WIRRAL COUNCIL

PENSION COMMITTEE

18 SEPTEMBER 2017

SUBJECT:	**GENERAL DATA PROTECTION REGULATIONS (GDPR)**
WARD/S AFFECTED:	**ALL**
REPORT OF:	**MANAGING DIRECTOR, DELIVERY**
RESPONSIBLE PORTFOLIO HOLDER:	
KEY DECISION?	**NO**

1.0 EXECUTIVE SUMMARY

1.1 This report updates Members on the duties and obligations arising out of the General Data Protection Regulations which come into force on 25 May 2018.

1.2 The GDPR is a European Union (EU) directive that will govern how personal data should be held and processed by all 28 EU member states.

1.3 The UK Data Protection Act 1998 will no longer apply after 25 May 2018. The potential fines for infringement under the new legislation are substantial, up to 4% of annual global turnover or 20,000,000 Euros.

2.0 BACKGROUND AND KEY ISSUES

2.1 The EU's General Data Protection Regulation (GDPR) is a legal framework with the aim of boosting online privacy rights and strengthening the digital economy in the European Union. The GDPR brings harmonisation by applying the same set of Data Protection rules across the EU.

The changes are in response to how both globalisation and technological change have impacted how data is collected, stored, shared and transferred since the introduction of the Data Protection Act in 1998.

2.2 The GDPR will come into force in all EU Member States on 25 May 2018. The UK will still be a member state of the EU on the 25 May 2018 and the government announced on 21 June 2017 that it would implement the GDPR and retain the new legislation following Brexit.

2.3 The GDPR does not mark a radical departure from the current data protection regime (the UK Data Protection Act 1998). There is already a legal obligation on LGPS Administering Authorities to keep member data secure, but new legislation will have a significant impact on the obligations of Administering Authorities and the potential financial penalties for non-compliance.

Key changes for the Pension Fund under the GDPR

2.4 In summary, the key areas covered by GDPR are as follows:

	Key Changes	Description
a	Stricter requirements around consent	The Fund must be able to demonstrate openly and transparently to members that it has 'lawful consent' to hold and process their personal data in its duties to administer the Local Government Pension Scheme.
b	Privacy notices on the use of personal data	Privacy notices to be provided to members detailing : • how their data will be used; • third-party recipients of their data; • the various rights members have in respect of their data; and • the period for which the data will be stored.
c	Right to be forgotten	Where the data is no longer necessary for the purpose of administering the Scheme, members can request the complete erasure of personal data. The Fund will need to demonstrate clearly to a member when it cannot comply with that request as part of the overarching statutory duties to the LGPS and HMRC.
d	Relevant & necessary	Information must be relevant and not kept for longer than is necessary. Pension schemes typically keep information for decades, the Fund (and the LGPS community as a whole) will need to agree on what information

		should be retained and for how long.
e	Data Processing contracts with third parties	Currently data sharing agreements are required and in place with third parties; or 'Data Processors'. However, GDPR will impose direct liability on data processors requiring a review of current agreements and related supplier contracts.
f	Reporting data breaches	Personal data breaches must be notified to the Information Commissioners Office within 72 hours of having become aware of a breach. The member must also be notified if the breach is likely to result in a high risk to the member.
g	Increased record keeping obligations	The Fund must ensure records are maintained to show how they comply with the GDPR.
h	Subject Access Requests	An individual can request a copy of all personal data held by the Fund, currently this is required to be processed in 40 calendar days. The GDPR will shorten this timescale to one calendar month from receipt of the request.

Increase in Monetary Penalties for Non-Compliance

2.5 The Data Protection Act 1998 is enforced by the Information Commissioner's Office (ICO). The ICO can currently fine an organisation in serious breach of the act up to £500,000

2.6 The GDPR will introduce a new upper limit of 20,000,000 Euros or 4% of annual global turnover (whichever is the higher for the private sector).

Cyber Security & IT Contingency

2.7 As the Fund utilises computer systems to hold and process member records, the effective security and governance of these systems is fundamental to ensuring compliance with GDPR. This is particularly important as the Fund makes its strategic move to conduct more of its business with scheme members via internet based online systems. The online availability of personal information places the Fund at an increased risk of cyber-crime and being

subject to sophisticated cyber-attack, with the potential for high volumes of personal data being stolen.

2.8 Wirral Council as the Administering Authority provides the computer network infrastructure for the Fund. Fund Officers work closely with colleagues within 'Wirral Digital' on ensuring the security and availability of the computer systems and member data.

2.9 The Fund has in place system security, anti-virus software, data encryption and secure-email facilities as part of the services provided by Wirral Digital. Systems are regularly updated for security patches and backups of data are stored offsite.

2.10 Whilst there is considerable media focus on sophisticated cyber-attacks, the majority of data breaches are as a consequence of organisations failing to put robust security controls in place. The GDPR consequently reinforces the need for both 'technical' (computer software and physical security) and 'organisational' (work practices and employee training) measures to keep personal data safe.

2.11 All Fund staff annually undertake an e-learning course entitled "Responsibility for Information" as staff awareness of data protection is a significant part of ensuring ongoing compliance.

Partnership working to meet GDPR duties and obligations

2.12 Fund officers are working with colleagues in Legal & Democratic Services and Wirral Digital as part of the larger Administering Authority plan to meet the new duties and obligations of the GDPR.

2.13 However, Fund Officers are also actively engaged with colleagues at other Funds and the Local Government Association (on behalf of all Funds) in gaining a clear, coherent and consistent response to the demands of GDPR compliance. In particular, a key work area being worked on collaboratively is appropriate communications to scheme members for use in advance of May 2018.

2.14 In gaining the clear, coherent and consistent approach across the LGPS community, the LGA are commissioning legal opinion on a number of areas from Squire Patton Boggs (SPB). A number of these areas are in response to questions raised by officers as part of the partnership work with the LGA.

3.0 RELEVANT RISKS

3.1 Non-compliance with the organisational and security requirements of the GDPR from 25 May 2018 introduces the potential of significant reputational risk and monetary risk to the potential maximum of 20,000,000 Euros or 4% of annual global turnover.

3.2 The strategic move to conduct more of its business online places the Fund at an increased risk of cyber-crime and being subject to sophisticated cyber-attack, with the potential for high volumes of personal data being stolen. This risk is mitigated by the continued high priority commitment to computer security, robust organisational work practice and staff awareness training.

4.0 OTHER OPTIONS CONSIDERED

4.1 Not relevant for this report.

5.0 CONSULTATION

5.1 Not relevant for this report.

6.0 OUTSTANDING PREVIOUSLY APPROVED ACTIONS

6.1 None associated with the subject matter.

7.0 IMPLICATIONS FOR VOLUNTARY, COMMUNITY AND FAITH GROUPS

7.1 None associated with the subject matter.

8.0 RESOURCE IMPLICATIONS: FINANCIAL; IT; STAFFING; AND ASSETS

8.1 Collaborative working with the LGA and other Funds continues the benefits that the Fund has experienced previously when sharing resources.

8.2 A number of questions have been raised by Fund officers to the LGA as part of the initial impact assessment of the GDPR. The LGA is meeting the expense of gaining legal opinion from Squire Patton Boggs.

9.0 LEGAL IMPLICATIONS

9.1 There are none arising from this report.

10 EQUALITIES IMPLICATIONS

10.1 Has the potential impact of your proposal(s) been reviewed with regard to equality?

No, because the General Data Protection Regulations have been assessed for equality by the European Commission whilst being formulated as a directive for EU states.

11.0 CARBON REDUCTION AND ENVIRONMENTAL IMPLICATIONS

11.1 There are none arising from this report.

12.0 PLANNING AND COMMUNITY SAFETY IMPLICATIONS

12.1 There are none arising from this report.

13.0 RECOMMENDATION

13.1 That members note the report.

14.0 REASON/S FOR RECOMMENDATION/S

14.1 There is a requirement for Members of the Pension Committee to be kept up to date with legislative developments as part of their stewardship function.

REPORT Guy Hayton

AUTHOR Operations Manager
Telephone (0151) 242 1361
Email guyhayton@wirral.gov.uk

BRIEFING NOTES HISTORY

Briefing Note	Date