REPORT TO: **PENSION SUB-COMMITTEE OF THE POLICY & RESOURCES COMMITTEE & PENSION BOARD– 4 DECEMBER 2017**

REPORT ON: **GENERAL DATA PROTECTION REGULATION (GDPR) – IMPACT ON PENSION FUNDS**

REPORT BY: **EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

REPORT NO: **408-2017**

1 PURPOSE OF REPORT

This report informs of the impact of the regulation replacing the existing UK data protection legislation from 25th May 2018.

2 RECOMMENDATIONS

The Sub-Committee are asked to note the information contained within this report.

3 BACKGROUND

Increased globalisation and technological developments have driven the need for a more consistent and robust data protection framework across the EU. This new regulation (EU) 2016/679 replaces the 1995 EU Directive.

4 KEY CHANGES

4.1 New & enhanced rights for members and beneficiaries

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.

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.

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'.

4.2 Greater responsibilities for data processors and controllers

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.

4.3 **Increased accountability and record keeping**

Scheme Managers (as data controllers) need to be able to demonstrate how they comply with the GDPR. Furthermore, any appointed service providers (as data processors) will have to maintain records of the processing activities for which they are responsible, and will be obliged to make those records available to the Information Commissioner's Office (ICO) on request.

4.4 **Reporting Breaches**

In addition to existing requirements of reporting breaches to regulation, schemes will have to report data breaches to the 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.

4.5 **Role of Data Protection Officer**

Scheme Managers are required to appoint a qualified person to fulfil the role of 'data protection officer' (DPO), responsible for (amongst other things) advising, monitoring compliance, and liaising with the ICO.

4.6 **Penalties**

Under GDPR, the ICO, as the UK Data Protection Ombudsman, will continue to impose upon those who breach its requirements administrative fines that are 'effective, proportionate and dissuasive'.

The level of fine imposed by the ICO will depend on considerations such as the nature and gravity of the infringement, and whether it was deliberate or negligent.

With their aim of being 'effective, proportionate and dissuasive', the maximum fine for the least-serious infringements will be €10m or, where the transgressor is a business undertaking, two per cent of its annual turnover if that is higher. These limits are doubled for the most serious breaches (at 4% of global annual turnover, up to a capped fine of €20m). The maximum monetary penalty that the ICO can impose under current UK legislation is £0.5m.

5 **STEPS BEING TAKEN BY TAYSIDE PENSION FUND**

Officers of Tayside Pension Fund are currently taking steps now to understand and document what data is held and how it is used; and becoming familiar with data subjects' rights under the GDPR, and when they will apply. The role of the appointed person for the scheme will be undertaken by the administering authority's Information & Governance Manager.

The new rules for processing by consent may prove extremely problematic, and Officers are considering current processes and their basis to ascertain what changes will be required. Current communications channels and content are being analysed and reviewed to ascertain the changes required by the new regulations.

Contractual arrangements with service providers (in their roles as data processors and joint data controllers) will be reviewed and updated, as the GDPR is more prescriptive about what needs to be set out in agreements.

6 **POLICY IMPLICATIONS**

This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti-Poverty, Equality Impact Assessment and Risk Management.

There are no major issues.

7 **CONSULTATIONS**

The Chief Executive and Head of Democratic and Legal Services have been consulted in the preparation of this report

8 **BACKGROUND PAPERS**

None

GREGORY COLGAN
EXECUTIVE DIRECTOR OF CORPORATE SERVICES **30 NOVEMBER 2017**