in respect of the personal data they have access to in fulfilling this role, a joint data controller with the administering authority or a data processor?'

APPENDIX 2

Scope of our advice

(a) The advice in this report is provided only to the Local Government Association to be shared with the administering authorities of the Local Government Pension Schemes. It was prepared solely for the purpose of assisting the administering authorities to address the specific issues/questions raised at Appendix 1 relating to the impact of the General Data Protection Regulation (GDPR). It is not advice to an employer, other connected or stakeholder parties, auditors or other advisers, or other third parties ("Third Parties"). No part of this advice 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 advice.

(b) This advice only considers the legal issues in relation to the questions/issued raised at Appendix 1. We have reached our conclusions based on an understanding of the law as at the date of this report. Accordingly, it is possible that this report will need to be updated if the law changes. However, we will only do so if you specifically instruct us to. We have not considered or advised on the tax efficiency of the matter or its commercial implications.

(c) The documents on which this advice is based are those that are referred to in it. Please let us know immediately if you think there are other documents or information relevant to this issue. In accepting instructions from the Local Government Association we are not agreeing to undertake, or be responsible for, a review of all or any elements of any other documentation unless we specifically accept in writing instructions to carry out such a review and advise upon issues arising therefrom. Accordingly, we do not accept liability should our advice be based on erroneous assumptions or there are documents or information which are relevant but with which we have not been provided.

(d) Our legal advice solely relates to English law.