Committee report

Proposed Internal Audit Plan Amendment - General data protection regulations update

Committee Audit and Standards

Date of meeting 12 June 2020 **Date of report** 1 June 2020

Report by Assistant Chief Executive

1. Object of report

To advise of a proposed amendment to the current year Internal Audit plan to accommodate a review of controls relating to SPT's approach to General Data Protection Regulations (GDPR).

2. Background

As members will be aware the revised GDPR came into effect in May 2018. At that time and in preparation of this significant change, SPT undertook a process of providing briefings and training to all staff, based on a risk-assessed approach. This was undertaken across the organisation with refresher sessions where it was deemed relevant or necessary to do so. In addition, briefing sessions were made available to all Board members.

Since the introduction of the GDPR, SPT has also implemented an Information Management Governance Group, again with representatives from all parts of the organisation. This group, chaired by the Assistant Chief Executive, seeks to bring up to date information management practices, recognising that information management is a difficult and complex area. The Group interfaces with the Digital Governance Group at all stages as there is a clear overlap between the two areas as much information is now held or processed in digital form.

Good progress has been made in the area of GDPR and information management over the last few years, although there is still much to do. The Partnership has already approved several papers relating to Information Management and GDPR policies.

Specifically relating to GDPR, good progress has been made in highlighting the importance of the good information practices and ensuring that the organisation takes its responsibilities in this area seriously, with all breaches and near misses investigated and learning points captured. SPT maintains and re-iterates staff communications in this field as well, to ensure that the learning points are disseminated accordingly.

It is proposed to include a detailed review of SPTs GDPR practices in the Internal Audit plan 2020/2021, bringing together all of the learning points that have been captured to date, and reviewing the control measures that have been implemented to date.

The purpose of this review is to ensure that, two years on from the implementation of the original GDPR processes, that the risks and controls now remain valid. GDPR remains a key operational risk principally as it includes both data but also human interaction in the management of that data. The review is intended to ensure that operational risk is managed accordingly, thus protecting both the reputation of SPT, and minimising the likelihood of financial penalties.

This proposal to review the controls follows an incident during the COVID – 19 working from home arrangements which resulted in the release of a small amount of data incorrectly to a small number of bus operators. Much of the information was already available publicly on the SPT website, however other details were not. Specifically, on 30 April 2020, a payment run for bus operator payments was processed, and the remittance advice report run electronically from the financial ledger system. However, due to the current lockdown arrangements (working from home), this report could not be printed in the normal fashion. Instead, the remittance advice for the 30 April payment run remained unsorted and unfortunately was sent in error to 15 bus operators.

This error was communicated to SPT by a bus operator quickly after the issue of the information, and the original communication was immediately recalled. SPT wrote to all affected bus operators to inform them of this incident on the same day.

As members are aware, some bus operators are sole traders, thus information contained in the remittance advice, namely bank account details, was deemed as personal data, and whilst this information is publically available from Companies House, regulators and their websites, it is not information that SPT would normally share.

The Information Commissioner's Office (ICO) define a personal data breach as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.*'

On 1 May 2020, as a result of the above, SPT made a self-declaration report to the ICO on the remittance advice incident of the previous day. Following consideration of the incident, and the steps that SPT took, the ICO has subsequently determined that no action will be taken.

An action plan on the remittance advice process is found below this report.

It is normal to review the circumstances around such matters, but given the timescale between implementation of the GDPR processes, it is considered timely to review the controls and reporting arrangements around such matters, and it is proposed to do this via the Internal Audit plan. This is an amendment to the approved Internal Audit plan and can be accommodated within the time available.

3. Committee action

The committee is asked to note the proposal to amend the Internal Audit plan to accommodate a review of the GDPR process and controls to ensure that they are operating effectively, and to note that this will be reported to a future Audit & Standards Committee.

4. Consequences

Policy consequences	*Management action was taken in accordance with the Information Security Policy.*
Legal consequences	*None.*
Financial consequences	*None.*
Personnel consequences	*None.*
Equalities consequences	*None.*
Risk consequences	*Management action to change the current process will mitigate information security risk.*

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

For further information, please contact Valerie Davidson, Assistant Chief Executive on 0141 333 3298.

Agreed action plan: Remittance advice process

Recommendation	Priority	Action Proposed	Lead Officer	Due date
<u>Remittance advice process</u> Finance management should review and where appropriate, automate the internal remittance advice process. Creditor standing data (email addresses) should be updated and used to communicate with service providers/suppliers. Personal data (bank account details) should be removed from standard remittance advice reports. Any revision(s) to the remittance advice process requires to be risk assessed and tested internally prior to making any changes.	High	The remittance advice process will be reviewed, updated, tested and documented to reflect changes to service provision. The software supplier will be contacted to remove bank account data from standard remittance advice reports.	Chief Accountant	June 2020