CYNGOR SIR *POWYS* COUNTY COUNCIL

Pensions and Investment Committee
29th September 2017

REPORT BY:	**Strategic Director of Resources**
SUBJECT:	**General Data Protection Regulations**
REPORT FOR:	**Decision**

1 Introduction

1.1 The General Data Protection Regulations 2017 come into force on 25th May 2018. These regulations apply to all EU member states and the UK Government have confirmed that in spite of the UK's intention to leave the EU in 2019, these regulations will be enforceable in the UK from next May. This paper is the first step in planning to ensure that the Powys Pension Fund is compliant with the requirements of these regulations.

2 Background

2.1 Pension schemes necessarily hold and process a large amount of personal data in relation to scheme members. As a matter of good governance it is important that scheme members' data is safeguarded. There is already a legal obligation on the County Council as an LGPS administering authority to keep member data secure, but these regulations will have a significant impact on the obligations of the County Council and the potential financial penalties that can result from failure. The maximum potential fine for breaching these regulations is €20 million.

3 General Requirements

3.1 The Pension Fund is required to demonstrate its compliance with these regulations. It should be able to show in a meaningful way that both the overall governance structure for data protection compliance and the individual policies and procedures relating to data processing are compliant.

4 Specific Requirements and Actions To Ensure Compliance

4.1 <u>Maintain Records of Data Processing</u>

It will be a mandatory requirement for organisations employing more than 250 people, or who process sensitive personal data, to maintain records of all personal data processing activities. The records may

have to be presented to the Information Commissioner's Office (ICO) on demand.

Action:

- Ensure that all personal data processes are recorded

4.2 Review Data Security Measures and Assess Adequacy

These regulations retain the current obligation to have appropriate technical and organisational data security measures in place, but in addition requires that certain specific measures (such as encryption) should be used "where appropriate". There is also a requirement that processes incorporate "privacy by design and default", ie compliance needs to be integrated into all data processing and should be the default position on all privacy matters.

Action:

- Develop a compliance plan to ensure appropriate technical and organisational data security measures are in place both within the Pension Fund and with third party providers (eg. Pensions admin system software supplier)
- Review existing applications and processes that involve the use of personal data and ensure that they are secure
- Implement a policy to ensure that personal data is only stored for the minimum period necessary
- Consider whether data encryption should be used, especially for sensitive personal data such as that relating to health matters

4.3 Update Service Provider Contracts

The regulations require new content to be inserted into service and data sharing agreements that govern the use of personal data. The regulations also impose direct liability on such service providers for data protection compliance.

Action:

- Work with service providers including any third parties who send/receive data in relation to the Pension Fund (eg LGPS Scheme Employers, Fund Actuary etc) to amend service contracts as required to ensure compliance.

4.4 Review and Update Privacy Notices and Consider Whether Member Consent is Required

The regulations require additional content to be included in all privacy notices regarding how personal data will be used by data controllers. Data controllers must tell anyone whose personal data they collect what information is held, how it is used, who it may be shared with and

what safeguards are in place. The regulations also make it more difficult to obtain valid consent for the use of personal data – consents must be fully informed, specific, unambiguous and freely given by way of a statement or clear affirmative action by the member. In addition, data controllers are required to retain proof of consent.

Action:

- Review and resend all member privacy notices in order to comply with these regulations
- Review the consents that the Council relies on to justify the processing of personal data
- Consider new or revised consent to data processing by the Pension Fund. New joiner information may need to be updated.

4.5 Establish a Breach Management Process

The regulations requires data breaches involving any risks to individuals to be reported to the ICO without delay. And in any case within 72 hours of the data controller becoming aware of the breach. Affected individuals must also be notified directly if the breach is a high risk to their rights or freedoms.

Action:

- Establish an effective data breach response plan that ensures that any breach is addressed and assessed and that any ICO report or member notification can be dealt with in a timely fashion.

4.6 Appoint a Data Protection Officer (DPO)

The European data protection authorities recommend that a DPO is appointed. The DPO is expected to be appropriately qualified; to report directly to senior management; and, will be the contact person for questions related to the processing of personal data.

Action:

- Confirm that this role for the Pension Fund can be met by the County Council's appointed general DPO.

4.7 Ensure that Processes are in Place to Cater for the New Individual Rights

These regulations introduce new rights for individuals, including the new right of data portability, the right to restrict processing, the right to object to processing, the right to object to direct marketing and the right to have personal data deleted.

Action:

- Identify which of the new individual rights may be exercised by members of the LGPS
- Establish procedures to ensure that these rights may be exercised.

4.8 Carry Out Data Protection Impact Assessments (DPIA)

DPIAs must be carried out in relation to "high risk" processing. This is where there is a high risk to rights and freedoms, for example, extensive profiling of individuals using automated processing or large scale processing of sensitive personal data (eg. national information).

Action:

- Assess whether any use of personal data by the Pension Fund would be classified as "high risk", and if so, complete a DPIA.

5 Proposed Next Steps

5.1 On approval of this report, the actions listed above will be carried out by Pension Fund Officers in conjunction with the County Council's general data protection arrangements. A further report will be submitted to this Committee in Spring 2018 setting out the procedures adopted and actions taken in order to ensure compliance with these regulations.

6 Recommendation

6.1 Committee is asked to note the contents of this report and to approve the actions contained herein.

Recommendation:			**Reason for Recommendation:**
• To note the contents of the report. • To approve the actions proposed			Statutory obligation
Person(s) To Action Decision:			
Date By When Decision To Be Actioned:			
Relevant Policy (ies):	N/A		
Within Policy:	N/A	**Within Budget:**	N/A
Contact Officer Name:	Tel:	Fax:	Email:
Joe Rollin	01597 827641	01597 826290	joe.rollin@powys.gov.uk

Relevant Portfolio Member(s):	Councillor Aled Davies
Relevant Local Member(s):	**N/A**