Data protection policy

GENERAL DATA PROTECTION REGULATIONS 2018

Context and overview

Key details

- **Approved by directors on:** **24th May 2018**
- **Policy became operational on:** **24th May 2018**
- **Next review date:** **24th November 2018**

Introduction

Thames Valley Vulcanising Services (TVVS) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures the company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it store and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations including **TVVS** must collect, handle and store personal information.

The rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for data protection compliance wherever they are based (and not just their EU-based offices) as long as they are processing EU citizens' personal data.

The Data Protection Act 1998 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subject
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

6 Principles of GDPR:

The data protection principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a way 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.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of **TVVS**
- All branches of **TVVS**
- All staff and volunteers of **TVVS**
- All contractors, suppliers and other people working on behalf of **TVVS**

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Name of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Data protection risks

This policy helps protect **TVVS** from some very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately.

Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive areas.

Responsibilities

Everyone who works for or with **TVVS** has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Directors are ultimately responsible for ensuring that **TVVS** meets its legal obligations.
- The **Director, Keith Ward** is responsible for:

    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data **TVVS** holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Director, Terri Ward** is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The **Director, Lori Howe** is responsible for:

    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalist or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by the policy should be those who **need it for their work.**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **TVVS will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data protection officer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**

- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location,** away from general office spaces.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use

Personal data is of no value to **TVVS** unless the balance can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically.** The IT manager can explain how to send to authorised external contacts.
- Personal data should **never be transferred outside the European Economic Area.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of data.

Data accuracy

The law requires **TVVS** to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort **TVVS** should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional sets.

- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.

- **TVVS** will make it **easy for data subjects to update the information TVVS** holds about them. For instance, via the company website.

- Data should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subjects access requests

All individuals who are the subject of personal data held by **TVVS** are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at **Stacy Pollard**. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request (not employees). The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handling over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, **TVVS** will discuss requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Directors and from the company's legal advisors where necessary.

Providing information

TVVS aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

(This is available on request. A version of this statement is also available on the company's website.)

Consent

The GDPR sets a high standard for consent. **TVVS** will ensure that any consent given is clear, explicit, given freely and relevant:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

- Consent means offering individuals genuine choice and control.
- Explicit consent requires a very clear and specific statement of consent.
- **TVVS** will keep your consent requests separate from other terms and conditions.
- **TVVS** will make it easy for people to withdraw consent and tell them how.
- **TVVS** will keep evidence of consent – who, when, how, and what you told people.
- **TVVS** will keep consent under review, and refresh it if anything changes.

Name: Keith Ward
Position: Director
Date: 24/05/2018
Review date: 24th November 2018