Agenda Item No: 13

CAMBRIDGESHIRE PENSION FUND

Pension Fund Board

Date: 27 October 2017

Report by: Head of Pensions

Subject:	**General Data Protection Regulation**
Purpose of the Report	To provide the Local Pension Board with an overview of the General Data Protection Regulation and a plan of action to ensure compliance with the regulation
Recommendations	**That the Local Pension Board notes the contents of this report**
Enquiries to:	Jo Walton – Governance and Regulations Manager, LGSS Pensions Email: jwalton@northamptonshire.gov.uk

1. Introduction

1.1. The General Data Protection Regulation is regulation by which European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.

1.2 The primary objectives of the General Data Protection Regulation (GDPR) are to give control back to citizens over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

1.3 The regulation was adopted on 27 April 2016 and becomes enforceable from 25 May 2018 after a two year transition period.

1.4 The UK government has confirmed that the decision to leave the EU will not affect the commencement of the GDPR.

1.5 GDPR applies to both data controllers and data processors. Under the GDPR, data controllers and data processors have broadly the same definitions under the Data Protection Act 1998 as set out below.

Type	Definition	GDPR obligations
Data controller	Specifies how and why personal data is processed.	Must ensure that contracts with processors comply with GDPR.
Data processor	Acts on the processor's behalf.	Required to maintain records of personal data and processing activities.

1.6 In terms of the Cambridgeshire Pension Fund and as per the constitution the administering authority is the Data Controller.

2. Personal Data

2.1 The GDPR's definition of 'personal data' is more detailed than under the Data Protection Act 1998 (DPA). For example, it makes clear that information such as an IP address can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about individuals.

2.2 The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA definition and could include chronologically ordered sets of manual records containing personal data.

2.3 The GDPR refers to sensitive personal data as 'special categories of personal data'. GDPR defines this as personal data that when processed reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and of data concerning health or sex life. As such, processing of sensitive personal data is prohibited subject to certain exceptions.

3. GDPR Data Protection Principles

3.1 Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the DPA but with a new accountability requirement which requires organisations to show how they comply with the principles (for example, documenting the decisions taken about a processing activity).

3.2 Article 5 of the GDPR requires that personal information must:

- Be fairly and lawfully processed;
- Be processed for limited purposes;
- Be adequate, relevant and not excessive;
- Be accurate and up to date;
- Not be kept for longer than necessary;
- Be processed in line with data subjects' rights
- Be secure; and
- Must not be transferred to others without adequate protection.

3.3 Article 5(2) requires that the data controller shall be responsible for, and be able to demonstrate, compliance with these principles.

4. Lawful processing

4.1 For processing to be lawful under the GDPR, organisations will need to identify and document the lawful basis before processing the personal data. Under the DPA, this is referred to as the "conditions for processing".

4.2 The following are lawful bases for processing personal data and special categories of data:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

5. Consent

5.1 Consent under the GDPR must be a freely given, specific, informed and ambiguous indication of the individual's wishes. There must be some form of clear affirmative action (a positive opt in). Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must be separate from other terms and conditions and organisations will need to provide simple ways for members to provide consent.

5.2 Consent has to be verifiable, and individuals generally have more rights where consent is relied on to process member data.

6. Children's personal data

6.1 The GDPR contains new provisions intended to enhance the protection of children's personal data. As such, privacy notices must be written is a clear, plain way that a child will understand.

7. Individuals' rights

7.1 The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The GDPR provides the following rights for individuals:

- The right to be informed (see 7.2)
- The right of access (see 7.3)
- The right of rectification (see 7.4)
- The right to erasure (see 7.5)
- The right to restrict processing (see 7.6)
- The right to data portability (see 7.7)
- The right to object (see 7.8)
- Rights in relation to automated decision making and profiling (see 7.9).

7.2 The right to be informed

7.2.1 The right to be informed encompasses an organisation's obligation to provide 'fair processing information' through a privacy notice.

7.2.2 The GDPR provide for the following information to be contained within the privacy notice;

- Identity and contact details of the Data Controller and contact details of the Data Protection Officer;
- The purpose of the processing and lawful basis for processing;
- The legitimate interests of the controller or third party;
- Categories of personal data;
- The recipient or categories of recipient of the personal data;
- Details of transfers to overseas and safeguards;
- Retention period or criteria used to determine the retention period;
- The existence of data subject's rights;
- The right to withdraw consent at any time where relevant;
- The right to lodge a complaint with a supervisory authority;
- The source the personal data originates from and whether it can be found in the public domain;
- Whether the provision of personal data is part of the a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data; and
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

7.3 The right of access

7.3.1 Under GDPR, individuals will have the right to obtain confirmation that their data is being processed, have access to their personal data and other supplementary information that should also form part of the privacy notice.

7.3.2 Individuals are entitled to access their personal data free of charge and without delay and within no later than one month from the date of request.

7.3.3 If the request is manifestly unfounded or excessive particularly if it is repetitive the GDPR allows for a reasonable fee to be charged based on the administrative costs of providing the information. Alternatively, the request can be denied provided an explanation is given to the individual as to the reason why. They must also be provided with information on their right to complain to the supervisory authority and to a judicial remedy within one month.

7.4 The right to rectification

7.4.1 Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete.

7.4.2 A response to a request for rectification must be issued within one month which can be extended to two months if the request is complex.

7.4.3 Where it is deemed that the request for rectification should be denied an explanation must be given to the individual along with the right to complain to the supervisory authority and to a judicial remedy within one month.

7.5 The right to erasure

7.5.1 The right to erasure is also known as the right to be forgotten and enables the individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

7.5.2 The right to erasure does not provide an absolute right to be forgotten. Individuals have a right to have personal data erased and to prevent processing in the following specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed; and
- The personal data has to be erased in order to comply with a legal obligation.

7.5.3 A request for erasure can be denied where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest, task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific and historical research or statistical purposes; and
- The exercise or defence of legal claims.

7.6 The right to restrict processing

7.6.1 Under the DPA, individuals have the right to block or suppress processing of personal data and this is similar under the GDPR.

7.6.2 If an individual exercises this right, the data can still be stored, but no further processing is permitted. The GDPR allows for enough information to be retained about the individual to ensure that restriction is respected in future processing.

7.6.3 Restriction of processing personal data is permitted in the following circumstances:

- Where an individual contests that accuracy of the data, processing should be restricted until the accuracy of the data has been verified;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and if it is considered that the organisation's legitimate grounds override those of the individual;
- When processing is unlawful and the individual opposes erasure and requests restriction instead; and
- If the personal data is no longer needed but the individual requires the data to establish, exercise or defend a legal claim.

7.7 The right to data portability

7.7.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7.7.2 The right to data portability only applies to personal data an individual has provided to a controller, where the processing is based on the individual's consent or for performance of a contract and when processing is carried out by automated means.

7.7.3 To comply with such a request the personal data must be provided in a structured, commonly used and machine readable form. Provision of data is free of charge and must be completed within one month or two months if the request is complex.

7.7.4 Where it is deemed that the request for data should be denied an explanation must be given to the individual along with the right to complain to the supervisory authority and to a judicial remedy within one month.

7.8 The right to object

7.8.1 Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

7.8.2 If data is processed for the performance of a legal task or for the organisation's legitimate interests, individuals must have an objection on "grounds relating to his or her particular situation". Data must not be processed unless;

- It can be demonstrated that compelling legitimate grounds for processing exist, which overrides the interests, rights and freedoms of the individual; or
- The processing of data is for the establishment, exercise or defence of legal claims.

7.8.3 Individuals must be informed of their right to object to processing of their personal data at the first communication and in the privacy notice.

7.8.4 The right to object must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

8. Rights relating to automated decision making and profiling

8.1 The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is made without human intervention.

8.2 Individuals have the right not to be subject to a decision when it has been based on automated processing and when it produces a legal effect or a similarly significant effect on the individual.

8.3 The right does not apply if the decision is necessary for entering into or performance of a contract, is authorised by law (e.g. for the purposes of fraud or tax evasion prevention) or it is based ion explicit consent.

8.4 The GDPR defines profiling as any form of automated processing that is intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour, location or movements.

8.5 When processing personal data for profiling purposes appropriate safeguards must be put in place as follows:

- Processing must be fair and transparent and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences;
- Use of appropriate mathematical or statistical procedures for profiling;
- Use of appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- Personal data must be secured in such a way that is proportionate to the risk and the interests of the individual and prevents discriminatory effects.

9. Accountability and governance

9.1 The GDPR includes provisions that promote accountability and governance and these complement the GDPR's transparency requirements.

9.2 Organisations are expected to put into place comprehensive but proportionate governance measures such as privacy impact assessments and privacy by design which are legally required in certain circumstances. These measures should minimise the risk of breaches and uphold the protection of personal data.

9.3 The accountability principle requires organisations to demonstrate that they comply with the principles and states explicitly that this is an organisation's responsibility.

9.4 To demonstrate compliance organisations must:

- Implement appropriate technical and organisational measures that ensure and demonstrate compliance such as staff training and internal audits of processing activities;
- Maintain relevant documentation on processing activities;
- Appoint a data protection officer;
- Implement measures that meet the principles of data protection by design and data protection by default, for example;
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis.

- Use data protection impact assessments where appropriate (see 9.7).

9.5 If an organisation has more than 250 employees it is required to maintain additional internal records of all of its processing activities as well as providing a comprehensive, clear and transparent privacy notice.

9.6 Internal records of processing activities must include the following information:

- Name and details of the organisation (and of other data controllers and data protection officer);
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of transfers to other countries including documentation of the transfer mechanism safeguards;
- Retention schedules; and
- Description of technical and organisational security measures.

9.7 Data protection impact assessments (DPIAs) or privacy impact assessments (PIAs) assist organisations in identifying the most effective way to comply with data protection obligations and to meet individuals' expectations of privacy. An effective DPIA will allow an organisation to identify and fix problems at an early stage, reducing costs and damage to reputation which may otherwise occur.

9.7 DPIAs are not a legal requirement but the Information Commissioner's Office (ICO) recommend them as good practice.

9.8 DPIAs should be carried out when using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals.

9.9 An effective DPIA will include:

- A description of the processing operations and the purposes including the legitimate interests pursued by the data controller;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An assessment of the risks to individuals; and
- The measures in place to address risk, including security and to demonstrate that you comply.

10. Implementation of the GDPR

10.1 Cambridgeshire County Council (CCC) in its role as the administering authority, must demonstrate compliance with the GDPR requirements by 25 May 2018. At the time of writing this report, no information or guidance has been released by CCC's Information Governance Team to assist officers of LGSS Pensions to demonstrate the necessary compliance.

10.2 Officers of LGSS Pensions have attended numerous seminars and presentations concerning the GDPR and have also formed a working group with a number of other LGPS funds including West Midlands Pension Fund, Greater Manchester Pension Fund, Local Pensions Partnership, Leicestershire, Derbyshire, Oxfordshire, Staffordshire and Shropshire Pension Funds.

10.3 The working group has met three times to discuss the impact of the GDPR and are working together to understand the specific requirements of processing pension scheme data to ensure that funds, in the absence of specific guidance from administering authorities, comply with the regulations.

10.4 In addition, officers of LGSS Pensions have raised concerns with the Local Government Pensions Committee (LGPC) that there seems to be different interpretations across the industry as to what level of compliance is actually required and whether funds need to produce their own privacy statements, separately from that of the administering authority. As a result, the LGPC are seeking legal clarification.

10.5 In the meantime, officers of LGSS Pensions are proceeding on the basis that they are responsible for the implementation of the GDPR in respect of the Fund's data processing activities. A high level action plan of the work to be undertaken to achieve compliance can be found in appendix one.

10.6 Given the Local Pension Board's role of assisting the administering authority in securing compliance with legislation it seems appropriate that it should oversee the implementation of the GDPR. As such, the Local Pension Board will receive an update at each meeting as to the progress made against the plan and other updates.

11. Relevant Pension Fund Objectives

1. Have robust governance arrangements in place, to facilitate informed decision making, supported by appropriate advice, policies and strategies, whilst ensuring compliance with appropriate legislation and statutory guidance.
2. Manage the Fund in a fair and equitable manner, having regard to what is in the best interest of the Fund's stakeholders, particularly the scheme members and employers.
3. Ensure the relevant stakeholders responsible for managing, governing and administering the Fund, understand their roles and responsibilities and have the appropriate skills and knowledge to ensure those attributes are maintained in a changing environment.
5. Continually monitor and manage risk, ensuring the relevant stakeholders are able to mitigate risk where appropriate.
10. Administer the Fund in a professional and efficient manner, utilising technological solutions and collaboration.
11. Maintain accurate records and ensure data is protected and used for authorised purposes only.

12. Finance & Resources Implications

12.1 The cost of implementing the GDPR will be met via normal operating activities of the administration budget.

13. Risk Implications

a) Risk(s) associated with the proposal

Risk	Mitigation	Residual Risk
There is no risk associated with preparing for and complying with the requirements of the GDPR.	N/A	Green

b) Risk(s) associated with not undertaking the proposal

Risk	Risk Rating
Failure to comply with the GDPR may result in a fine of up to £17m or 4% of global turnover	Red

14. Communication Implications

Website	Privacy notices will be published on the Fund's website
Communications	Scheme members will be contacted at appropriate times as to their rights under the GDPR.
Training	All officers of LGSS Pensions will receive training as to the requirements and provisions of the GDPR.

15. Legal Implications

15.1 Legal advice will be sought where deemed necessary during the implementation of the GDPR.

16. Consultation with Key Advisers

16.1 Consultation will take place as the project progresses.

17. Alternative Options Considered

17.1 Not applicable

18. Background Papers

18.1 Not applicable

19. Appendices

19.1 Appendix one – The GDPR implementation project plan.

Checklist of Key Approvals	
Is this decision included in the Business Plan?	Not applicable
Will further decisions be required? If so, please outline the timetable here	Yes – Annual Business Plan 2018-19 (March 2018)

Has this report been cleared by Head of Pensions?	Mark Whitby – 18 August 2017