Division(s): N/A

PENSION FUND COMMITTEE – 1 DECEMBER 2017

GENERAL DATA PROTECTION REGULATIONS (GDPR)

Report by Director of Finance

Introduction

1. The current data protection regulations are being replaced by the European General Data Protection Regulations (GDPR) which will automatically take effect in the UK on 25 May 2018 without any action needed by the UK Government. These regulations will be supplemented by a piece of new UK legislation, the Data Protection Act 2018.

2. This legislation aims to reinforce individual rights in the digital / information age and give citizens back control over their personal data and to reduce administrative burdens.

3. There are specific roles set out in the legislation – a glossary of these and other relevant terms is attached at Appendix A

4. The headlines around this legislation say "that it heralds a complete change to the way anyone processing data needs to think". This coupled with the absence of any phasing in of the requirements and significantly higher sanctions which can be levied for a breach means that all actions to ensure full compliance must be completed by the end of April 2018.

Key Changes

Consent

5. Implied consent from scheme members is no longer sufficient to enable data to be processed. Now data processing will only be lawful if conducted with the explicit consent of the scheme member.

6. In seeking this consent the Data Processor must ensure that it tells data subjects the basis on which data is to be processed in a concise, transparent, intelligible and easily accessible form using clear and plain language. In seeking such consent it also must be clear if the data will be used in different processes, in which case separate consent must be obtained.

7. Consent can be withdrawn at any time.

Right to be Forgotten

8. Data subjects can exercise their “right to be forgotten” and insist that his/her data is permanently deleted from the Data Controller’s records

Right to Access

9. Data subjects can request details of any data held about them. This must be provided, at no cost, within 20 working days.

Data Portability

10. Allows a user to request a copy of personal data in a format usable by them and electronically transmissible to another processing system

Privacy by Design

11. GDPR requires that systems and processes must consider compliance with the principles of data protection. The essence of privacy by design is that privacy in service or product is taken into account from the inception of the product concept

Breach Notification

12. Data controllers will be required to report data breaches within 72 hours of becoming aware of the breach. Where the risk to the individual is high then data subjects must be notified.

Sanctions

13. These will increase from the maximum of £500,000 to between 2% and 4% of turnover (depending on transgression) or 10,000,000 or 20,000,000 Euro.

Implications for the Fund

14. Consent – processing of data by the Fund is necessary for compliance to meet legal obligations, however what actions will need to be taken remain unclear in absence of the Information Commissioner’s guidance.

15. Right to be Forgotten – if left as is then this could cause issues in cases where scheme members take a refund of contributions or transfer out of the scheme, and subsequently make a claim. It is rumoured that the Data Protection Act 2018 will address this issue in respect of pension fund, however this has yet to be confirmed.

16. However, Funds have been advised that legal advice is due to be issued confirming that there is a statutory need for the Fund to obtain and retain information.

17. Pension Funds generally hold a large amount of both current and historical data. This legislation will require a review of what should be retained and retention periods for this information.

Timetable and Actions for Implementation

18. Officers have been in contact with colleagues in ICT to establish what is being done corporately and how that impacts on the proposed implementation for the Fund. The corporate team is running some session which will be attended by the Service Manager for Pensions and are available for advice and guidance but it is down to each team to ensure that they are compliant with the regulations.

19. One point discussed was whether the Fund needed to put a Data Protection Officer in place but advice from the corporate team suggests that the Fund will fall under the remit of the OCC Data Protection Officer which would also mean that the Fund would report any breaches under the OCC arrangements.

20. Below is a timetable for the actions to be taken to ensure that the Fund is compliant by end of April 2018.

Action		**Date Due**
Information Audit	What data is held; where did it come from; how is it being processed; is it secure; map processes etc. Review Data Retention	January 2018
Privacy Impact Assessment	Assess any processes deemed as high risk – carry out assessment	January 2018
Privacy Notices and Consent	Update all communications so members understand all uses of information; Update Fund Policies; Obtain consent where necessary	February 2018
Service Provider Contracts	Review / Ensure GDPR Compliance	April 2018
New Individual Rights	Establish and implement new procedures so that these rights can be exercised	April 2018
Breach Management	Work under OCC procedure for reporting any breaches	Waiting on OCC
Awareness & Training	Pension Team to be briefed monthly; Engage with Scheme Employers; Update Committee & Board	Regular Briefings

21. The most significant part of this plan for implementation is the information audit. Given the amount of data and the multiple data sources, to do this work properly will be time consuming. On that basis, officers are intending to outsource this part of the process to an external consultant. This is currently being investigated and so no other details are yet available.

RECOMMENDATION

22. The Committee is RECOMMENDED to note the report

Lorna Baxter
Director of Finance

Contact Officer: Sally Fox, Pensions Manager; Tel: (01865) 323854

November 2017