**Trading Standards South West Data Protection Policy**

Author: Lisa Peters

Date: 29 May 2018

Version 1.1

1. **Our commitment**

Trading Standards South West (TSSW) Community Interest Company is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection.

TSSW are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation of the EU General Data Protection Regulations (GDPR) and the UK’s Data Protection Act. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

We aim to ensure that all employees, members, Directors and contractors who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under this legislation.

1. **Legitimate Interests**

TSSW needs to collect and use certain types of information about people with whom it deals in order to perform its functions and offer services, such as training to business and Local Authority partners. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material.

The purpose of this policy is to explain how TSSW will ensure compliance with the data protection legislation in the UK. It provides outline measures and puts in place a structure for monitoring compliance.

1. **Legal Context and Definitions**

|  |
| --- |
| **Key terms:**A **Data Subject** is an individual who is the subject of the data. A **Data Controller** is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed. A **Data processor** is any organisation or person (other than an employee of the data controller) who processes data on behalf of the data controller. **Processing** means obtaining, recording, viewing, holding or carrying out any operation on data and includes organisation, alteration, retrieval, disclosure and destruction of the data.  |

**General Data Protection Regulations (GDPR) 2018**

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

The GDPR places specific legal obligations on data processors; for example, a requirement to maintain records of personal data and processing activities. The data processor will have legal liability if they are responsible for a breach. The GDPR applies to processing carried out by organisations operating within the EU. The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

|  |
| --- |
| **What is personal data under GDPR?*** The GDPR applies to the processing of personal data that is:
* wholly or partly by automated means; or
* the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
* Personal data only includes information relating to natural persons who:
* can be identified or who are identifiable, directly from the information in question; or
* who can be indirectly identified from that information in combination with other information.
 |

The GDPR sets out seven key principles:

* Lawfulness, fairness and transparency
* Purpose limitation
* Data minimisation
* Accuracy
* Storage limitation
* Integrity and confidentiality (security)
* Accountability
* These principles should lie at the heart of your approach to processing personal data.
1. **Personal Data Held by TSSW**

This policy applies to all processing of personal data held by TSSW. This includes:

* Personal data processed by TSSW.
* Personal data controlled by TSSW, but processed by another organisation, on the TSSW’s behalf (for example private sector contractors).
* Personal data processed jointly by TSSW and its partner authorities (through projects, tasking and intelligence processes and through our specialist groups). We will only share data where we are legally permitted to do so, data that forms part of an legal investigation is exempt (as is monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention);

The policy does not cover personal data held by Local Authority members acting within a TSSW grant, which are data controllers in their own right.

Personal data held by TSSW may be held in many forms including:

* Database records
* Computer files
* Emails
* Paper files
* Film
* Sound recordings
* Photographs
* Website
* Mobile phones
1. **GDPR for TSSW**

We have a number of services we supply to consumers, businesses and local authorities, each hold data in distinctly different ways. The next few sections show what that data is for each service and what we have put in place to meet the legal requirements of the legislation.

**5.1 Definition of the data held in TSSW systems**

ELP manual - we have the users name and email, we store a data log, their IP address and where they visit within the site

TSSW.org.uk – we monitor hotspots on the site via IP addresses only, no personal data is stored beyond this.

BWBS.org.uk – we monitor hotspots on the site via IP addresses only, no personal data is stored beyond this.

NPOANS.org.uk – we hold training data on behalf of our subscribing business, we hold the business name, name of the main contact and their email, we hold the data they set up for their business including the bespoke element of the site and the staff details they set up.

Local authority eLearning for TSSW and NTS - we hold training data for our own training packages and on behalf of NTS. We hold the, name of the delegate, their email and their local authority.

TSSW Intranet – the dashboards hold a lot of data on who has posted content to the site or commented on a project / query or regional return, but it is private to TSSW and isn’t be shared outside of TSSW and members of specialist groups (some of which include occasional guests from Central Government agencies).

5.2 **Updates we have made to meet our “Legitimate interests”, as defined by GDPR**

ELP manual – we have updated our terms and conditions to access the resource to include GDPR.

TSSW.org.uk – we have put a new cookies policy in place.

BWBS.org.uk – we have put a new cookies policy in place.

NPOANS.org.uk – we have updated our privacy policy and our terms and conditions to reflect GDPR.

Local authority eLearning for TSSW and NTS – we have updated our privacy policy and our terms and conditions to reflect GDPR.

TSSW Intranet – we have added a privacy policy to the site.

1. **Access to data**

As detailed above we have amended terms and conditions to our services. Any subscriber to our services can request this data at any time and we have 30 days to comply. They can also ask for that data to be removed from the system.

1. **Privacy policies for TSSW**

Our privacy policies do vary slightly from service to service, accordingly to the role we play within that service, however each have been revised in order to comply with GDPR, ensuring that all individuals whose personal information we process have been informed of the following core information:

* Who is collecting and using your personal data
* Why are we collecting your personal data
* Who we will share your personal data with
* How long will we hold your personal data
* How we protect you data in the unlikely event of a data breach
* Who to contact if you have a request, enquiry or complaint
1. **Review process**

Annually TSSW will review the following:

* that what is stored is fair and lawful
* that what is stored is not excessive and that purpose limitations are considered
* data stored is kept at the minimum amount required to deliver the service
* accuracy and integrity of the data stored
* retention of data does not exceed the max. of 6 years)
1. **Security**

An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

All data breaches (however minor) should be reported to the Operations Manager for TSSW.

Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices.

Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data.

1. **Complaints procedure**

The first point of contact for data subjects should be via the specific service which holds their data.. Matters will be resolved at a local level as quickly and effectively as possible.

Subject access requests and data protection complaints should be addressed to the service administrator in the first instance.

|  |
| --- |
| We welcome comments and suggestions from readers. They will help us to improve this document in later editions. Please make them to lisa.peters@tssw.org.uk  |