Nottinghamshire County Council

Report to Nottinghamshire Pension Fund Committee

19 April 2018

Agenda Item: 9

REPORT OF THE SERVICE DIRECTOR – CUSTOMERS AND HUMAN RESOURCES

IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION

Purpose of the Report

1. The purpose of this report is to update and seek Pensions Committee approval for the actions proposed by the Pension Administration Team in preparation for the introduction of the new General Data Protection Regulation (GDPR) from 25 May 2018.

Information

Background

2. On 25 May 2018 the EU's General Data Protection Regulation (GDPR) comes into force containing new standards for the protection of individuals' personal data in the European Economic Area. The change will impact on the way pensions schemes can lawfully collect, use, retain and share information. GDPR applies to organisations that handle the personal data of EU residents and will replace the UK's Data Protection Act 1998 (DPA).

3. Although the GDPR is EU legislation, UK organisations will still need to apply it, and after Brexit the UK is likely to adopt its own legislation to align with GDPR.

4. In July 2017, the LGPC Secretariat circulated a document commissioned from a firm of independent legal advisers to provide a brief overview of the new requirements and the steps which local authority pension funds should be taking to prepare for GDPR coming into force. A copy of this document is attached as Appendix A to the report and has been used to inform the Nottinghamshire Pension Fund GDPR action plan.

5. The definition of personal data is wider under GDPR than under the UK's current Data Protection legislation. Personal data means any information about an individual where that person can be identified directly or indirectly from the data. This will therefore require a range of actions to be identified and undertaken by the Nottinghamshire Pension Fund to enable legal compliance. Discussions have taken place and advice sought from the Programme Manager for the Council's programme of work to ensure GDPR compliance. The action plan attached as Appendix C will be implemented alongside the Council's corporate GDPR action plan to identify and exploit synergies and interdependencies and share learning between the two programmes of work.

Implications of the implementation of GDPR for the administration of the fund

6. GDPR brings with it not just the need to comply with the new requirements, but also the need to demonstrate compliance, if requested by the Information Commissioner's Office. The intention of GDPR is to raise the level of personal data security and privacy protections across the board.

7. In summary, implementation of GDPR has the following implications for the Nottinghamshire Pension Fund:

    a. The scale of the financial penalties for non-compliance is much greater;
    b. Authorities must create and maintain records of all personal data processing activities, to be presented to the Information Commissioner's Office (ICO) on demand;
    c. Authorities must review and assess the adequacy of their data security measures in place, and use encryption where appropriate
    d. Authorities must review and update all relevant third party service and data sharing contracts to ensure GDPR compliance;
    e. Authorities must revise privacy notices and consider whether member consent is required. Advice to date is that it is likely that authorities will be able to reply on the "performance of a legal obligation" exemption;
    f. Authorities must establish, or update, breaches management processes so that relevant breaches can be reported within 72 hours of the authority becoming aware of the breach;
    g. Authorities must appoint a Data Protection Officer (DPO);
    h. Authorities must ensure processes are in place to cater for new individual rights, particularly the right to have personal data deleted; and
    i. Authorities should consider whether to carry out a Data Protection Impact Assessment (DPA).

8. Under GDPR there are a number of Data Protection roles:

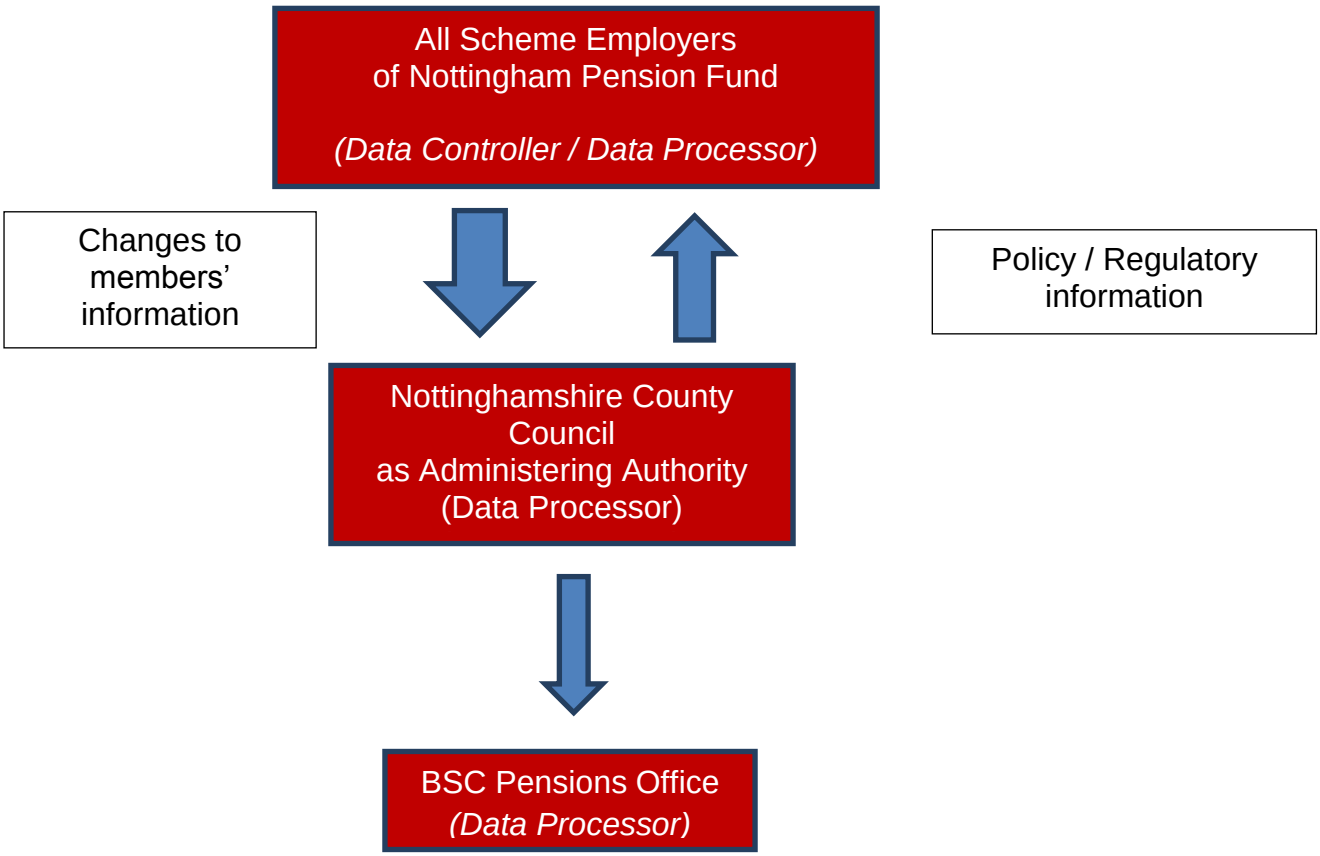
    a. Information Commissioner – person who has the power to enforce the Act
    b. Data Controller – person or organisation that collects and keeps data about people
    c. Data Processor – person or organisation that processes data on behalf of the data controller
    d. Data Subject – person who has data about them stored outside their direct control.

    With effect from 25 May 2018 GDPR applies to Data Processors and Data Controllers.

9. Nottinghamshire County Council will be establishing and appointing a dedicated Data Protection Officer. Consideration will be given to whether it would be appropriate for this role to also undertake the DPO role for the Nottinghamshire Pension Fund, with an appropriate recharge being made to the Fund. If not, alternative arrangements will need to be made. It is also proposed that the Nottinghamshire Pension Fund review the Nottinghamshire County Council processes for handling data breaches and subject access requests to determine whether these would be suitable for adoption by the fund. Further advice will be taken on both these aspects and reported back to a future meeting.

10. In April 2017 Nottinghamshire Pension Fund implemented an Administration Strategy. Work is in progress to review and update the strategy to incorporate GDPR requirements. This will include the Administering Authority and Scheme Employers roles and responsibilities as Data Controllers and Data Processors.

11. The diagram below shows the roles of Scheme Employers, the Administering Authority and the Pensions Office regarding the data protection roles.



National Developments

12. The full implications of GDPR for the LGPS are still being worked through by national organisations, such as the LGPC. In Bulletin 160, the Secretariat states:

"*We are aware that GDPR is an area that is getting increased attention across the LGPS and there are a number of crucial questions where there are different views, in particular:*

a) The implications of GDPR for LGPS funds, and
b) The work that needs to be undertaken to ensure administering authorities are fully compliant by the time GDPR comes into force.

In general, we recommend that LGPS administering authorities which form part of a local authority discuss and become involved in the local authority's broader project for the implementation of GDPR. However, at a national level plans are also in place to help funds with their GDPR responsibilities".

13. In addition to the document attached as Appendix A the LGA have commissioned a firm of independent advisors to produce further documents including:

a. Template privacy statements specifically for LGPS administering authorities that all administering authorities can tailor to meet with own requirements.

b. A Memorandum of Understanding document for employers. The aim of this document would be to set out that participating employers in the LGPS are able to share data with the LGPS administering authority without a data sharing agreement being in place.

14. The LGPS Communications Working Group has established a GDPR sub group. This group is also drafting a number of key documents to support Administering Authorities. This will include Privacy Impact Assessment (PIA) template and Fair Processing Notice, Incident Report Form and the Data Protection Policy. The fund will administration team will review these when available and consider if they are suitable for application for Nottinghamshire.

15. The LGPS has also produced a helpful document "General Data Protection Regulation Question and Answer for LPGS Members ". A copy of which is attached as Appendix B. This will be used to update the website re GDPR and to inform communication with scheme members and employers as set out in the action plan.

Privacy Impact Risk Assessment and Civica UPM GDPR Modules

16. A Data Protection Privacy Impact assessment will be completed for the Civica UPM system. The Pension system team are currently working on implementing the latest version of the system. This is scheduled to be completed by the end of April 2018. This version of the software provides some standard GDPR functionality covering deletion of member records and documents, retention rules and document bundling to support response to subject access requests. It is proposed to purchase additional GDPR modules from Civica which enable the anonymization of personal data within the test system to support GDPR implementation.

Third Party Contracts

17. Contracts with third party providers will need to be updated to ensure that they are GDPR compliant. This work is being led by Nottinghamshire County Council's Procurement Centre who are adopting the Crown Commercial Services Policy Procurement Notes 03/17 covering GDPR compliance. Identified suppliers for the Nottinghamshire Pension Fund include Civica, the software provider for the pension administration system; Barnett Waddingham, the Fund actuaries; Citibank – through which overseas based pensioners are paid and the in-house AVC providers – Prudential and Scottish Widows. All of whom have access to varying amounts of members' personal data.

18. The Nottinghamshire Pension Fund are also required to engage with a number of other bodies to meet statutory and legal obligations such as HMRC, National Fraud Initiative, Pension Regulator, Pension Ombudsman, Government Actuaries Department. Advice is being sought as to requirements to review existing data sharing agreements and update to reflect GDPR and whether or not these bodies are required to confirm their GDPR compliance.

Data Improvement Plan

19. All Pension Schemes are required by the Pension Regulator to have a data improvement plan. The Regulator expects schemes to undertake an annual data review and an additional review if anything significant happens to the Scheme.

20. The details of the Nottinghamshire Pension Fund Data Improvement Plan are the subject of a separate Pension Committee report. This plan will contribute to the Fund's GDPR compliance by ensuring data accuracy.

Other Options Considered

21. The Administering Authority is taking advice and has considered a range of activities to ensure GDPR compliance. These have been developed into an Action Plan for approval. This will be reviewed and developed as further information and advice emerges.

Reason/s for Recommendation/s

22. To raise awareness of the implications of GDPR amongst employers and scheme members and ensure that the Nottinghamshire Fund is compliant with the legislative requirements and best practice.

Statutory and Policy Implications

23. This report has been compiled after consideration of implications in respect of crime and disorder, data protection and information governance, finance, human resources, human rights, the NHS Constitution (public health services), the public sector equality duty, safeguarding of children and adults at risk, service users, smarter working, sustainability and the environment and where such implications are material they are described below. Appropriate consultation has been undertaken and advice sought on these issues as required.

Data Protection and Information Governance

24. The report and attached action plan set out how the Administering Authority intends to ensure GDPR compliance.

RECOMMENDATION

It is recommended that Members:

1) Approve the Nottinghamshire Pension Fund GDPR action plan and receive quarterly progress reports.

Marjorie Toward
Service Director – Customers and Human Resources
Resources Department

For any enquiries about this report please contact:
Sarah Stevenson, Group Manager Business Support Centre, on 0115 9775740 or sarah.stevenson@nottscc.gov.uk

Constitutional Comments (KK 05/04/2018)

25. The proposals in this report are within the remit of the Nottinghamshire Pension Fund Committee.

Financial Comments (KP 10/04/2018)

26. There are no direct financial implications arising from the contents of the report.

Human Resources Comments

27. Not applicable

Background Papers and Published Documents

None

Electoral Division(s) and Member(s) Affected

All