Data Protection Policy (GDPR)

Introduction

Everyone has rights with regard to how their personal information is handled. During the course of the activities of **Thames Valley Vulcanising Services (TVVS- 'The Company')** we will collect, store and process personal information about our staff, customers, and suppliers, and we recognise the need to treat all data in an appropriate and lawful manner.

The types of information that TVVS may be required to handle include details of current, past, and prospective employees, contractors, agency workers, customers, suppliers, partners, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and other relevant regulations. The Act which makes allowances for GDPR imposes restrictions on how we may use that information.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

Status of the policy

This policy sets out TVVS's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation, and destruction of personal information.

The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer, Terri Ward.

If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with your line manager or Company Director.

Definition of data protection terms

Data is information, which is stored electronically, for example on a computer or in certain paper-based filing systems as well as written notes and files.

Data Subjects for the purpose of this policy include all individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data means data relating to an individual who can be identified from that data or from that data and other information in our possession. Personal data can be factual such as a name, address or date of birth or it can be an opinion such as a performance appraisal.
Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

Data Users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data Processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.

Sensitive Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data protection principles.

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant, and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

Fair and lawful processing

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, who the data controller's representative is (in this case the Data Protection Officer), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for limited purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant, and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely processing

Personal data will not be kept longer than is necessary its intended purpose. This means that data should be destroyed or erased from TVVS's systems when it is no longer required.

Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security

TVVS will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.
The Act requires TVVS to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity, and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

Entry controls. Any stranger seen in entry-controlled areas should be reported.

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind such as personal information is always considered confidential.

Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Password protection. Data should be protected by strong passwords that are changed regularly, and never shared between employees.

Approved storage. Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.

Servers. Servers containing personal data should be sited in a secure location, away from general office spaces.

Backing up. Data should be backed up frequently and tested regularly.
Firewalls. All services and computers containing data should be protected by approved security software and a firewall.

Dealing with subject access requests

A formal request from a data subject for information that we hold about them must be made in writing to the Data Protection Officer (Terri Ward). A fee is not normally payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their line manager immediately, and is 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**

Requests will normally be handled within one month of the written request being made, but depending upon the complexity, reasonable additional time may be required.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Company. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked, and
- Refer to their line manager for assistance in difficult situations. No-one should be bullied into disclosing personal information

Data Archiving, Weeding and Deletion

The current rules under GDPR stipulate no personal data should be held for longer that it is needed and adopted under the Data Protection Act 2018. The ICO has given an indicative standard for the deletion of sensitive data after 6 years and any other data after 2 years. The exceptions being data needed to fulfil a contract or obligation or which its retention is a legal requirement or in the best interests of the subject. Standard terms and conditions for TVVS provide legal justification for the possible retention of operational data for 7 years upon becoming historic as an operational safeguard against wrongful deletion.

The Right to be Forgotten

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten.' All employees, contractors, agency workers, suppliers, and clients, can make a request for erasure verbally or in writing. TVVS have one month to respond to a request. The right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for.
- we are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent.
- we are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.
- we are processing the personal data for direct marketing purposes and the individual objects to that processing.
- we have processed the personal data unlawfully (i.e., in breach of the lawfulness requirement of the first principle).
- we must do it to comply with a legal obligation.

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, Terri 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, Terri Ward** 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 Employee 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.

Please note that the policies may change from time to time and the most recent version will be available in the main office.