SQUIRE PATTON BOGGS

LOCAL GOVERNMENT ASSOCIATION

***McCLOUD* AND COLLECTION OF MEMBER PERSONAL DATA**

1 BACKGROUND AND SCOPE

1.1 We have been asked to answer the following specific question, in the context of anticipated amendments to the Local Government Pension Scheme Regulations 2013 (the **"LGPS Regulations"**) to address the age discrimination issues identified in the benefit structure of the LGPS Regulations following the Court of Appeal's judgment in the *McCloud* case[1]:

Under data protection and GDPR rules, can an administering authority collect and store information about part time working hours and service breaks for all members with membership after 31 March 2014?

1.2 The notes at the end of this advice contain important information about its scope.

2 INITIAL ANALYSIS OF QUESTION

2.1 There are two constituent parts to this question, namely:

(a) the collection of working hours and service breaks from 31 March 2014 onwards; and

(b) the storage and retention of such data.

2.2 For the purposes of this response, it seems highly likely that the working hours and service breaks of pension members will constitute 'personal data' under the General Data Regulation 2016/679 ("**GDPR**") and UK Data Protection Act 2018 ("**DPA**"), together the "**Data Protection Laws**".

2.3 When considering this question we are mindful that the Government is still consulting on the precise terms of the benefit changes to address the *McCloud* decision. Furthermore, if as expected the benefit changes include an underpin, Administering Authorities are likely to be able to identify now most (but perhaps not all) members who are potentially in scope for underpin protection and for whom additional data must be collected. Whilst technically Administering Authorities will not know until a particular member retires whether the underpin will "bite", the fact that a comparison between the two benefit structures is needed means data relating to part time working hours and service breaks for membership from 31 March 2014 is required in order to calculate the benefits of all members who are in scope for underpin protection.

2.4 We recognise that Administering Authorities will likely wish to collect any data that may potentially be needed now, because that data may not be available from employers when the member retires (for example, if the member left an employer's service some years previously). The fact that some members not presently in scope for underpin protection may be in scope by the time they retire (for example, if they subsequently aggregate separate periods of pensionable service) means that Administering

[1] *Lord Chancellor & Others v McCloud & Others* [2018] EWCA Civ 2844

Authorities will likely wish to collect additional data in respect of *all* members and not just those identified now as definitely in scope for underpin protection.

2.5 The key to lawfully collecting this personal data will be to analyse and prove that the collection of this personal data is necessary for your Fund's purpose – i.e. to pay a data subject's correct benefit entitlement if the member qualifies for underpin protection. The Fund should specifically consider whether it will struggle to calculate benefits correctly without this personal data, including for members who qualify for underpin protection in the future.

3 COLLECTION OF THE PERSONAL DATA

3.1 Under Data Protection Laws, Controllers must have a lawful basis for the collection of personal data. Here, the Administering Authority will act as a Controller of Fund personal data. Selecting an appropriate lawful basis is a fact specific exercise. We have set out below an example analysis for legal obligation, which we anticipate will apply in this circumstance. You only need to have one lawful basis for collecting personal data.

3.2 When considering the below analysis for your specific Fund, it is important to document a fact-specific assessment. You will have done this as part of your initial GDPR compliance exercise in 2018 but, where this is an extension to the type of data the Fund collects, the assessment should be repeated.

3.3 **Legal obligation (Article 6(1)(c) GDPR)**

(a) In order to address the issue of unlawful age discrimination raised in the *McCloud* case, an Administering Authority will need to reconcile or supplement its previous records for Fund members to ensure that members receive their correct benefit entitlement. Given that this need has arisen out of case law and subsequent amendments to the LGPS Regulations, we consider Funds will be able to consider legal obligation as the lawful basis for collecting additional member personal data.

(b) In order to rely on legal obligation, the Administering Authority will need to demonstrate that its overall purpose for the collection and processing of this additional personal data is to comply with a legal obligation. It is not necessary for there to be an explicit legal obligation to collect the specific personal data or carry out a specific processing activity, but the collection or processing of this personal data is nonetheless necessary to enable Administering Authorities to comply with their legal obligation to calculate benefits correctly.

(c) In this instance, it is likely that the Administering Authority will be collecting and processing the additional personal data to ensure that it provides the correct benefit entitlement in accordance with the updated legal principle established in the *McCloud* case (which is expected to be reflected in the LGPS Regulations).

(d) Therefore, it is likely that the Administering Authority's overall purpose for processing this personal data is to comply with a legal obligation.

(e) Legal obligation is also likely to apply for the category of members where it is currently unknown whether they will benefit from underpin protection at a later date, for example due to future aggregation of periods of pensionable service. This is on the basis that, if this additional personal data is not collected for those specific members now, there is an appreciable risk that the Administering Authority will need this personal data at a later date, but not be able to collect it. If the necessary data is not available when needed, Administering Authorities will be unable to calculate the correct benefit entitlement and comply with the McCloud ruling.

(f) Consequently, we consider Administering Authorities can justify collecting additional personal data for all members, on the grounds that that data will be necessary to comply with their legal obligation to calculate benefits correctly if in future those members are in scope for underpin protection.

3.4 Special Category Personal Data (Article 9 GDPR)

For the purposes of this question, we have assumed that no Special Categories of Personal Data are to be collected as part of the additional data requirements. However, if you are planning to collect such data, Article 9 GDPR and Schedule 1 DPA will need to reviewed, considered and applied.

4 STORAGE AND RETENTION OF ADDITIONAL PERSONAL DATA

4.1 Once the Administering Authority has collected the additional data, it will need to consider the appropriate retention period. The same considerations apply regardless of the basis on which personal data is collected and processed. Administering Authorities should have carried out this assessment as part of its general GDPR compliance. However, it is necessary to repeat the analysis when additional personal data is collected. Often, pension funds need personal data for a very long period of time, so it can be difficult to stipulate a precise retention period. It is important to consider how long the Administering Authority will genuinely need the personal data for and it should document that decision-making analysis.

4.2 The Information Commissioner's Office (the "**ICO**") specifically state that Controllers should not retain personal data for an indefinite period "just in case", or if there is only a small possibility of using the data in the future. Whilst it is not possible to say definitively now that the additional data will be necessary to calculate the correct benefits for every member not already known to be in scope for underpin protection, there is a clear and legitimate reason why the Administering Authority needs to collect this data now. Nevertheless, the Administering Authority should try to specifically identify a retention period or, at a minimum, the criteria for determining an appropriate retention period. At the same time, the Administering Authority should also document why it is collecting this data: i.e. in case the member qualifies for underpin protection in the future when there is increased difficulty in obtaining the personal data such that the Administering Authority may not be able to calculate a data subject's correct benefit entitlement. In order to aid this decision-making analysis, consider how long the Fund would usually retain payment and wage data and assess whether that continues to be an appropriate approach in these circumstances.

SQUIRE PATTON BOGGS

4.3 The Administering Authority will also need to consider how best to protect this additional personal data. It will need to ensure that it implements appropriate technical and organisational security measures to protect against loss, destruction, damage or unauthorised disclosure or processing. The Administering Authority should consider how it holds existing wage data and assess whether those security measures continue to be appropriate in these circumstances. The Administering Authority may well have reviewed its security measures as a part of its GDPR compliance, but we recommend that the Administering Authority undertake an annual review of its technical and organisational measures as a matter of good practice.

4.4 Many of the regulatory actions taken by the ICO have been related to organisations failing to adequately protect personal data. Recently, organisations have been criticised for not encrypting data, failing to act upon known vulnerabilities within their networks, continuing to use out of date operating systems and inappropriate account privileges. Organisations have also been criticised for retaining personal data for too long, the argument being that the less personal data that is retained, the less personal data that can be compromised in a personal data breach. Therefore, it is important to have robust security measures in place and to document any decision-making in relation to the retention of personal data.

4.5 Other compliance documents may need to be updated as a result of this new processing activity, including Records of Processing and Privacy Notices.

Squire Patton Boggs (UK) LLP
July 2020

SCOPE OF THIS ADVICE

1 This advice has been prepared for the Local Government Association. We understand that copies will be provided to the administering authorities of Local Government Pension Scheme funds in England and Wales. **This advice will need to be considered in the specific circumstances of each fund.** Accordingly we accept no liability to individual funds or their administering authorities unless we provide formal advice specific to that authority.

2 This advice 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 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 template.

3 This advice has been prepared based on an understanding of the law and guidance issued by the Information Commissioner and the European Data Protection Board as at the date of issue. It is possible that this advice 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 advice is intended to enable administering authorities, in their capacity as data controller of personal data relating to the Local Government Pension Scheme fund for which they are responsible, to consider their personal data collection and retention policies in light of the *McCloud* case. We have not considered or advised on any tax or commercial implications that individual funds may wish to consider in conjunction with this issue.