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	04/12/2020	1.01	MT	MT
Updated following Brexit	15/01/21	1.02	MT	IGG
Approved by Partnership	12/03/21	2.0	MT	Approved by Strategy Group Jan 21

Contents

1. Introduction

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 local authorities, customers, and other stakeholders with whom SPT communicates. In addition, SPT may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies.

The Data Protection Act 2018 (DPA) requires 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 securely when it is no longer required. The General Data Protection Regulation (GDPR) has now been absorbed into the DPA as part of UK law following Brexit, and is known as “the UK GDPR”.

Under the UK GDPR and the DPA individuals have certain rights with regard to their data and SPT ensures we are able to provide for these rights.

The Privacy and Electronic Communications Regulations (PECR) have also been set out in UK law. These regulations cover marketing, cookies and electronic communications and also form part of the data protection legislation.

The Information Commissioner’s Office (ICO) is the UK regulator (supervisory authority) for all matters relating to data protection.

1. Scope of Policy

This policy is applicable to all personal data held by SPT, whether the information is held or accessed on SPT premises or elsewhere.

It applies to all employees, members of the Partnership, third party suppliers, contractors, agents, consultants and any other individuals with access to SPT’s information.

2. Definitions

“Personal data” is information that relates to an identified or identifiable individual.

“Special category data” is personal data which is more sensitive, and requires greater protection. Special category data can only be processed in more limited circumstances. The types of special category data are:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)

- health
- sex life
- sexual orientation.

Criminal offence data (e.g. Disclosure or PVG returns) is treated similarly to special category data.

“Data Controller” - determines the purposes and means of processing personal data.

“Data Processor” - is responsible for processing personal data on behalf of and in accordance with instructions given by a controller.

3. Legal Basis for Processing

All processing of personal data must meet one of the six lawful bases defined in Article 6 of the UK GDPR:

- Where we have the **consent** of the data subject
- Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject
- Where necessary to meet a **legal obligation**
- Where necessary to fulfil a **contract**, or pre-contractual obligations
- Where we are protecting someone’s **vital interests**
- Where we are fulfilling a **public task,** or acting under official authority

There are certain conditions that must be met before we process special category data, and this requires a second legal basis for processing to be defined under Article 9 of the UK GDPR. We require a basis in law to process this kind of data or meet a condition from Schedule 1 of the DPA 2018. This is especially relevant where we rely on the ‘substantial public interest’ condition, which is common in SPT, for processing special category data.

UK GDPR Condition	**Schedule 1 Condition**
Explicit consent	
Employment, social security and social protection	+ Condition 1
Vital Interests (life or death)	
Not for profit bodies (membership data)	
Manifestly made public by the data subject	
Legal claims or judicial acts	
Substantial public interest	+ one of Conditions 6-28
Health or social care	+ Condition 2
Public health	+ Condition 3
Archiving, research, statistics	+ Condition 4

The ICO has published detailed guidance on processing of special category data and you can find more information *here*.

If you are processing special category data or criminal offence data, please also contact the Information Governance Officer for further advice. Data processing relating to criminal offences (or potential criminal offences) may also require to be justified.

The most appropriate legal bases for processing different kinds of data are recorded in the Information Asset Register.

4. The Data Protection Principles

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. SPT endorses and adheres to the **Data Protection Principles** set out in the legislation:

- **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. Information about how long different records should be held can be found in the Records retention schedules published on the Intranet.

- **Integrity and Confidentiality (Security)**

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

In addition, organisations have to demonstrate their accountability and compliance with the legislation.

5. Data Subject Rights

The individual about whom personal data is held (the data subject) has rights under the legislation as follows:

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

To access personal data held about them. Data subjects can request information about the data that an organisation holds about them, known as a 'data subject access request', or DSAR. Organisations have 1 month to provide this information. In certain cases, this may be extended to three months.

Individuals can also 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.

SPT provides information to individuals as to exercising their rights under the GDPR on our website and intranet.

6. Data Protection by Design and Default

Under the legislation, SPT has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy. Data protection by design is about considering data protection and privacy issues upfront in everything we do.

An example of these measures include the use of data protection impact assessments where we undertake new or change activity.

7. Data Security

All users of personal data in SPT must ensure that personal data is always held securely and not disclosed to any unauthorised third party either accidentally, negligently or intentionally. The Digital Acceptable Use Procedures have more information about data security. However, this also applies to hard copy records both on and off site.

A data breach occurs if personal data is accidentally disclosed, lost or made unavailable. All data breaches and near misses should be reported under the Security Incident Reporting procedure.

Certain breaches require to be reported to the ICO within 72 hours so it is essential that breaches are reported immediately.

8. Procurement

Both data controllers and processors have legal obligations under the legislation. Where data is to be shared between two or more parties, specific contractual elements are required to outline the status and responsibilities of each party. These are known as Data Sharing Agreements or Data Processing Agreements.

During any procurement exercise, consideration will be given to the need for such agreements and advice should be sought from the Legal and Property team.

9. Marketing

SPT complies with PECR and any similar e-privacy legislation that may be in force at the time. We make people aware of the use of cookies on our website. Where we undertake marketing activity, we record and manage consent as required, and use privacy notices to explain how personal data is used.

10. Roles and Responsibilities

Assistant Chief Executive

The Assistant Chief Executive is SPT's appointed Data Protection Officer and has overall responsibility for Data Protection and for overseeing the development, maintenance and monitoring of SPT's arrangements for Data Protection.

Information Governance Officer

The Information Governance Officer (IGO) is responsible for developing, delivering and maintaining a comprehensive information management framework for SPT and acts as the principal contact for any data protection matters.

Directors/ Managers and Department Heads

Directors/ Managers and Department 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 legislation
- 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
- ensuring that breaches or near misses are reported and managed in line with the legislation and SPT's internal procedures

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 managed at all times. This requires continued compliance with SPT's information management and governance policies, procedures and other guidance.

11. Related Guidelines and Policies

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

Staff are encouraged to contact the IGO for information and support relating to the use of personal data and the content of this policy.

12. Training

The IGO 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.

13. Review

The policy and the associated procedures will be reviewed every three years by the Assistant Chief Executive.

Signature:_____ Print: _____

Date:_____ Designation: Assistant Chief Executive