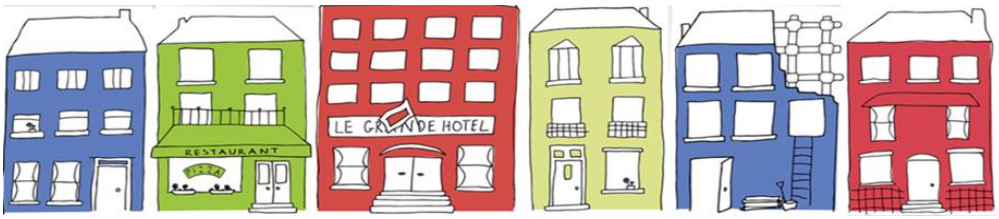
TOUCHSTONE
CORPORATE LIMITED



Data Protection Policy

1. Policy Scope and Objectives

1.1 Touchstone Corporate Limited needs to gather and process certain information about individuals.

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

1.2 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.

2. Why this policy exists

2.1 This data protection policy ensures Touchstone Corporate Limited

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

3. Data protection law

3.1 The General Data Protection Regulation (GDPR) prescribes how organisations — including Touchstone Corporate Limited — must collect, handle, store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

3.2 The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and

- free of charge

3.3 Article 5 of the GDPR requires that personal data shall be;

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 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.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4. People, risks and responsibilities

4.1 Policy scope

This policy applies to:

- The offices in Hove of Touchstone Corporate Limited
- All staff including self-employed advisors both based at Hove and external advisors.
- Anyone working on behalf of Touchstone Corporate Limited

4.2 It applies to all data that the company holds relating to individuals. This can include:

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

5. Data protection risks

5.1 This policy helps to protect Touchstone Corporate Limited 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 data.

6. Responsibilities

6.1 Everyone who works for or with Touchstone Corporate Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Touchstone Corporate Limited will provide each customer with a privacy notice as upon receipt of individual data or within a month if the data has been provided from a third party.

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

6.2 However, these people have key areas of responsibility:

- The Principles of the Firm, Phil Moore and David Warnes, are ultimately responsible for ensuring that Touchstone Corporate Limited meets its legal obligations.
- Handling data protection questions from staff and anyone else covered by this policy.
- Approving any contracts or agreements with third parties that may handle the company's sensitive data.

The Data Protection and Compliance Officer is responsible for:

- 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.
- Dealing with requests from individuals to see the data Touchstone Corporate Limited holds about them (also called 'subject access requests').
- Checking any contracts or agreements with third parties that may handle the company's sensitive data.

6.3 The Compliance Officer 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.
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

7. General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**.
- Touchstone Corporate Limited **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.
- 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.
- 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**.
- Personal data should **never be transferred** outside of the European Economic Area unless the non-member state has comparable safeguards to the GDPR.
- Employees **should not save copies** of personal data to their own computers. Always access and update the central copy of any data.

8. Data storage

8.1 These rules describe how and where data should be safely stored.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see or have access to it.

8.2 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**.

8.3 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.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- 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.

9. Data use

9.1 Personal data is of no value to Touchstone Corporate Limited unless the business 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, theft or misuse.

Touchstone Commercial Limited will identify the lawful basis for processing personal data before it can be processed; this will include documenting the lawful reasons for processing data.

Some of the reasoning for processing data could be, but not limited to;

- Consent of the data Subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

9.2 The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Data will be provided in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, Touchstone Corporate limited may be required to transmit the data directly to another organisation if this is technically feasible. If the personal data concerns more than one individual, Touchstone Corporate Limited must consider whether providing the information would prejudice the rights of any other individual.

Touchstone Commercial Limited will respond to these requests within one month or two months if the request is complex.

9.3 Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation".

Touchstone Corporate Limited must stop processing the personal data unless:

- can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

Touchstone Corporate Limited must inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Touchstone Corporate limited must stop processing personal data for direct marketing purposes as soon as an objection is received. There are no exemptions or grounds to refuse.

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

10. Lawful Processing

For Processing to be lawful under the GDPR Touchstone Corporate Limited must establish and identify the lawful basis before processing of personal data can commence.

Processing of personal data is necessary for compliance with a performance of a contract with the data subject. In order for Touchstone Corporate Limited to provide any of it services as a Commercial and Regulated Mortgage Broker to our customers, personal data must be processed.

A Privacy statement is provided to customers which captures explicit consent to process customer data. Without this Touchstone Commercial Limited cannot process any data provided.

Special categories of data may be required for the performance of a contact with the data subject, explicit consent from the data subject will be gathered unless reliance on consent is prohibited by EU or Member State Law.

11. Data accuracy

11.1 Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

11.2 If personal data has been disclosed to third parties, Touchstone Corporate Limited will inform them of the rectification where possible. Touchstone Corporate Limited will inform the individuals about the third parties to whom the data has been disclosed where appropriate.

11.3 Where a request for recertification to data has been revived, Touchstone Corporate Limited will respond within one month or two months where this is complex.

11.4 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

11.5 Touchstone Corporate Limited is required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, until verification of the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and are considering whether the organisation's legitimate grounds override those of the individual.
- When processing is unlawful, and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

12. Subject access requests (SAR)

12.1 All individuals who are the subject of personal data held by Touchstone Corporate Limited are entitled to:

- Obtain **confirmation** that their data is being processed;
- **Access** to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be **provided in a privacy notice.**

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

12.3 SAR's from individuals should be made by email, addressed to the data controller at smoore@touchstonecommercial.co.uk The data controller can supply a standard request form, although individuals do not have to use this.

12.4 The SAR will be provided **free of charge**. If the request is manifestly unfounded, excessive or repetitive, then Touchstone Corporate Limited will charge a reasonable fee for this. The fee will be based on the administrative cost of providing the information. The data controller will aim to provide the relevant data within **one month of receipt**.

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

12.5 If the request for a SAR is made electronically, Touchstone Corporate Limited will provide the information in a commonly used electronic format.

13. Disclosing data for other reasons

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

13.2 Under these circumstances, Touchstone Corporate Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

14. Breach Notification

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Touchstone Corporate Limited will notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What our breach notification must contain;

- The nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Touchstone Corporate Limited will report a notifiable breach to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The breach will be fully investigated, and information provided in phases.

Touchstone Corporate Limited will ensure all staff are trained and understand the requirements of this document. If a breach is identified, the Directors are responsible for;

- Logging the breach
- Investigating the extent of the breach
- Placing measures and testing controls to mitigate future events

15. Complaints

If you are unhappy with the outcome of any of your requests to exercise your rights, or how we handle your personal data then please let us know. You are also entitled to complain to the Information Commissioner's Office: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Email: Casework@ico.org.uk Tel: 0303 123 1113