Committee report

Regularity audit of the General Data Protection Regulations arrangements

Committee Audit and Standards

Date of meeting 19 February 2021 **Date of report** 27 January 2021

Report by Assistant Chief Executive

1. Object of report

To provide the committee with the findings of a regularity audit of the General Data Protection Regulations processed within SPT. Members agreed, at the committee meeting of 12 June 2020, to amend the Internal Audit plan for 2020/2021 to include this engagement.

2. Background

As members will be aware, the General Data Protection Regulation (GDPR) came into force on 25 May 2018. As a result, all organisations, public and private, were required to reassess and implement significant changes to organisational processes to ensure processes are consistent with the significant data protection changes. The revised regulations are based on seven key principles to processing personal data:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security); and
- Accountability.

The objective of this engagement was to reassess the post implementation arrangements of the General Data Protection Regulations (GDPR), assess whether they were operating as intended and were effective.

This engagement tested elements of the internal controls and mitigation against SPT22: Governance arrangements, as identified in the corporate risk register.

3. Outline of findings

SPT has a Data Protection Policy, processes and procedural guidance in place to maximise the compliance with Data Protection legislation.

The internal arrangements for processing data within SPT apply to all employees, members and other stakeholders. These arrangements implemented around May 2018 are applied to all areas of service delivery and require constant monitoring and review.

Engagement testing (November 2020) identified a requirement to refresh and update internal procedures, having assessed their operation within the revised regulatory framework, as well as the need to improve data cleansing and data processing arrangements

The audit identified some areas for improvement, and these have been addressed by seven recommendations.

Legal services management have agreed to implement these recommendations, which are currently being actioned.

4. Conclusions

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

While seven recommendations have been made, members are advised that key controls exist and are applied consistently and effectively in the majority of areas tested, and thus reasonable assurance can be taken from this engagement.

5. Committee action

The committee is asked to

- note the contents of this report, including the recommendation of 7 action points; 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.*
Equalities consequences	*None.*
Risk consequences	*As detailed in the report.*

Name	Valerie Davidson	**Name**	Gordon Maclennan
Title	**Assistant Chief Executive**	**Title**	**Chief Executive**

For further information, please contact Iain McNicol, Audit and Assurance Manager.

Reasonable assurance

Agreed action plan: regularity audit of the General Data Protection Regulations arrangements

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1	Information Governance Group Governance arrangements for the internal Information Governance Group (IGG) should be reviewed and refreshed.	Medium	The Terms of Reference for the internal IGG will be reviewed and updated, where required.	Information Governance Officer	March 2021
2	Policy and procedures Policy and procedures related to data protection should be updated annually as required by the Data Protection Policy.	Medium	The Data Protection Policy will be reviewed and updated to reflect any change(s) to Scottish Government/UK Government guidance following Brexit agreement.	Assistant Chief Executive	March 2021
3	Information Asset Register The Information Asset Register should be reviewed and updated in accordance with Information Commissioner's Office (ICO) GDPR guidance and Public Records (Scotland) Act 2011 requirements.	Medium	The Information Asset Register will be reviewed and updated to reflect service provision.	Information Governance Officer	March 2021
4	Data cleansing project The internal data cleansing initiative requires a refresh with milestone and reporting requirements identified. Digital data should be regularly reviewed and managed to comply with guidance and standards.	High	The internal data cleansing project will be reviewed with clarity on milestones and reporting requirements.	Information Governance Officer	February 2021

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
5	<u>Data Processing Agreements</u> Arrangements for updating and reviewing Data Processing Agreements should be clarified (e.g. for changes in systems and processes) to ensure they remain fit for purpose.	Medium	The data processing arrangements will be reviewed and updated, where required.	Information Governance Officer	March 2021
6	<u>Data Protection Impact Assessment(s)</u> The Information Governance officer should review the process for undertaking Data Protection Impact Assessment(s).	Medium	The process for undertaking data protection impact assessments will be reviewed and updated, where required.	Information Governance Officer	March 2021
7	<u>Near misses and breaches</u> Records maintained in respect of near misses and breaches should be reviewed and enhanced. The records should be complete and provide a holistic overview of incidents, lessons learnt, actions taken and follow-up work undertaken.	Medium	The data protection incident log will be refreshed to provide performance management information.	Information Governance Officer	March 2021