General Data Protection Regulation (GDPR) and Cyber Security

1. INTRODUCTION

1.1 The purpose of this report is to provide the Board with an update on the work being undertaken by Officers in preparation for the GDPR and the Scottish Government's (SG) Cyber Security Action Plan.

2. BACKGROUND

2.1 The GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

2.2 The GDPR will introduce significant new fines for personal data breaches from May 2018 which reinforces the key role that cyber security has in underpinning digital public services that handle personal data.

3. GDPR

3.1 Following a review of the status of current information governance initiatives, it was concluded that while SEStran holds little personal data, there are a number of compliance tasks which must be addressed in a proportionate way.

3.2 The following draft documents (Appendix 1) have been prepared and have been reviewed by the Partnership's legal advisers.

- A SEStran Privacy Notice to describe, for the public, SEStran's use of personal data with the details required by GDPR.
- A revised SEStran Data Protection Policy to outline arrangements for GDPR compliance.

3.3 Other actions include reviewing our SLAs to incorporate the requirements of GDPR article 28 and reviewing disposal periods for staff mailboxes.

4. CYBER SECURITY

4.1 Following on from reports presented to the September and November meetings last year, which outlined the requirements of the SG Cyber Security Public Sector Action Plan, the Committee should note that SG have issued grant award letters of up to £1000 for Cyber Essentials Pre-Assessment.

4.2 The pre-assessments are a precursor to Cyber Essentials accreditation and will identify any remedial actions that may be required before accreditation can be awarded. The pre-assessment also recommends the level of accreditation required.

4.3 Members should note that the cost of any remediation work will be the responsibility of SEStran, as is the cost of accreditation. Whilst the cost of remedial works is unknown, indications, so far, suggest that the organisation is already 85% compliant.

4.4 Timescales for the project are:

- Pre-Assessment March 2018
- Accreditation October 2018

5. RECOMMENDATIONS

5.1 The Board is asked to:

5.2 Approve the Data Protection Policy and Privacy Notice for implementation in advance of the GDPR regulations coming into force on 25th May 2018, and:

5.3 Approve the appointment of the Business Manager as SEStran Data Protection Officer, and:

5.4 Note that further progress reports on Cyber Security will presented to the Partnership Board.

Angela Chambers
Business Manager
9th March 2018

Appendix 1 Draft Data Protection Policy and Privacy Notice

Policy Implications	Revised Data Protection Policy to be adopted
Financial Implications	Potential remedial works and cost of accreditation but it is anticipated that the costs will be contained within existing budgets.
Equalities Implications	None
Climate Change Implications	None

DATA PROTECTION POLICY

DOCUMENT VERSION CONTROL – GOVERNANCE SCHEME **Date**	**Author**	**Version**	**Status**	**Reason for Change**
Oct 2017	SEStran	1.0	Adoption of version control	Implementation
Feb~~Jan~~ 2018	SEStran	1.2~~1~~		Adapted for GDPR compliance.

A. **INTRODUCTION**

1.This is a statement of the Data Protection Policy adopted by SEStran, the Regional Transport Partnership (RTP) for the South East of Scotland. This policy is applicable to all personal data held by the RTP. It applies to all employees and elected members of the RTP and to any contractors or agents performing work for or on behalf of the RTP and any other individuals with access to SEStran's information.

2.SEStran is a partnership of 8 councils; Edinburgh, Fife, Clackmannanshire, Scottish Borders, Falkirk, West Lothian, East Lothian, and Mid Lothian and provides a wide range of services not only within these boundaries but as part of a group of RTPs across Scotland.

3. SEStran needs to process certain types of data about people with whom it deals in order to operate ("personal data"). This includes current, past and prospective employees, suppliers, clients and customers, and others with whom it communicates.

4. In order to comply with the GDPR and the Data Protection Act 2018 (GDPR), SEStran must ensure that all personal data are securely stored and processed lawfully, however it is collected, recorded and used. Safeguards are in place to support compliance with the legislation and these are detailed below.

5. SEStran regards the safekeeping of all personal data as paramount to maintaining confidence between it and those with whom it deals. SEStran endeavours to fulfil all the requirements of the ~~Act~~ GDPR while remaining open and accessible by the public.

B. **SCOPE**

This policy is applicable to all personal data held by SEStran whether the information is held or accessed on SEStran premises or accessed remotely via mobile or home working or by using network access from partner organisations. Personal information held on removable devices and other portable media is also covered by this policy.

C.**THE DATA PROTECTION PRINCIPLES**

To that end, SEStran fully endorses and adheres to the six GDPR Principles set out below. ~~These Principles are that personal data must be:~~

~~a) processed lawfully, fairly and in a transparent manner… ('lawfulness, fairness and transparency');~~

~~b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ('purpose limitation');~~

~~c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');~~

~~d) accurate and, where necessary, kept up to date… ('accuracy');~~

~~e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed… ('storage limitation');~~

~~f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). (GDPR Article 5)~~

Lawfulness, fairness and transparency

1. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation

2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).

Data minimisation

3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

4. Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

Integrity and confidentiality

Formatted: Default, Space After: 9.1 pt, No bullets or numbering, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

6. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

In addition, SEStran is responsible for, and must be able to demonstrate compliance with, the data protection principles listed above, in accordance with the principle of accountability. It must keep a full and accurate record of its personal data processing activities, e.g., the lawful basis for the processing in question, who is undertaking these activities and with what data, the results of any data protection impact assessment or data protection audit and details of any data breaches and actions taken.

Formatted: No bullets or numbering, Tab stops: Not at 1.27 cm

RESPONSIBILITIES

- The Partnership Director has specific senior responsibility for data protection within SEStran. The Partnership Director has responsibility for ensuring that the information under their control is collected, processed and held in accordance with this policy and the GDPR.
- The Business Manager is the designated Data Protection Officer for SEStran, advising on and monitoring SEStran's compliance with GDPR and providing a point of contact for data subjects and the Information Commissioner's Office.
- All employees and elected members of the RTP and any contractors or agents performing work for or on behalf of the RTP and any other individuals with access to SEStran's information have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with the SEStran's information policies, procedures and other guidance.
- All users have a responsibility to report any observed or suspected breach of this Data Protection Policy or related information procedures and guidance. All incidents must be reported to ~~t~~the Data Protection Officer.~~Office Manager~~

WHAT SESTRAN WILL DO

To ensure compliance with the above data protection principles SEStran shall, through appropriate management and strict application of criteria and controls;

- maintain appropriate and accurate transparency information (a privacy notice) on its website clearly signposted from any portals or forms which may collect personal data;
- meet its legal obligations to specify the purposes for which data is used;
- collect and process appropriate data, and only to the extent that it is required to fulfil~~l~~ operational needs or to comply with any legal requirements;
- ensure the quality of the data used;
- apply the retention policy set out in the Business Classification Scheme to determine the length of time the data is held;
- ensure that rights of people about whom data is held can be fully exercised under the GDPR (~~T~~hese these are described below~~.~~);
- ensure that e-newsletters and similar materials are only distributed to corporate email addresses or to the personal email addresses of current board members, current forum members or individuals who have signed up to receive them;
- ensure that the Data Protection Officer has sight of all new projects and business activities to consider whether data protection issues arise and to include Privacy By Design as appropriate;
- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred outside the European Economic area without suitable safeguards.

In addition, SEStran will ensure that:

- there is a ~~designed~~ designated Data Protection Officer for the organisation;
- everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal data is appropriately trained do to so;

- everyone managing and handling personal data is appropriately supervised;
- anyone wishing to make enquiries about handling personal data knows what to do;
- queries about handling personal data are competently and courteously dealt with;
- methods of handling personal data are clearly described;
- a regular review and audit is made of the way personal data is managed;
- methods of handling personal data are regularly accessed and evaluated; and
- performance with handling personal data is regularly accessed and evaluated.

DATA RIGHTS

SEStran will ensure individuals' rights are respected with regard to their personal data. Rights under GDPR include:

- the right to be informed that processing is being undertaken;
- the right to withdraw consent to processing, where appropriate
- the right of access to one's own personal data and to specific information about the processing;
- the right to object to and prevent processing in certain circumstances;
- the right to be notified of certain data breach incidents that relate to their personal data (see below)
- the right to rectify or restrict inaccurate data
- the right or erase data or to data portability in certain circumstances
- the right to challenge processing reliant on legitimate interests or public interest
- the right to make a complaint to the UK Information Commissioner.

All requests relating to GDPR rights must be directed to the Data Protection Officer who will ensure that appropriate actions are taken and a response issued without undue delay and, except in certain ~~at~~circumstances, at least within one month.

Formatted: Font: Arial

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

Formatted: Font: Arial

Formatted: Font: Arial

Formatted: No bullets or numbering

Formatted: Font: Arial

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

PERSONAL DATA BREACHES

Any incident which may impact on the confidentiality, integrity or availability of personal data held by SEStran must be reported immediately to the Data Protection Officer. She will record the incident, ensure appropriate mitigation measures are in place and consider whether the incident is a personal data breach which presents a risk to individuals.

The DPO will present a report to the Partnership Director including if appropriate, a recommendation on whether to report a breach to the Information Commissioner's Office within 72 hours of SEStran becoming aware of the incident.

If the Partnership Director decides that an incident constitutes a reportable breach, the DPO will report the incident to the ICO and liaise as appropriate. Affected data subjects may also require to be informed if there is a high risk to their rights and freedoms as a consequence of the data breach.

GENERAL

This document states SEStran's primary, general policy with regard to Data Protection. SEStran also has policies, procedures and guidance, as appropriate, for specific types of data maintenance and data type. Additional data specific policies, procedures and guidance will be adopted as and when necessary.

REVIEW

This policy will be reviewed annually, to take account of developments within ~~SESTRAN~~ SEStran and legislative requirements

Use of personal data at SEStran

This document describes how SEStran uses personal data (information relating to individuals).

South East of Scotland Transport Partnership (SEStran) is a **Data Controller** (ICO Registration Number: Z9382423), which means we are responsible in law for how we use any personal information.

Our **Data Protection Officer, Angela Chambers,** can be contacted with any concerns or requests relating to our use of personal data**:**

Angela Chambers

Business Manager

Area 3D (Bridge)
Victoria Quay
Edinburgh
EH6 6QQ

Direct Dial: 0131 524 5154
Mobile: 07703 974 311
Email: angela.chambers@sestran.gov.uk

Why does SEStran process personal data?

SEStran processes a minimal amount of personal data in the exercise of our official authority under the Transport (Scotland) Act 2005 including:

- Administration of the partnership;
- Development and publication of regional transport strategies;
- Consultation, promotion and communication on issues relating to sustainable and efficient transport in the partnership area;
- Administration of projects and grant schemes.

SEStran also processes personal data relating to its staff to meet our legal obligations as an employer (including in connection with employment law, social security and social protection law) and for the performance of our contracts of employment with our staff. This may include processing some special categories of personal data such as health information.

What personal data does SEStran process?

Formatted: Normal

The personal data SEStran processes includes:

- **For the public:** Names and contact details for individuals responding to consultations, raising concerns or complaints, subscribing to newsletters or attending events;
- **For staff:** Name and contact details, banking details for payroll management; performance and health information for employment administration and contract purposes;

- **For suppliers and contractors:** Names and contact details for the management of the supplier relationship; bank details of sole traders for the purposes of making payments;
- **For Forum members:** Names and contact details for the administration of meetings and distribution of newsletters and information on SEStran activities;
- **For partnership board members:** Name and contact details; banking details for payment of expenses; records of views expressed and of attendance at and contributions to meetings.

Formatted: Font: Not Bold

SEStran undertakes no automated decision making affecting individuals or profiling of personal data.

With whom will SEStran share personal data?

The following organisations will receive personal data as necessary from SEStran:

- Microsoft UK are data processors, hosting SEStran's IT systems on Office 365;
- Partner local authorities or the Scottish Public Sector Ombudsman may receive data relating to complainants or correspondents where correspondence from the public should appropriately be redirected to the authority or SPSO;
- City of Edinburgh Council will receive personal data relating to employees and contractors for the purposes of the management of our payroll and for financial management, which they provide on our behalf;
- Falkirk Council will receive personal data relating to staff and job applicants for the purposes of the human resources management support they provide on our behalf;
- Scottish Government receive personal data relating to our staff and visitors for the purposes of providing facilities management services at our Victoria Quay office.

SEStran will put appropriate written arrangements in place with these organisations to protect your personal data.

SEStran transfers no personal data outside the European Economic Area. Microsoft hosts data on our behalf on servers within the UK and the European Union.

How long does SEStran retain personal data?

Personal data is managed in line with our records retention policy [Link to Business Classification Scheme]. For example, consultation responses are retained for five years before being securely deleted.

Your Rights ~~to personal data~~

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

~~Under data protection law you have the right to:~~

- ~~See and receive a copy of the personal data SEStran holds relating to you;~~
- ~~To have inaccuracies in your own corrected;~~
- ~~To receive specific information relating to our reasons for processing your data.~~

~~In limited circumstances, you may have the right to have data deleted or to object to our processing your data.~~

These rights are subject to certain caveats and exemptions under GDPR.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

To exercise these or any of your rights under ~~data protection law~~GDPR, please contact the Data Protection Officer using the details above.

For more information on data rights see the website of the Information Commissioner's Office.

Complaints or concerns relating to SEStran's use of personal data

If you have any concerns relating to SEStran's management of personal data, you can raise them with the Data Protection Officer, Angela Chambers at the contact details above.

If you remain dissatisfied you can complain to the Information Commissioner's Office by phoning their helpline on 0303 123 1113, by using their online portal for raising concerns or by post at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF