Pensions Committee

2.00pm, Wednesday, 27 June 2018

Regulatory Update – General Data Protection Regulation (GDPR) & LGPS Regulations

Item number	5.9
Report number	
Executive/routine	
Wards	All
Council Commitments	Delivering a Council that works for all

Executive Summary

The General Data Protection Regulation (2016/679) (**GDPR**) came into force on 25 May 2018 and impacts how the Lothian Pension Fund (**LPF**) (acting through its administering authority the City of Edinburgh Council (**CEC**) manages its data protection and information systems, controls, policies, and procedures.

This paper is intended to provide Committee with an update on LPF's GDPR and wider Information Governance project and highlight what LPF has been doing to ensure best practice in this area, compliant with GDPR and other applicable data protection law and regulation in force from time to time (**Data Protection Law**).

The report provides a high-level update on the Local Government Pension Scheme (**LGPS**) regulations which came into effect on 1 June 2018 and a verbal update will be provided to Committee.

Report

Regulatory Update – General Data Protection Regulation (GDPR) & LGPS Regulations

1. Recommendations

Committee is requested to:

1.1 Note the update on the Fund's preparedness for GDPR; and

1.2 Note the update on the new LGPS regulations which came into force on 1 June 2018.

2. Background

General Data Protection Regulation (GDPR)

2.1 LPF uses personal data to administer the relevant pension funds, and must therefore comply with Data Protection Law.

2.2 Prior to the implementation of GDPR on 25 May 2018, LPF had to review its business processes to ensure that these were fully compliant with the new law. This included a review of LPF's data storage, information governance, ICT, office procedures and third-party relationships and required LPF to clearly communicate with its members and employer stakeholders.

2.3 For most purposes, LPF is a 'data controller', responsible for managing and retaining personal data that it holds. Suitable arrangements must be in place with any third parties LPF shares such data with ('data processors') to effectively administer pension benefits in the interests of its members and employers. LPF's relationship with its employer bodies is that of a joint controller, which necessitates a different approach to managing data (see 10.2 below).

2.4 LPF broadened the scope of its compliance project to ensure best practice information governance in all areas, which includes other non-personal data handled by it and its subsidiary companies LPFI Limited (**LPFI**) and LPFE Limited (**LPFE**).

3. Main report

3.1 As mentioned in quarterly risk management summaries, LPF has been working towards best practice compliance in information governance for the last 12-15 months. LPF continues to monitor industry standards against best practice recommendations to ensure it delivers an efficient and reliable level of compliance,

but Committee should note the following key actions and outcomes from the project to date:

3.1.1 **Legal basis for processing data:** The Local Government Association instructed Squire Patton Boggs (a reputable firm with a strong presence in the pension sector) to issue a legal opinion for UK LGPS administering authorities. The legal opinion confirms that LPF's statutory obligation to provide pension benefits to members constitutes a legal basis to process all personal data without the express consent of any member (i.e. data subject). The LGPS regulations require LPF to receive, hold and use that data to effectively administer the relevant pension funds. LPF has concluded that it does not require express consent to process personal data (including sensitive personal data) for carrying out pensions administration.

3.1.2 **Data audit and processing register:** Following a review of the data it holds for pensions administration, LPF developed a GDPR-compliant 'Register of Processing' based on CEC's template.

3.1.3 **Privacy policy:** LPF's updated privacy policy (see 10.1) has been published on its website and communicated to employers and pensions. Reference to the policy will be included in the summer newsletters for deferred and active members.

3.1.4 **Document retention policy:** LPF has developed a bespoke document retention policy for the LPF group. It is based on the CEC policy, and incorporates the requirements of the Pensions Regulator, HMRC and FCA.

3.1.5 **Intra-group governance and data sharing arrangements:** CEC is both the administering authority of LPF and a scheme employer. There needs to be sufficient governance separation between the functions of LPF and CEC. An intra-group information compliance agreement between LPF, CEC, LPFI and LPFE will:

i. clearly govern and narrate the flow and treatment of data amongst group entities;
ii. ensure the correct balance of responsibility and oversight as between LPF and CEC; and
iii. provide greater detail around the services LPF receives from CEC's information compliance team, by way of a service level arrangement.

LPF is aiming to have this intra-group agreement in place as soon as possible.

3.1.6 **Third party arrangements, systems audit and engagement:** LPF engaged with its third-party suppliers and partners to ensure that the contractual arrangements are up to date, GDPR-compliant, and to ensure that those third parties have adequately secure systems for information exchange. Given the number of LPF's third party relationships, this is an ongoing process which now forms part of LPF's compliance and risk reporting procedures.

3.1.7 **Portable storage hardware:** LPF has transferred data to the secure G drive from historic LPF portable hard drives, to mitigate the risk of unauthorised

access or loss of old data. The redundant portable devices and other desktop equipment, historically used for homeworking, are being securely destroyed.

Testing of mobile data-sticks and other portable storage devices to ensure these only be used on a read-only basis and that no LPF member of staff has permissions to write to such storage devices has been completed. This will be routinely checked for LPF staff.

3.1.8 **Confidential waste arrangements and procedures:** LPF is working with CEC to review the adequacy of the confidential waste services, checking for gaps in the process from collection to destruction. LPF will ensure that it has adequate contractual protection with any existing or new supplier of confidential waste services.

3.1.9 **Paper files, storage and security:** LPF has a practice of holding 'clear out' days and due to office moves over recent years, much of its historic paper filing is already gone. Committee should also be aware that there are minimal paper files specifically for the administration of members benefits as documents are scanned and stored electronically on the pensions administration system.

3.1.10 **Electronic files, storage and security:** As a priority, LPF needs to put in place a document management system to help it mitigate risk around unauthorised access to sensitive documents, duplication of information (with cost and Data Protection Law implications) and to support the move towards a fully paperless office. Meantime, LPF continues to review, organise, and rationalise the data it holds on its section of the CEC network.

3.1.11 **Transfer of files and security:** LPF currently uses the encryption software provided by Civica under the PensionsWEB package to share data with employers. The contract with Civica will expire in October 2018 and LPF is reviewing other potential encryption solutions. LPF also has access to encryption software (Winzip 22) which it uses for the secure transfer of personal and other sensitive data to other parties.

3.1.12 **Pruning of files:** LPF may only hold personal data which it requires for administering the pension funds. LPF's 'pruning' programme aims to delete/destroy any information that LPF has received but which it is not strictly required to retain (e.g. where a member has sent LPF additional medical details to prove their long-term ill health, when a letter from a qualified medical practitioner is sufficient). Staff are aware that extraneous data should not be retained and LPF will put in place more detailed controls to ensure that this policy is implemented.

3.1.13 **Recent and ongoing staff training:** Staff training sessions were held prior to the implementation of GDPR and new policies have been communicated to staff. A reminder of the data protection obligations will be included in the quarterly compliance email to the team. Annual completion of the data protection e-learning modules will be compulsory for all staff.

3.1.14 **Registration with the Information Commissioner Office:** Since 2015, LPF has been separately registered with the Information Commissioner Office (**ICO**). The decision has been made for LPF to fall under the umbrella of the CEC registration, a responsibility of the CEC Information Governance Unit. LPF is currently reviewing the implications of this and how to support CEC oversight without compromising the integrity of LPF's separate governance structures and operations. Assurances concerning the ringfencing of liability between LPF and CEC are needed to ensure that any fines levied by the ICO (see 5.2) would be the sole responsibility of either LPF/CEC, as appropriate.

LGPS Regulations

3.2 As reported to Committee in December, the Scottish Government consulted on changes to the current LGPS 2014 regulations, to consolidate all amendments made since April 2015. The main changes to the scheme rules include:

- members of LGPS 2015 scheme will be able to elect to take early payment of their pension from age 55, with an actuarial reduction, and will no longer need their employer's consent;
- additional flexibility for administering authorities to manage liabilities when employers leave the scheme and to provide for an 'exit credit' to exiting employers if appropriate; and
- changes to Additional Voluntary Contributions following the introduction of the UK Government's 'Freedom and Choice in Pensions', to allow payment from age 55 as a lump sum.

The regulations are also being brought into line with recent legislation including the Finance Act, redefining the pensionable pay used for ill health and returning officers, and removing the requirement for a member to take all their benefits if made redundant.

The final regulations have just been released and a verbal update will be provided to Committee.

4. Measures of success

4.1 Improving LPF's information governance processes more generally and ensuring compliance with the Data Protection Law, including GDPR.

4.2 Mitigating risk around any breach of Data Protection Law by LPF and so providing enhanced reassurance to its member and employer stakeholders.

5. Financial impact

5.1 There are no direct financial implications as a result of this report.

5.2 GDPR introduced enhanced powers for the ICO to levy fines. Under the Data Protection Act 1998 the maximum fine that can be levied is £500,000. Under GDPR, the maximum fine is to be the higher of EUR20,000,000 or 4% of annual turnover.

6. Risk, policy, compliance and governance impact

6.1 New document retention and privacy policies have been introduced as a result of GDPR.

6.2 Risk and compliance framework updated to include providers.

6.3 Office procedures are continuing to be enhanced around information governance.

7. Equalities impact

7.1 There are no equalities implications as a result of this report.

8. Sustainability impact

8.1 None, although there is significant resource being deployed to this at present. In future it will be important to ensure the new policies, procedures and controls are proportionate to the risk presented by any breach of Data Protection Law and in the context of LPF's other business priorities and risks.

9. Consultation and engagement

9.1 The Pension Board, comprising employer and member representatives, is integral to the governance of LPF and they are invited to comment on the relevant matters at Committee meetings.

10. Background reading/external references

10.1 LPF's updated Privacy Policy – link.

10.2 LPF's Memorandum of Understanding with Employers - link.

Stephen S. Moir

Executive Director of Resources

Contact: Struan Fairbairn, Chief Risk Officer, Lothian Pension Fund

E-mail: struan.fairbairn@edinburgh.gov.uk | Tel: 0131 529 4689

11. Appendices

None.