Committee report

General Data Protection Regulations implementation arrangements

Committee Audit and Standards

Date of meeting 9 February 2018 **Date of report** 26 January 2018

Report by Assistant Chief Executive (Business Support)

1. Object of report

To advise the committee on the findings of a regularity audit of the General Data Protection Regulations implementation arrangements. This engagement is included in the annual Internal Audit plan for 2017/18.

2. Background

SPT is obligated to process data for business purposes. Data can be of a personal sensitive nature and must be processed in line with the 1995 European Union (EU) data protection directive (Data Protection Act 1998). New EU General Data Protection Regulations (GDPR) are due to come into force on 25 May 2018. The new regulations replace the 1995 data protection directive, thus do not require any enabling legislation to be passed by the bloc's national governments, and extend the scope of EU data protection law to all foreign companies that process the data of EU residents. The rules are designed to strengthen the privacy rights of European citizens and make businesses more accountable for data protection.

SPT has documented procedures and processes in place for compliance with Data Protection Act 1998. These arrangements are actively being reviewed for compliance with the new regulations.

The objective of this engagement was to assess the arrangements for implementation of the General Data Protection Regulations (GDPR) in accordance with legislation.

This engagement tested elements of the internal controls and mitigation against SPT 22: Governance arrangements, as identified in the corporate risk register.

3. Outline of findings

The engagement found that a GDPR gap analysis has been carried out, a data mapping process is underway and a working group has been convened to agree a work plan and actions for compliance with the new GDPR requirements.

The engagement identified a requirement to review subject access request procedures and reporting arrangements in compliance with the new GDPR requirements.

There are areas for improvement, and these areas have been addressed by six audit recommendations. Legal services and Digital management have agreed to implement these recommendations, which are currently being actioned.

Note: training for members on GDPR will be scheduled for a future date in regard to the committee cycle.

4. Conclusions

The Audit and Assurance team has undertaken a regularity audit of the General Data Protection Regulations implementation arrangements. Six recommendations have been agreed from this engagement.

Key controls exist and are applied consistently and effectively in the majority of areas tested in this engagement.

Reasonable assurance can be taken from the controls in place for the areas covered in this engagement.

5. Committee action

The committee is asked to note the contents of this report and agree that the Audit and Assurance Manager submits a follow-up report on the implementation of the recommendations to a future meeting.

6. Consequences

Policy consequences	*None*
Legal consequences	*None*
Financial consequences	*None*
Personnel consequences	*None*
Social Inclusion consequences	*None*
Risk consequences	*As detailed in the report*

Name	Valerie Davidson	**Name**	Gordon Maclennan
Title	**Assistant Chief Executive (Business Support)**	**Title**	**Chief Executive**

For further information, please contact Iain McNicol, Audit and Assurance Manager on 0141 333 3195.