1 Privacy Policy

2 Purpose

To define how the Organisation controls the sensitive information processed or controlled in regard to or on behalf of our staff, customers, visitors and suppliers.

3 Scope

This policy is intended to cover all systems and areas of the business where sensitive information is processed or stored and all users of those systems containing personal information.

4 Introduction

The Organisation acknowledges that controlling the confidentiality, integrity and availability of information is key to Data Privacy. The formal controls that both a ISO27001 and Cyber Essentials Plus certified system provides ensure that the foundations for Data Privacy are in place.

The Data Protection Act reforms of 2018 requires further focus of our management system controls into the area of Personally Identifiable information to ensure that adequate controls are in place to protect such information. This also provides assurance to all interested parties that such controls are in place and controlled as required by UK Law.

5 Personal Information collection

Personal Information is any information that can be used to identify, locate or contact a living individual. The Personal Information that is collected by the Organisation is done so with data minimisation in mind and is only conducted after determining the purpose for which the information is to be used. The collected information is only used for the purpose intended and should further processing of any kind be desired the data subject will always be consulted and given the option to opt in. Consent to hold and process personal information is always obtained and a legal basis for holding this information is always understood.

5.1 Where we collect Personal information

As a business we collect personal information from a number of sources.

- Information on the Organisations employees/contractors/agency staff (including personal sensitive information) for the basis of employment.
- Prospective candidate information who engage with the organisation with the intention of employment (including personal sensitive information).
- Personal information from our customers/contractors often including email, phone and address details and in some instances these details are both corporate and personal.
- Prospect information from potential customers including business card style personal information.

- Visitors to our websites who place orders with us or have registered interest in a product or service we offer for the purpose of conducting business.
- Visitors/contractors who attend our sites.

6 Purpose for processing Personal Data

In all instances the data subject is providing the Organisation with information for a clear and explained reason. In all cases the processing of personal data is either conducted under consent, is a requirement to fulfil a contract into which both parties have agreed, there is a legal obligation or vital interest to process it or we have identified a legitimate interest.

The organisation is responsible for maintaining a register of those permissions; this register is defined within SMS038 Information Asset Register within Privacy Impact Assessments. For members of TVS SCS a separate register called SMS068 TVS Staff Privacy Matrix has been provided to all staff detail how personal data is processed and controlled by the company.

7 Security of Personal Information

The Organisation takes all practicable measures to protect the Personal Information it holds in an effort to prevent loss, misuse and unauthorised access, disclosure, alteration and destruction in line with UK Data Protection Laws. TVS Supply Chain Solutions Limited is registered with the information Commissioners Office (ICO) under registration number Z6021849.

The Organisation has adopted the rigorous physical and logical security controls required to become certified to ISO27001 and Cyber Essentials Plus in locations where data is stored and processed.

All Information is categorised dependent upon its classification in line with formal Information Classification Policy SMS-00014. Assets are also formally controlled within Information Asset Registers SMS-00038.

Access to the corporate network is controlled via Access Control Policy SMS-00004 and network monitoring and alerting is controlled via Network Monitoring policy SMS-00021. All changes to our network are controlled via a change control process outlined within Change Management Policy SMS-0007.

All information will be held within the European Economic Area, this includes all off site backups.

8 Staff

All members of staff employed by the Organisation are required to sign confidentiality agreements and a security code of conduct as part of the recruitment process. Training on Data Protection and information security principles are provided at induction and are backed up with regular communications and refresher training thereafter. Staff working in increased risk areas including those where large amounts of personal information are stored, face additional formal background checks and tailored security training so that adequate protection is provided.

9 Third parties

Any third party that the Organisation requires Personal Information to be shared with will only be undertaken under contract where Data Privacy rules have been agreed and formalised. Where risk levels are deemed to be high the Organisation may require increased security levels of its systems. Where applicable independent certification to recognised standards such as Cyber Essentials, Cyber Essentials Plus and ISO27001 or have the ability to demonstrate a proportionate level of control may be required before information is shared between parties.

10 Information choices and changes

The Compliance Manager has been appointed lead for all Data Protection queries entering the business by the Operational Board as this role also captures Information Security and Compliance to certified security standards. This role is also separate to any business channels obtaining Personal Information so that an unbiased opinion can review and mange any submission or complaints.

The Organisation has made it simple to contact the Compliance Manager either in writing to the head office address or via a dedicated mailbox displayed on communications and on websites: dataprotectionmanager@tvsscs.com.

11 Subject access requests

All data subjects have a right to request a copy of the information the Organisation holds about them without charge. The Organisation will endeavour to provide this information within 30 calendar day. Data subjects can request this by simply contacting the Organisation.

12 Destruction/Disposal of Personal Information

Data is kept controlled within Information Asset Registers with retention periods outlined for the control of this retention period. Data is only held for the prescribed amount of time which has been agreed due to business need. Regular internal audit of the Information Asset Registers ensures that no information is kept beyond the agreed retention period and that all information is kept up to date.

13 Incidents involving Personal Information

The Organisation takes all practicable steps to secure and protect the confidentiality, integrity and availability of all personal information. Should a data breach incident occur where Personal Information was suspected or confirmed as occurring the Organisation would report the incident to the ICO within 72 hours and where applicable inform the data subject without undue delay.

The Organisation has a formal, exercised Incident Response plan SMS-00013 that covers incidents such as those involving personal information. Any report of a suspected Data Breach would invoke the incident response plan, meaning a preselected team with authority would convene to manage the incident at hand.

The Organisation has put in place adequate insurance cover to protect against liabilities arising from any data breach incident.

14 Correcting Personal Information

If a data subject believes that any Personal Information the Organisation holds is incorrect or incomplete at any point then the subject should contact the Organisation without delay. The Organisation will then endeavour to correct any information promptly.

15 Contacting the Organisation

All Subject access requests should be made in writing to the Compliance Manager using the email address:

dataprotectionmanager@tvsscs.com

Alternatively in writing to:

TVS Supply Chain Solutions Ltd
Logistics House
Buckshaw Avenue
Chorley
Lancashire
PR6 7AJ

Issue History

Issue	Date	Changes	Changed by:
2	05/11/2018	Added link to SMS068 for TVS staff in section 6 to detail how personal information is used by the organisation. Updated format.	Kevin Johnson/Lyndsay Chapman.
3	24/08/2020	Update to section 5.1 to clearly define prospect information. Update to corporate logo	Kevin Johnson.