GENERAL DATA PROTECTION REGULATION (GDPR)

Report by Chief Officer Human Resources

JOINT PENSION FUND COMMITTEE AND PENSION FUND BOARD

8 March 2018

1 PURPOSE AND SUMMARY

1.1 **The purpose of this report is to advise on the requirements for the General Data Protection Regulations (GDPR) due to come into force on 25 May 2018 and the implications for the Pension Fund.**

1.2 The Scottish Borders Pension Fund, as part of a Public Authority, is required to comply with the Regulations and implement the changes as required.

1.3 Scottish Borders Council has established a project to assess the GDPR regulations and its impact on the Council as a whole. The project will also determine any gaps in existing controls and seek to implement a robust framework for managing compliance into and post May 2018.

1.4 The considerations of the GDPR for the Pension Fund will be taken into account under the project being progressed by the Council and any recommendations for change will follow whilst taking account of specific advise from a Pensions perspective, specifically guidance due to be issued by the Local Government Association.

2 STATUS

2.1 Due to competing deadlines and the information gathering required for this report the consultation procedure was not complete prior to issuing the report to Committee. Comments received during the consultation will be highlighted at the meeting.

3 RECOMMENDATIONS

3.1 **It is recommended that the Pension Fund Committee;**

(a) Notes the new requirements under the General Data Protection Regulations effective from 25 May 2018;

(b) Agrees that the Pension Fund will follow the direction of Scottish Borders Council whilst taking account of advice specific from a Pension perspective.

4 GDPR – BACKGROUND AND CHANGES

4.1 Increased globalisation and technological developments have driven the need for a more consistent and robust data protection framework across the European Union (EU). The Data Protection Act 1998 is being superseded by the new General Data Protection Regulation 2016. All organisations that handle personal data will be required to have a reasonable level of compliance prior to 25 May 2018.

4.2 The GDPR is set to ensure that businesses and organisations that collect, process and delete personal data, do so in a fair, open and secure manner to protect the data subjects.

4.3 Although the UK has voted to leave the EU and Article 50 was enacted, the Government has outlined that the UK will in the first instance transpose all EU legislation into UK legislation. Moreover, the UK Government has recently introduced its own Data Protection Bill to embed the GDPR within the UK.

4.4 Public Authorities are required to appoint a Data Protection Officer (DPO). The role must be independent and autonomous and its primary functions are to understand and interpret the GDPR and advise on and monitor compliance with the regulation. The Council's DPO is the Service Director Regulatory Service who will also act as the DPO for the Pension Fund.

4.5 Unlike under current rules, the new regulations make providers of third-party administration and other services (in their role as data processors) directly responsible for certain aspects of compliance. Appointed professional advisers and scheme actuaries will have a joint data controller role with scheme managers, thus division of responsibilities will need to be agreed; the details of which must be available to pension scheme members.

4.6 In addition to existing requirements of reporting breaches to regulation, schemes will have to report data breaches to the Information Commissioners Office (ICO) if there is a likelihood of risk to people's rights and freedoms 'without undue delay' and where feasible within 72 hours of the scheme managers becoming aware of breaches. If the breach is deemed 'high risk' and is not mitigated by data encryption or other measures, the scheme manager will have to inform affected individuals without undue delay.

4.7 There is a heightened requirement to report data breaches to the ICO within 72 hours. However, this does not apply to all incidents but is dependent on the prejudice to data subjects and the security measures that are in place. For example if encryption has made the data unintelligible there is no need to notify the ICO. At present self-reporting breaches to ICO is considered to be best practice.

4.8 Under the GDPR, the ICO has increased regulatory powers which cover new areas such as data protection impact assessments and DPOs. The ICO can also issue higher monetary penalties, especially for breaches of the GDPR principles and rights of data subjects. These fines can potentially be up to 4% of annual turnover or £17 million whichever is higher. However, the ICO has stated that it will continue to use monetary penalties as a last resort and in cases where a penalty is issued, it will be proportionate.

5 NEW AND ENHANCED RIGHTS FOR MEMBERS AND BENEFICIARIES

5.1 The GDPR will provide members and beneficiaries of the pension scheme with easier to access and enhanced rights of access to their personal data, and new rights of erasure (the 'right to be forgotten'), and data portability.

5.2 Although the need to identify the legal basis on which members' personal data are processed remains, often done by seeking members' consent; the GDPR defines 'consent' as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing', and emphasises that it can no longer be inferred from silence, pre-ticked boxes or inactivity. Furthermore, the new regulation goes on to state that 'consent' is not freely given if data subjects are unable to refuse or withdraw it without suffering detriment.

5.3 Under all grounds for processing regardless of the legal basis, members must be told how their data is used and shared. The GDPR says that the necessary information must be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.

6 SBC PROJECT

6.1 The objectives of the project is to create a framework and environment to ensure the Council is compliant with the GDPR by May 2018; build compliance into policies and procedures; provide training and raise awareness of data protection among staff and create a Data Protection Officer role.

6.2 The project scope is:

a) Review of all policy and procedures that will be impacted by the GDPR
b) Consideration of all service areas that process personal data
c) Review of all systems and technologies that enable the processing of personal data
d) Liaison (is it just liaison or something more than that?) with all third parties that process personal data on behalf of SBC
e) Delivery of controls required by the GDPR
f) Raise awareness among staff of the project and GDPR requirements

6.3 In addition to the above the Local Government Association (LGA) has commissioned Squire Patton Boggs to produce the following specifically for Local Government Pension Funds: -

- Template privacy notice
- A detailed privacy notice
- A summary privacy notice
- A memorandum of understanding document for employers

7 IMPLICATIONS

7.1 **Financial**
There are no financial implications relating to this report.

7.2 **Risk and Mitigations**
Failure to comply with the change in Regulation may lead to penalties outlined at 4.8 above. By following the lead of Scottish Borders Council and taking account of the Pensions specific advice from the Local Government Association mitigates this risk.

7.3 **Equalities**
It is anticipated that there are no adverse impact due to race, disability, gender, age, sexual orientation or religion/belief arising from the proposals in this report.

7.4 **Acting Sustainably**
There are no direct economic, social or environmental issues with this report which would affect the Council's sustainability policy

7.5 **Carbon Management**
There are no direct carbon emissions impacts as a result of this report.

7.6 **Rural Proofing**
It is anticipated there will be no adverse impact on the rural area from the proposals contained in this report.

7.7 **Changes to Scheme of Administration or Scheme of Delegation**
No changes to the Scheme of Administration of Scheme of Delegation are required as a result of this report.

8 CONSULTATION

8.1 The Chief Financial Officer, the Monitoring Officer, the Chief Legal Officer, the Chief Officer Audit and Risk and the Clerk to the Council are being consulted on and comments received will be reported at the meeting.

Approved by

Clair Hepburn **Signature .....**
Chief Officer human Resources

Author(s)

Name	Designation and Contact Number
Anthea Green	HR Shared Services Team Leader, 01835 826722

Background Papers:
Previous Minute Reference:

Note – You can get this document on tape, in Braille, large print and various computer formats by contacting the address below. The Pensions Administration Team can also give information on other language translations as well as providing additional copies.

Contact us at, Pensions Administration Team, HR Shared Services, Old School Building, Newtown St Boswells, Melrose, TD6 0SA; Tel: 01835 825205; E-mail pensions@scotborders.gov.uk.