Strathclyde Partnership for Transport

Data Protection Policy

Action	Date	Version	Owner	Review by
Created	12/09/2018	0.3	HM	
Updated	06/11/2018	1.0	HM	
Updated				

Contents

1. Introduction

1.1. SPT collects, uses and shares certain personal information about individuals in order to allow it to undertake its statutory functions and to deliver services. This includes information about current, past and prospective employees, suppliers, pupils being transported in accordance with agency agreements with our constituent councils, customers, and others with whom SPT communicates.

1.2. In addition, SPT may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies. This personal data must be dealt with properly however it is collected, recorded and used - whether on paper, held on or produced by a computer or recorded on other material - and there are safeguards to ensure this. The General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018, both introduced in May 2018, require organisations which handle personal data to collect, process and hold that information securely and responsibly. This includes only collecting and using what we absolutely require, and destroying the information safely when it is no longer required.

1.3. The GDPR creates rights for individuals and also strengthens some of the rights that previously existed under the Data Protection Act 1998. We have worked to make sure that these rights are properly implemented, and any changes in the ways we collect, store, use or share data are appropriately communicated.

1.4. SPT will comply with the GDPR.

2. Scope of Policy

2.1. This policy is applicable to all personal data held by SPT, whether the information is held or accessed on SPT premises or SPT-issued devices, on removable devices and other portable media, or accessed via mobile or home working.

2.2. It applies to all employees, members of the Partnership, third party suppliers and any other individuals with access to SPT's information.

3. The Data Protection Principles

3.1. The lawful and correct handling of personal data is fundamental to SPT's successful operation and to maintaining confidence in SPT. SPT will ensure that it will treat personal data lawfully and correctly.

3.2. To that end, SPT endorses and adheres to the **Data Protection Principles** set out in the GDPR, which are as follows:

- **Lawfulness, fairness and transparency**

  Organisations should only process personal data lawfully and in a fair way. We must tell people very clearly what we intend to do with the personal data we collect about them.

- **Purpose Limitation**

  Personal data should be collected for specific, explicit and legitimate purposes. If we have collected personal data, and told the individual what we will do with it, we can't use the information for another purpose simply because we hold it.

- **Data Minimisation**

  Collected personal data should be adequate, relevant and limited to what is needed. We should only collect the personal data that is required for the task.

- **Accuracy**

  Personal data must be accurate and kept up to date. Reasonable steps should be taken to rectify any data that is found to be inaccurate. Any personal data we hold should be routinely reviewed to ensure it is accurate.

- **Storage Limitation**

  Personal data should not be kept in a form which allows individuals to be identified for any longer than is necessary for the purpose for which it was collected. Our systems and processes should be designed to delete personal data as soon as it is no longer needed. This might mean that parts of records are deleted at different times.

- **Integrity and Confidentiality**

  Personal data should be protected against unauthorised access, accidental loss, destruction or damage. Both physical and technical controls should be used as appropriate.

4. Data Subject Rights

4.1. The individual about whom personal data is held (the data subject) also has rights under the GDPR and SPT endorses and adheres to these rights.

4.2. To be informed about what will happen to their personal data. This will be managed through privacy notices.

4.3. To access personal data held about them. Under GDPR organisations have 30 days to provide this information. That said, in certain cases, where there is a lot of material, this may be extended to three months. Individuals can request:

- to have inaccurate personal data amended.
- to object to certain types of processing.
- to restrict automated decision-making and profiling.
- to have their personal data deleted. This 'right to be forgotten' will only apply in certain circumstances.
- to have their personal data transferred directly to another data controller. Again, this will also only apply in certain circumstances.

4.4. SPT will provide information to individuals as to exercising their rights under the GDPR.

5. How we will ensure compliance

To ensure compliance with the data protection principles in the GDPR, SPT will adopt new processes, including:

5.1. We will maintain an Information Asset Register, identifying the personal information we hold, the reasons why we hold it, and the Information Asset Owner (IAO) for each type of information. Tool-box talks are delivered to each IAO, tailored to the data for which they are responsible.

5.2. We will observe conditions regarding the fair collection and use of data.

5.3. We will meet the legal obligations in relation to specification of the purposes for which data is used.

5.4. We will 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.

5.5. We will ensure the quality of the data used.

5.6. We will apply checks to determine the length of time the data is held.

5.7. We will take appropriate technical and organisational security measures to safeguard personal data.

5.8. We will ensure that personal data is transferred in accordance with the GDPR.

5.9. We will ensure that all our staff managing and handling personal data are appropriately trained and supervised and is fully aware of their data protection responsibilities.

5.10. We will regularly review and audit internal data handling processes and procedures.

5.11. We will ensure that data subject rights can be exercised under the GDPR.

6. SPT's Incident Notification Process

6.1. If, despite the security measures taken by SPT to protect the data held by it, a breach occurs the breach must be dealt with effectively and in accordance with the terms of the GDPR.

6.2. The breach may arise from a theft, a deliberate attack on SPT's systems, the unauthorised use or sharing of personal data, accidental loss or equipment failure. However a breach occurs, it must be responded to and managed appropriately.

6.3. All staff will be aware of their obligations in terms of SPT's Incident Notification Process, which is also available on the intranet. The first stage of reporting shall be to SPT's Information Governance and Committee Services Officer, and SPT's internal procedures in relation to this will be reviewed annually.

7. Roles and Responsibilities

7.1. Information Governance and Committee Services Officer

The Information Governance and Committee Services Officer (IGO), in conjunction with the Senior Legal Advisor, is responsible for developing, delivering and maintaining a comprehensive information governance and security framework for SPT. The IGO will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information, and will be responsible for ensuring staff are aware of their duties and responsibilities under the GDPR and keeping the intranet up to date.

The IGO is responsible for monitoring the personal information SPT is holding and processing, and keeping the IAR and record of IAOs updated.

The IGO will assist departments in the carrying out of data protection impact assessments (DPIA) where required. The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If a DPIA identifies a high risk which cannot be mitigated, the Information Commissioner's Office ("the ICO") must be consulted.

7.2. Assistant Chief Executive

SPT's Assistant Chief Executive has overall responsibility for Data Protection and for overseeing the development, maintenance and monitoring of SPT's arrangements for Data Protection including:

- the development, publishing, maintenance and administration of the Data Protection Policy;
- the provision of data protection training for staff within SPT;
- the development of best practice guidelines; and
- the carrying out of compliance checks to ensure adherence, throughout SPT, with the GDPR.

7.3. Directors/Managers and Departmental Heads

7.3.1. Directors/Managers and Departmental Heads have responsibility for:

- ensuring that their staff undertake and understand their roles and responsibilities in terms of collecting, using and processing personal information in accordance with this policy and the GPDR;

- ensuring that their department/team adopts a Privacy by Design approach across their service areas, i.e. to ensure that all new processes, ways of working and systems must be designed to ensure that personal data is only processed when necessary and personal data is deleted as soon as possible; and

- undertaking DPIAs in respect of all new processes, ways of working and systems, e.g. a DPIA might relate to large scale processing such as the introduction of an SPT-wide case management system, or smaller scale processing like the introduction of a new form or app which collects personal data.

7.3.2. All employees, Partnership members, contractors, consultants, partners, agents and other individuals handling personal information on behalf of SPT have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with SPT's information management and governance policies, procedures and other guidance.

8. Related Guidelines and Policies

8.1. This policy statement is underpinned by SPT's supporting policies, procedures and guidelines including the documents listed below:

- Digital and Information Security Policies
- CCTV Guidance
- Information Management Strategy
- Code of Conduct for Employees
- Incident/Breach Notification Process

9. Breach of policy

9.1. A breach of this policy shall not be permitted and may lead to disciplinary action.

10. Training

10.1. The Information Governance and Committee Services officers, in conjunction with the Senior Legal Advisor and the HR team, will arrange for appropriate training to be delivered to all staff in line with their involvement in handling personal data as part of their role within SPT. The training requirement will be reviewed annually and, where appropriate, refresher training will be delivered.

11. Review

11.1. The policy and the associated procedures will be reviewed annually by the Assistant Chief Executive.

Signature:_____ Print: _____

Date:_____ Designation: Assistant Chief Executive