Technische und organisatorische Maßnahmen (TOM) gem. Art. 32 DSGVO der Stein & Stein Versicherungsmakler GmbH

1. Vertraulichkeit

a. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Es erfolgt eine ständige Zutrittskontrolle für die Büroräume durch die im Empfang sitzenden Kollegen. Für alle anderen Räumlichkeiten erfolgt eine Zutrittskontrolle durch die im Trakt sitzenden Kollegen.
- Unbefugten und insbesondere betriebsfremden Personen ist der Zugang grundsätzlich verwehrt; er kann erst nach ausdrücklicher Freigabe durch einen Mitarbeiter unter Benennung des Anlasses ermöglicht werden.
- Es existieren sowohl Sicherheitsschlösser wie auch eine Schlüsselregelung und eine Alarmanlage.
- Serverschrank ist verschlossen und im abgeschlossenen Raum untergebracht.
- Datensicherungen auf portable Sicherungsmedien (z.B. CD/DVD, Bänder) sind in zutrittsgeschützten Räumen untergebracht.

b. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Der Zugang zur technischen Arbeitsumgebung ist durch ein bündiges Zylinderschloss geschützt.
- Nicht mehr benötigte Zugangsberechtigungen werden zeitnah entzogen.
- Der Arbeitsplatzrechner wird nach einer vorgegebenen Zeitdauer der Inaktivität gesperrt.
- Es werden Logs der Benutzeranmeldungen erstellt.
- Die Arbeitsplatzrechner sind durch Anti-Viren-Software geschützt.
- Das Reinigungspersonal wird sorgfältig ausgesucht.
- Besucher und Handwerker dürfen sich nicht alleine in den Büroräumen aufhalten.

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Es sind ausschließlich Personen, die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Auftragsverarbeitung betraut sind, berechtigt, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen. In diesem Zusammenhang bestehen klare Regelungen zur Vergabe von Zugriffsberechtigungen, die einen differenzierten Zugriff (lesen, ändern, löschen) berücksichtigen und den Zugriff auf den verschiedenen Ebenen regeln.
- Für eventuelle Fernadministration sind Sicherheitsregeln in Kraft.
- Es existieren folgende technische Sicherheitseinrichtungen zum Schutz gegen einen Zugriff aus nicht vertrauenswürdigen Netzwerken (z.B. Internet):
  - Firewall
  - IPS
  - SSL
- Die technischen Sicherheitseinrichtungen werden regelmäßig auf ihre Wirksamkeit hin geprüft.
- Unsere Mails werden über TLS verschlüsselt. Dies geschieht über unseren Anbieter IS FUN Vom Homeoffice wird über VPN-Tunnel zugegriffen, um verschlüsselte Übertragungswege zu nutzen. Es greift die SSL-Verschlüsselung.

2. Integrität

a. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Die Verwendung von externen Datenträgern (USB-Stick, externe Festplatte, CDs, DVDs) außerhalb der geschützten Unternehmensumgebung ist verboten.
- Die datenschutzgerechte Datenvernichtung ist gewährleistet. Bei Papierdokumenten erfolgt sie durch einen Papierreißwolf. Bei Datenträgern (z.B. defekte Festplatte) erfolgt sie physikalisch.
- Bei Weitergabe von Daten per Telefax ist der Einzelfaxnachweis und das Journal zu archivieren.
- Bei Weitergabe von Daten in Onlineformulare - z. B. Onlinebeantragung - ist zu beachten dass es sich um eine verschlüsselte Anwendung (https://..) handelt. Die Eingabebestätigung ist zu archivieren.
- Die Weitergabe per Email erfolgt verschlüsselt, da wir über unseren Anbieter TLS-Verschlüsselung nutzen.

b. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Um zu gewähren, dass im Nachhinein geprüft werden kann, ob, von wem und wann personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, erfolgt eine entsprechende Protokollierung.
- Administrationstätigkeiten werden ebenfalls protokolliert.

3. Verfügbarkeit und Belastbarkeit

a. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Die Daten sind gegen zufällige Zerstörung oder Verlust geschützt. Sämtliche personenbezogene Daten, insb. Datenhaltung vom Maklerverwaltungsprogramm, sowie Emaildateien sind auf dem Server abzulegen. Auf den Arbeitsplätzen dürfen personenbezogene Daten nicht gespeichert werden. Die Daten des Servers sind täglich zu sichern.
- Mindestens einmal wöchentlich ist eine Sicherung außer Haus durch eine besonders zuverlässige Person (Geschäftsführer, Prokurist, Datenschutzbeauftragten) zu verbringen.
- Es gibt ein Backup- und Recoverykonzept.
- Die Backups werden regelmäßig daraufhin getestet, ob ein reibungsloses Zurücksichern möglich ist.

b. Unverzügliche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall unverzüglich wiederhergestellt werden können.

- Es existiert ein Konzept für die Wiederherstellung des Geschäftsbetriebs nach einem Notfall.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a. Datenschutz-Management

- Es ist ein Datenschutz- und Sicherheitskonzept vorhanden, das regelmäßig überprüft wird.
- Das Datenschutz- und Sicherheitskonzept wird an sich ändernde Bedingungen angepasst.

b. Incident Response-Management

- Es gibt eine Prozessbeschreibung zur Behandlung von Datenpannen.
- Die Mitarbeiter sind über den Ablauf der Behandlung von Datenpannen informiert.

c. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Alle Mitarbeiter sind auf die Grundsätze der Vertraulichkeit eingewiesen worden. Die Unterweisung wird jährlich wiederholt.
- Mit jedem Dienstleister, der in unserem Auftrag personenbezogene Daten verarbeitet oder in Zusammenhang mit seiner Tätigkeit Einblick und Zugriff auf personenbezogene Daten haben könnte, wird ein Vertrag zur Auftragsverarbeitung mit eindeutiger Leistungsbeschreibung geschlossen.
- Für die vereinbarte Auftragsverarbeitung werden ggf. Cloud-Lösungen eingesetzt. Die genutzten Rechenzentren befinden sich in der EU. Die Cloud-Datenkommunikation ist verschlüsselt.