Local
Government
Association

Pensions Dashboards Programme (PDP)

Answers to be submitted online

12 March 2021

Dear Sir or Madam

Pensions Dashboards: Call for Input

Thank you for the Pensions Dashboards Programme (PDP) Call for Input seeking views on a range of questions in relation to what data providers believe would be an acceptable identity standard for them to provide pension information to a user.

I respond on behalf of the Local Government Association (LGA) and the Local Government Pensions Committee (LGPC).

The LGA is a politically led, cross-party membership organisation that works on behalf of councils to ensure local government has a strong, credible voice with national government. 335 councils in England including district, county, metropolitan, unitary, London boroughs and the City of London are members of the LGA. There are 22 Welsh unitary authorities in membership via the Welsh Local Government Association (WLGA). The LGPC is a committee of councillors constituted by the LGA, the WLGA and the Convention of Scottish Local Authorities (COSLA). The LGPC considers policy and technical matters affecting the Local Government Pension Scheme (LGPS) in England & Wales, a scheme which has approximately 5.9 million members.

This response sets out the LGA's view, where appropriate, on the questions posed in the Call for Input.

I hope the content is helpful; if you have any questions, please do not hesitate to contact me.

Yours faithfully

Jeff Houston

Head of Pensions

Questions raised in the Pensions Dashboards Call for Input

1. **Do you agree that finding pensions and viewing pension details via a pensions dashboard should include a central digital identity, asserted to an appropriate standard, in accordance with the GPG 45? If no, what alternative approach would you recommend?**

   Yes, we agree that finding pensions and viewing pension details via a pensions dashboard should include a central digital identity in accordance with the National Cyber Security Centre's Good Practice Guide 45.

2. **The proposal includes a level of confidence in identity and a level of authentication. Do you have a view on the level of assurance that needs to be achieved to provide comfort to release pension information? If Yes, what elements do you think are the primary factors? If No, what additional information would you need to be able to make an assessment?**

   Yes, we have a view on the level of assurance that needs to be achieved to provide comfort to release pension information. The pensions finder service will be accessing multiple pension administration systems containing confidential secure data. Initial user authentication must be of a sufficient level to maintain confidence in the digital architecture from both a user and a scheme administrator's perspective.

   The authenticators should be of a high quality and independently tested to prove they meet industry standards.

   User asserted information (ie data input by the user), that the pension finder service will use to locate a user's pension records, must as a bare minimum include national insurance number together with the information set out in points 15(a) to (d).

3. **The suggested levels of confidence (GPG 45) and authentication (GPG 44) are 'medium', which equates to the previous versions of the standard level of assurance two. Do you agree that this is the correct level? If No, what would you suggest is the correct assurance level for both proofing of identity and strength of authentication?**

   Whilst we understand that users may favour a simple authentication process, as scheme administrators we have a duty to ensure scheme data is only shared with an appropriately validated third party. The pension finder service will be accessing multiple pension administration systems containing confidential secure data. Initial user authentication must be of a sufficient level to maintain confidence in the digital architecture from both a user and a scheme administrator's perspective.

In line with the National Cyber Security Centre’s Good Practice Guides 45 and 44, in our view the authentication level should be set to ‘high’ for both proofing identity and the strength of authentication. This means that the authenticators can be relied upon because they:

- cannot belong to anyone other than the user that created the account
- cannot contain a secret that is easy to steal, guess or copy (whether this be static or dynamic)
- must be independently tested to prove they meet industry standards.

4. **Is there an alternative to the default levels of assurance from the Good Practice Guidelines and how would you anticipate them being measured?**

   No, in our view there is not an alternative nor any benefit, from diverging away from using the standardised National Cyber Security Centre’s Good Practice Guides.

5. **Does your firm have any view on proofing or authentication methods and operate a current internal standard that differs from the GPGs medium level? If Yes, could you please provide an overview that could help direct the programme’s approach?**

   There is a variety of authentication methods operated by host administering authorities in the LGPS, including multifactor authentication passcodes and biometric. Many will require authentication on entry by the user and will not include any timed passcodes or ‘remember me’ facilities.

   Some will also operate ‘yes lists only’ for external Internet Protocol (IP) addresses to access systems within the host firewall.

6. **The architecture includes the central identity service to ensure that a uniform, controlled process exists, and that a user can easily manage their own consents. Please provide your thoughts on this approach and any challenges that you may foresee.**

   It is our view that the central identity service has to exist to ensure that a uniform, controlled process exits and that a user can easily manage their own consents. The central identity service should adhere to common authentication standards such as Open Authorisation and Security Assertion Markup Language plus other common use protocols. Further information on how the central identity service will integrate with multiple dashboards would be appreciated.

7. **Are there any specific requirements that you would anticipate the Pensions Dashboards Programme having to meet when seeking:**

a) your firm’s approval for a standard approach to identity assurance

In our view, for LGPS administering authorities to approve a standard approach to identity assurance:

- the authentication level must be set to ‘high’, giving LGPS administering authorities assurance that the correct user is accessing the Pensions Dashboards
- compliance with local authority data protection controls ensuring that the data will indeed be viewed by the correct user, for the data to be released beyond the authority’s firewalls.

b) a cross industry agreement on a standard for identity assurance

In our view, for LGPS administering authorities to approve a standard approach to identity assurance:

- the authentication level must be set to ‘high’, giving LGPS administering authorities assurance that the correct user is accessing the Pensions Dashboards
- compliance with local authority data protection controls ensuring that the data will indeed be viewed by the correct user, for the data to be released beyond the authorities firewalls.

8. What security related controls (other than identity proofing and authentication) do you see as important in your acceptance of the PDP solution for Pensions Dashboards?

In answering this question we have assumed that the identity proofing and authentication is of a sufficient level to maintain confidence in the digital architecture from both a user and a scheme administrator’s perspective. We have major concerns around the Pension Finder Service’s:

- ability to locate and extract the correct data based on the user asserted information
- maintain end to end encryption of the data identify and report data breaches to all systems potentially affected
- ability for the host system to block access to the dashboard without notice
- compliance with GDPR.