SOUTH YORKSHIRE PENSIONS AUTHORITY

30th November 2017

The General Data Protection Regulation (GDPR)

1. Purpose of the Report

To inform members of the background and general principles of the GDPR and to update on preparation for its implementation on 25th May 2018.

---

2. Recommendations

Members are recommended to note the contents of the report and to comment on the progress made towards the implementation of the GDPR thus far.

---

3. Background Information

3.1 Whilst Data Protection is well established in the UK the current legislation was prepared almost twenty years ago and in that time the way we handle and move data has changed significantly, especially in recent years.

3.2 The globalisation of services through increased use of the internet, the ability to transfer huge volumes of data both faster and easier and all the new ways in which personal data can be used have culminated in the need for the revised protocols and protections that are enshrined in the GDPR which is operative from 25th May 2018.

3.3 As a pensions scheme administrator we are responsible for maintaining and processing huge amounts of personal data and whilst we have an excellent record of managing our data under the provisions of the Data Protection Act we must now review all aspects of our data management in line with the GDPR.

3.4 The GDPR will be supplemented by a substantial piece of new domestic legislation, the Data Protection Act 2018 which was introduced into Parliament in September. Whilst it sets out some important features and contains additional detail not contained in the GDPR it has been made clear that until our withdrawal from the EU it will be the GDPR itself which lays down the requirements of the new regime.

3.5 As our review will take some time the purpose of this report is to explain the key objectives and principles of the GDPR as well as provide a progress report on the work undertaken thus far.

4. The GDPR – Objectives and Outcomes

4.1 The GDPR has a number of key objectives and outcomes as follows,

- To ensure citizens have control over their personal data
- To require data holders to demonstrate how they protect personal data.
- To require data holders to be more transparent about how data will be used and who it will be shared with.
- To make all parties accountable for data protection, not just the data controller.
- To bring consistency across EU member states and globally for EU citizens (Brexit will not delay or stop the implementation of GDPR)

4.2 The Information Commissioner has expressed concern that data is not being given priority in the UK and therefore GDPR is being backed by significantly larger fines. In recent weeks, in response to speculation, the Information Commissioner has expressed that fines will remain proportionate to the level and circumstances of a breach but nevertheless it should be noted that the maximum fines are €20m or 4% of group turnover if greater.

4.3 The cornerstone of GDPR is Privacy by Design which ensures that those responsible for managing and processing personal data must adhere to the following principles,

- Personal data must be processed lawfully, fairly and in a transparent manner
- Personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
- Personal data must be adequate, relevant and limited to what is necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
- Personal; data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data is processed
- Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.4 The additional responsibilities within the GDPR require a review of our use and management of data as well as the many data relationships we have in place. The following list is not exhaustive but does contain the most significant areas that we currently have under review,

- Understanding our responsibilities as a data controller
- Map all personal data processing activities
- Understanding the legal basis for processing personal data
- The management of consent to processing data and being aware of any special category data that may require explicit consent
- Review of privacy notices and member communication of the GDPR
- Developing a breach management process

- Review our data sharing agreements and develop GDPR links with our partners
- Review/revise data retention policies
- Review personal data security policies
- Update and implement the GDPR requirements into our governance arrangements and risk management framework.

5. Progress Update

5.1 Although we are in the early stages of this major project we have made progress in a number of areas especially in relation to awareness and training. The table below identifies the work undertaken so far and its purpose in relation to the GDPR.

Work Undertaken	Purpose	Progress
GDPR Training	Management Awareness	Webinar Participation Seminar Attendance Receipt of Guidance Notes and Legal Opinion
IT Staff Certification	Training	IT Manager and Assistant IT Manager attended a full week training course with an examination to become Certified General Data Protection Regulation Practitioners
Secure E-Mail	GDPR Compliance	Purchase of Egress e-mail management system to enhance the security of data we receive and share
Data Protection Officer	GDPR Compliance	Discussions with BMBC regarding the buying in of DPO services on an as and when basis. This is in the very early stages.
Network Data Tidy	GDPR Preparation	Based on the principles of keeping data for no longer than necessary all staff have been tasked with deleting data that is no longer required and data that is required is catalogued with a review date and stored in a secure location. This is well underway.
Possible Software Purchase	Data Loss Prevention	SQL Server 2017 software contains the ability to encrypt all data at rest reducing the threat of data loss from a cyber-

		attack. The software is currently being evaluated
Staff Training	Training	Mandatory training for all staff to take place in 2018 prior to the GDPR implementation. The intention is to use BMBC's online development tool although this is subject to our evaluation of the training material once available

5.2 Further progress reports will be brought to the January & March 2018 meetings.

6. Implications and risks

- **Financial** - Expenditure to date has been contained within existing budgets. However there are potential costs associated with the implementation of the GDPR and these will be explained and itemised in the further progress reports.
- **Legal** - There are no specific legal considerations.
- **Diversity** - None

Officer responsible:
Gary Chapman Head of Pensions Administration
Phone 01226 772954
E-mail: gchapman@sypa.org.uk

Background papers used in the preparation of this report are available for inspection in the Pensions Administration Unit.