TOUCHSTONE DATA PROTECTION POLICY

Date of issue	October 2023
Replacing/Updating	Previous version
Review Date	October 2023
Drafted by	Data Protection Compliance Manager
Responsible Director	Data Protection Compliance Manager
Circulation List	Available electronically here and on The PfP Group Intranet and SharePoint. Policy is also available to all Clients, Customers and third party Data Processors

CONTENTS

1. POLICY SCOPE AND BACKGROUND

1.1 SCOPE

This Data Protection Policy sets out Touchstone's commitment and approach to data protection. The policy's objectives are:

- To provide a clear frame of reference for those who handle personal data to determine Touchstone's standards, aims, and ideals in respect of data protection compliance;
- To provide information to data subjects, data processors and the regulatory authorities about how Touchstone approaches data protection compliance;

1.2 BACKGROUND

This Policy is designed to accommodate the Data Protection Act 2018 together with all applicable laws and regulations from time to time in force relating to data protection, privacy and the processing of personal data, including the UK GDPR and the Privacy and Electronic Communications Regulations 2003 as amended, and the Freedom of Information Act (2000). These laws are collectively referred to in this Policy as Data Protection Legislation. Additionally various guidelines, codes or practice, case law and other information relating to data protection must be considered by Touchstone.

The Data Protection Legislation sets out legal responsibilities on Touchstone processing personal data and provides for rights in the law for those people whose data are being processed. This Policy is a public statement describing Touchstone's approach to complying with its legal responsibilities in the Data Protection Legislation and how it enables individuals' rights to be upheld and exercised.

Penalties can be imposed on processing personal data including fines of up to £17,000,000 or 4% of prior year global annual turnover whichever is the greater. There are a number of criminal offences set out in the Data Protection Legislation and individuals can be held accountable and be sentenced by the courts for offences under the Legislation.

Related and connected laws:

- The Data Protection Bill UK
- The General Data Protection Regulations 2018
- The UK General Data Protection Regulations 2018 (the retained EU law version of the European General Data Protection Regulation, namely Regulation (EU) 2016/679, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018)
- The Common Law Duty of Confidentiality
- The Freedom of Information Act 2000

- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- Human Rights Act 1998
- Investigatory Powers Act 2016

2. POLICY STATEMENT

The Touchstone Executive team are committed to compliance with all relevant Data Protection Legislation and will formally delegate appropriate powers and responsibilities to its staff to ensure that it is fully able to comply with the Data Protection Legislation and its own defined standards in the field of data protection and information governance.

The Executive Team will ensure that all relevant staff have received appropriate and sufficient training in the application of the company's policies and will make policies and procedures available to other persons it commissions to process personal data on its behalf, either directly or indirectly.

The Executive Team will ensure that sufficient and appropriate resources are available to ensure that it meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

The Executive Team will ensure that Touchstone works within the 6 data protection principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and decisions relating to data processing activities.

Touchstone will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights.

This policy applies to all of Touchstone's activities or operations which involve the processing of personal data.

This policy has been approved by Touchstone CPS Ltd Board of Directors. It sets out our 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 Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by **Jon Clark**, Director, 01225 838425 ext. 2025, jon.clark@touchstoneresi.co.uk Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Manager.

Touchstone is registered to handle data by the Information Commissioner under registration number Z7881658.

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 the Data Protection Compliance Manager.

3. RESPONSIBILITIES

3.1 Data Controllers

Touchstone are registered as Data Controllers or Data Processors and maintain Records of Processing Activities in line with the requirements of the Accountability principles of the UK GDPR and Data Protection Legislation.

All Records of Processing Activities are available for inspection by the Information Commissioners Office.

3.2 Management and supervisory staff

Protecting data and thus maintaining confidentiality is pivotal to Touchstone being able to operate.

The Data Protection Compliance Manager is the accountable officer responsible for the management of Touchstone's activities and ensuring appropriate mechanisms are in place to support service delivery and continuity.

Each Director, in their respective areas of responsibility, must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Director must ensure this policy is adhered to.

Managers and supervisory staff are responsible for ensuring that all data processing operations under their control or domain of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

3.3 Employees, volunteers, casual/temporary workers, directors and officers

Anyone who is directly engaged by Touchstone to undertake data processing activities including but not limited to employees, volunteers, casual/temporary workers, directors and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact the Data Protection Compliance Manager. Individuals are expected to complete appropriate training from time to time. Everyone within Touchstone has a duty to respect data subjects' rights to confidentiality and a private life.

Disciplinary action may be imposed on staff for non-compliance with the relevant policies and procedures.

3.4 Partner & Third-Party Responsibilities

Any partner or third party of Touchstone that is commissioned to process data or receives data from the Touchstone, or is able to access any personal data **must** complete an Information Sharing Protocol with Touchstone or have appropriate contractual documentation that confirms both parties commitment to compliance with the UK GDPR and which will be determined by the level of involvement with the data that is held/shared/accessed. Any high-risk data processing activities must be approved by the Data Compliance Manager.

4. DATA PROTECTION PRINCIPLES

Article 5 of the UK GPDR requires that all processing of personal data must comply with the 6 enforceable principles of good practice, as set out below. These provide that processing of personal data must be:

1. Lawfulness, fairness and transparency	Processed lawfully, fairly and in a transparent manner
2. Purpose limitation	Collected for specified, express and legitimate purposes and not processed in a manner that is incompatible with those purposes.
3. Data minimisation	Relevant and limited to what is necessary in relation to the purpose for which they are processed.
4. Data quality	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Data retention	Kept for no longer than is necessary for the purposes for which they are processed.
6. Data security	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, damage, using appropriate technical or organisational measures.

5. LAWFUL BASES TO PROCESS PERSONAL DATA

5.1 The Act is intended not 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 (in this case Touchstone CPS Ltd, who the data controller's representative is (in this case the DPCM), 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.

5.2 For personal data to be processed lawfully, certain conditions have to 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.

1. Consent	The Data Subject has given consent to process their personal data for one or more specific purposes.
2. Contract	Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps, at the request of the Data Subject, prior to entering into a contract.
3. Legal obligation	Processing is necessary for compliance with a legal obligation to which Touchstone is subject.
4 Vital interests	Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
5. Public interests of official authority	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Touchstone.
6. Legitimate interest	Processing is necessary for the purposes of the legitimate interests pursued by Touchstone or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

6. PROCESSING FOR LIMITED PURPOSES

6.1 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.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 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.

8. ACCURACY OF DATA

8.1 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.

9. TIMELY PROCESSING

9.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Data Protection Compliance Manager.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

10.1 Articles' 15-22 of the UK GDPR give Data Subjects the following rights over their personal data:

1. Informed	The right to be informed about the collection and use of their personal data.
2. Access	The right to obtain confirmation that Touchstone holds their personal data, to access copies of their personal data and to obtain a copy of Touchstone's privacy policy.
3. Rectification	The right to obtain from Touchstone rectification of inaccurate personal data or completion of incomplete personal data.
4. Erasure	The right to obtain from Touchstone the erasure of their personal data.
5 Restriction	The right to request the restriction or suppression of how Touchstone uses their personal data.
6. Data portability	The right to obtain a copy of their personal data in a machine-readable format.
7. Objection	The right to object to the processing of their personal data.
8. Automated decision making and profiling	The right to not be subject to a decision based **solely** on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the Data Subject.

11. INFORMATION SECURITY

Touchstone will ensure that any personal data that it processes or commissions the processing of is processed in a manner 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. In particular an Information Security Policy will be maintained setting out specific policies in relation to maintaining personal data secure, confidential, available and with integrity.

12. DATA BREACHES

12.1 A breach occurs where personal data within its control is:

- Accidental or unlawful destroyed
- Lost
- Accidentally altered
- Disclosed without authorisation
- Exposed without authorisation

12.2 All data breaches must be immediately reported **BOTH** to the DPCM by e-mail (jon.clark@touchstoneresi.co.uk) and copied to data.protection@touchstoneresi.co.uk and to the relevant departmental director with responsibility for the property or customers in question to ensure a written record. The breach or potential breaches must also be reported to Places for People's breach recording portal at https://dataprotection.pfpshare.co.uk/breach/Lists/Breach/NewForm.aspx. The DPCM will undertake an initial assessment and, where Touchstone is the Data Processor, immediately inform the Data Controller.

Where Touchstone is the Data Controller, a decision will be made as to whether the breach requires notification to the ICO, which if applicable will be notified within 72 hours.

Where Touchstone is the Data Processor, all incidents must be reported to the Data Controller within 48 hours.

12.3 If the initial or any subsequent assessment identifies that a the breach exposes data subjects to a high risk of identity theft, fraud, financial loss, damage to the data subject's reputation, loss of confidentiality, unauthorised reversal of pseudonymisation, discrimination or other significant economic or social disadvantages Touchstone will implement a communication strategy to notify the affected data subjects of the specific details of the breach.

12.4 If Touchstone believes there to be a high risk of identity theft, fraud or financial loss as a result of a breach, they will notify the police, its insurers and bank and credit card companies as deemed appropriate.

12.5 Touchstone will maintain a register of all breaches and any associated notifications to Data Controllers or the ICO.

13. DEALING WITH SUBJECT ACCESS REQUESTS

13.1 A formal request from a data subject for information that we hold about them must be made in writing. A fee is no longer payable unless there are exception circumstances, and only on authorisation of the DPCM. Any member of staff who receives a written request should forward it to their line manager **OR** the DPCM immediately.

14. DEALING WITH RIGHT TO ERASURE REQUESTS

14.1 A formal right to erasure request from a Data Subject must be made in writing and passed to the DPCM on receipt. Any requests will be considered against the guidelines set out in the UK GDPR and will action the request within 1 month of the request.

14.2 The Data Subject's right to erasure applies where:

- The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The Data Subject withdraws consent for Touchstone to process their personal information if the processing is based on consent;
- The Data Subject objects to Touchstone processing their personal data;
- The personal data has been processed unlawfully; or
- The personal data has to be erased for compliance with a legal obligation to which Touchstone is subject.

14.3 The Data Subject's right to erasure does not apply where the processing is necessary:

- For exercising the right to freedom of expression and information;
- For compliance with a legal obligation which requires processing;
- For the performance of a task carried out in the public interest or in the exercise of official authority vested in Touchstone;
- For public health reasons;
- For archiving purposes in the public interest, scientific or historical research or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

15. PROVIDING INFORMATION OVER THE TELEPHONE

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

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) 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.

(c) Refer to their line manager **OR** the DPCM for assistance in difficult situations. No-one should be bullied into disclosing personal information.

16. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

16.1 Touchstone will complete a DPIA for any new work undertaken or where a change to existing processes results in a change in personal data processing or an increase in the processing of data by a sub-processor.

16.2 Touchstone will maintain a register of all DPIA undertaken.

17. INTERNATIONALISATION OF PERSONAL DATA

Touchstone will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that Touchstone undertakes or commissions whether directly

or indirectly must be approved by the DPCM and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has an adequacy decision issued by the European Commission;
- The transfer is to the United States of America and the recipient is registered under the EU/US Privacy Shield scheme;
- The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

18. RISK ASSESSMENT

Touchstone will embrace the principles and foster a culture of privacy by design and by default. It will maintain a policy requiring data protection impact assessments (DPIA) to be undertaken and documented and ensure that appropriate resources are available to advise on DPIAs.

19. TRAINING AND AWARENESS

Touchstone will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided annually.

20. AUDIT AND COMPLIANCE CHECKING

Touchstone will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where non-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits.

21. MONITORING AND REVIEW OF THE POLICY

21.1 This policy is reviewed annually by the Executive Team. Recommendations for any amendments are reported to the DPCM or the Directors.

21.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

21.3 We also maintain a Privacy Policy for the benefit of our customers and which sets out the obligations we have towards them and how we deal any information provided which is covered by the Act.

GLOSSARY

22. DEFINITION OF DATA PROTECTION TERMS

22.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

22.2 **Data subjects** for the purpose of this policy include all living 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.

22.3 **Personal data** means data relating to a living 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).

22.4 **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. We are the Data Controller of all personal data used in our relation to running our business (see comments under Data Processors below for management activities). **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.

22.5 **Data processors** include any person who processes personal data on behalf of a data controller. We are the Data Processor where we are undertaking business activities as services for other parties, for example landlords who appoint us to provide management services. Data processors could also be suppliers who provide services to us and who handle personal data on our behalf of our corporate activities.

22.6 **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.

22.7 **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.

22.8 **Sub-processors** are those persons who process personal data on behalf of a Data Processor, for example contractors, solicitors and other service providers with whom we share personal data.

22.9 **Data protection compliance manager (DPCM)** is the person appointed by Touchstone to ensure that all associated policies and procedures are fit for purpose, compliant with legislation and updated as required by changes to legislation and/or best practice, for ensuring all colleagues of Touchstone receive appropriate training and that this policy is reviewed on an at least annual basis.