SEStran
South East of Scotland Transport Partnership

DATA PROTECTION POLICY

DOCUMENT VERSION CONTROL

Date	Author	Version	Status	Reason for Change
Oct 2006	SEStran	1.0	FINAL	Policy Adopted
Oct 2017	SEStran	1.1	FINAL	Adoption of version control
Feb 2018	SEStran	1.2	FINAL	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 Midlothian 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 General Data Protection Regulations (GDPR) and the Data Protection Act 2018, 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 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.

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

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.

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 the Data Protection Officer.

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 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 (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 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 circumstances, at least within one month.

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. They 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 and legislative requirements