Vertrag Nr. Vertragsnummer vom Datum

Zwischen der

TrustStone Software GmbH

Am Sandtorkai 68

20457 Hamburg

im Folgenden „TrustStone Software“ genannt

und

Kanzlei

Kanzleizusatz

Strasse Nr

PLZ ORT

nachfolgend „Kanzlei“ genannt,

wird hiermit ein Vertrag über die Nutzung von Leistungen der TrustStone Software geschlossen.

§1 Gegenstand des Auftrags

TrustStone Software stellt der Kanzlei die Nutzung der Online-Plattform „kanzlei.land“ zu den unter §2 genannten Konditionen zur Verfügung. Das kanzlei.land ist eine webbasierte Online-Plattform für den einfachen und sicheren Austausch und die Aufbereitung von Daten und Belegen zwischen der Kanzlei und den Mandanten der Kanzlei.

§2 Konditionen

Es gelten die Konditionen gemäß der **„Anlage 1 zum Vertrag Nummer Vertragsnummer: Konditionen kanzlei.land“**. Alle Preise sind netto und verstehen sich zuzüglich der jeweils gültigen Umsatzsteuer.

§3 Leistungsumfang

- Online-Plattform „kanzlei.land“ mit allen Standardleistungen
- Ersteinrichtung gemäß der **„Anlage 3 zum Vertrag Nummer Vertragsnummer: Ersteinrichtung kanzlei.land“**

Die nachfolgend aufgeführten Anlagen sind verbindlicher Bestandteil dieses Vertrages:

- **Anlage 1** zum Vertrag Nummer Vertragsnummer: Konditionen kanzlei.land
- **Anlage 2** zum Vertrag Nummer Vertragsnummer: Datenschutzrechtliche Vereinbarung (nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)
- **Anlage 3** zum Vertrag Nummer Vertragsnummer: Ersteinrichtung kanzlei.land
- **Anlage 4** zum Vertrag Nummer Vertragsnummer: SEPA-Lastschriftmandat
- **Anlage 5** zum Vertrag Nummer Vertragsnummer: Allgemeine Geschäftsbedingungen der TrustStone Software GmbH

Wir haben diese zur Kenntnis genommen und sind damit ausdrücklich einverstanden.

X

Ort, Datum, Kanzlei (Unterschrift Vertretungsberechtigter)

(Auftraggeber)

Hamburg, den Datum Philip Hellmig

Ort, Datum, TrustStone Software GmbH

(Auftragsverarbeiter)

Anlage 1 zum Vertrag Nummer Vertragsnummer:

Konditionen kanzlei.land

1. Kosten für die Einrichtung

Einrichtung Grundsystem Whitelabel (Logo, Farbe, Subdomain)

2. Kosten für die Kanzleinutzung

Server (inklusive 100 GB Speicherplatz und 1 Mitarbeiterzugang)
jeder weitere Mitarbeiterzugang
jede weiteren 100 GB

3. Kosten für die Mandantennutzung

Mandanten Grundzugang („Digitaler Schuhkarton“)
Für betriebliche Mandate
Für private Mandate (Einkommensteuer)

4. Erweiterungen

Hinweis: Die Erweiterungen funktionieren natürlich nur mit Verträgen / Lizenzen zu den entsprechenden Produkten.

Opti.Tax Verfahrensdokumentation
kontool-Verknüpfung
GetMyInvoices-Schnittstelle

Alle Preise netto.

Anlage 2 zum Vertrag Nummer Vertragsnummer: Datenschutzrechtliche Vereinbarung (nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)

zwischen

Kanzlei

Kanzleizusatz

Strasse Nr

PLZ ORT

- „Auftraggeber“ -

und

TrustStone Software GmbH

Am Sandtorkai 68

20457 Hamburg - „Auftragsverarbeiter“ –

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

- Administrative Wartung und Betreuung der beim Auftraggeber genutzten Produkte des Auftragsverarbeiters
- Wartung und Support der Datenverarbeitungsverfahrenen mit der Möglichkeit des Zugriffs auf personenbezogene Daten
- Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in Deutschland erbracht. Jede Verlagerung der Dienstleistung oder Teilarbeiten in ein Mitgliedsstaat der Europäischen Union oder in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der

Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Die Dauer und die Kündigungsfristen des Vertrags richten sich nach dem zwischen Auftraggeber und Auftragsverarbeiter geschlossenen Hauptvertrag. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Zweck, Umfang und Art der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden.

Der Zweck der Verarbeitung personenbezogener Daten, ist die organisatorische Zusammenarbeit zwischen Kanzleien und deren Mandanten zu unterstützen. Ins Besondere geht es darum, Dokumente sicher und einfach auszutauschen sowie Mandanten eine einfache und zeitgemäße Möglichkeit zu bieten, Daten für die anfallenden Tätigkeiten des Auftraggebers bereitzustellen. Die Plattform dient dabei lediglich als Drehscheibe. Das Ziel ist es, alle Dokumente und Daten in der jeweils eingesetzten Kanzleisoftware zu verarbeiten (z.B. DATEV). Der Umfang der Verarbeitung richtet sich nach Ermessen des Auftraggebers. Der Auftraggeber kann individuell für jeden Mandanten entscheiden, in welchem Umfang er Daten benötigt. So werden bei Neumandaten z.B. Stamm-, Bank-, Finanzamts- und Kommunikationsdaten (siehe unten) zur weiteren Bearbeitung und Generierung von Vollmachten oder Verträgen erfasst. Von einem Mandanten, der beispielsweise nur Dokumente für die Finanzbuchhaltung übermittelt, werden hingegen lediglich Grunddaten wie Name, E-Mailadresse und Ähnliche erfasst. Hier gilt der Grundsatz der Datensparsamkeit!

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Auftraggeberdaten
- Kundendaten des Auftraggebers (= „Mandanten“)
- Mitarbeiterdaten des Kunden des Auftraggebers (=“Mitarbeiter des Mandanten“)
- Mitarbeiterdaten des Auftraggebers
- Mitarbeiterdaten des Auftragsverarbeiters

- Beschäftigtendaten
- Interessenten- / Kundendaten
- Dienstleister- / Lieferantendaten
- Kommunikationsdaten (z.B. zu Email, Internet, Telefon)
- Vertragsstammdaten
- Vertragsbewegungsdaten (z.B. Abrechnungsdaten und Zahlungsdaten)

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

- Stammdaten
    - Firmendaten
    - Persönliche Daten
    - Daten der Ansprechpartner
    - Adressdaten
    - Kommunikationsdaten
    - Bankdaten
    - Steuerliche Daten
    - Statistische Daten (z.B. „Wie sind Sie auf uns gekommen?“)
    - Alle restlichen Daten, die im Rahmen einer Beauftragung eines Steuerberaters anfallen
- Einkommensteuerdaten
    - Alle im Rahmen der Bearbeitung einer Einkommensteuererklärung notwendigen Daten zu den einzelnen Sachverhalten und Veranlagungsjahren. Als Beispiele seien aufgeführt:
        - Private Stammdaten
        - Angaben zu steuerlichen Sachverhalten (z.B. durch „ja“, „nein“, „kann ich nicht beurteilen“)
        - Angaben zu Einkünften und Einkunftsarten
- Dokumentendaten
    - Alle im Rahmen der Bearbeitung von Dokumenten notwendigen Daten. Als Beispiele seien aufgeführt:
        - Dateiname
        - Größe der Datei
        - Dateiinhalt
        - Datum des Uploads
- Finanzbuchhaltungsdaten

- Alle im Rahmen der Bearbeitung einer Finanzbuchhaltung notwendigen Daten zu den einzelnen Sachverhalten und Veranlagungsjahren. Als Beispiele seien aufgeführt:
  - Gewinnzahlen pro Monat
  - Auswertungen und Bescheide

- Lohnbuchhaltungsdaten
  - Alle im Rahmen der Bearbeitung einer Lohnbuchhaltung notwendigen Daten zu den einzelnen Sachverhalten. Als Beispiele seien aufgeführt:
    - Stundennachweise
    - Gehaltsabrechnungen
    - Sozialversicherungsdaten
- Sonstige im Zusammenhang mit der Bearbeitung eines steuerlichen Sachverhalts stehende Daten von Kanzlei und Mandant (=Kunde der Kanzlei).
- Nutzungs- und Zugriffsdaten
- Fehlerprotokolldaten
- Unterstützungs- und Supportdaten der Mitarbeiter des Auftragsverarbeiters (z.B. wer hat wann, wem, wie bei was geholfen?)
- Zugangsdaten

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Personen beim Auftraggeber sind in der „**Anlage 1 zum AVV: Weisungsberechtigte Personen beim Auftraggeber**“ gelistet.

Weisungsempfänger beim Auftragsverarbeiter sind in der „**Anlage 2 zum AVV: Weisungsempfänger beim Auftragsverarbeiter**“ gelistet.

Für Weisung zu nutzende Kommunikationskanäle:

- postalisch an folgende Anschrift:
  TrustStone Software GmbH, Am Sandtorkai 68, 20457 Hamburg oder
- per Email an folgende Adresse:
  info@truststone-software.com oder an die jeweilige Mailadresse des Ansprechpartners oder
- per Telefon an folgende Rufnummer:
  +49 40 368 811 170

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen/Auftraggeber diese rechtlichen Anforderungen vor der

Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Verfügbarkeitskontrolle der Daten durch mindestens tägliche Datensicherung
- Plausibilitätskontrolle der Verarbeitungsergebnisse

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die in Ziffer 4 genannten weisungsberechtigen Personen des Auftraggebers weiterzuleiten.

Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit/Home Office von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

- Bankgeheimnis
- Fernmeldegeheimnis nach dem TKG und TMG
- Sozialgeheimnis
- Berufsgeheimnis nach § 203 StGB

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:

IITR GmbH
Rechtsanwalt Dr. Sebastian Kraska
Marienplatz 2
80331 München

Email: email@iitr.de

Tel: +49 89 1891 736 0

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern für Kerndienstleistungen (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragsverarbeiter muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des

Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

- Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) mittels eines Fragenkataloges oder
- Regelmäßige Prüfung der beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre) oder
- Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) durch eine Begehung vor Ort oder
- Regelmäßige Einholung von Zertifikaten über eine gültige Zertifizierung nach der DS-GVO.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragsverarbeiter die in der „**Anlage 3** zum AVV - Unterauftragsverhältnisse“ genannten Subunternehmer tätig. Der Auftraggeber erklärt sich hiermit einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Der Auftraggeber erhält die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben, sofern die bisher vereinbarten und von Auftragsverarbeiter zugesicherten technischen und organisatorischen Maßnahmen nicht vollständig gewährleistet werden können (§ 28 Abs. 2 Satz 2 DS-GVO). In diesem Fall darf die beabsichtigte Änderung nicht vollzogen werden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.

Das in „**Anlage 4** zum AVV – Technische und organisatorische Maßnahmen / Datenschutzkonzept“ beschriebene Datenschutzkonzept stellt die Mindestanforderungen der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar. Hierbei ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).

Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im

Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen (unter Zuhilfenahme eines für die sichere Datenlöschung zugelassenen Softwareprogramms).

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das von Auftragsverarbeiter örtlich zuständige Gericht vereinbart.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

X

Ort, Datum, Kanzlei (Unterschrift Vertretungsberechtigter)

(Auftraggeber)

Hamburg, den Datum

Ort, Datum, TrustStone Software GmbH

(Auftragsverarbeiter)

Anlage 1 zum AVV: Weisungsberechtigte Personen beim Auftraggeber

Name, Vorname	Position
Weisungsberechtigte Pers	Geschäftsführer

Für Änderungen der weisungsberechtigten Personen beim Auftraggeber, wird der Auftraggeber dies schriftlich, in Textform oder mittels systeminterner Mitarbeiterverwaltung dem Auftragsverarbeiter mitteilen.

Anlage 2 zum AVV: Weisungsempfänger beim Auftragsverarbeiter

Name, Vorname	Position
Herr Krys, Kilian	Geschäftsführer
Herr Hellmig, Philip	Geschäftsführer

Für Änderungen der Weisungsempfänger beim Auftragsverarbeiter, wird der Auftragsverarbeiter dies mittels systeminterner Kanzleieinstellungen dem Auftraggeber zu erkennen geben.

Anlage 3 zum AVV - Unterauftragsverhältnisse

Aktuell bestehen die nachfolgenden Unterauftragsverhältnisse im Zusammenhang mit der Auftragsverarbeitung:

Pos	Unternehmen	Kontaktdaten	Beschreibung
1	Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen +49 (0) 9831 505-0	Deutsches Hochleistungsrechenzentrum https://www.hetzner.de
2	hostNET Medien GmbH	Osterdeich 107, 28205 Bremen +49 (0) 421 37966-0	Deutsches Hochleistungsrechenzentrum https://www.hostnet.de
3	STRATO AG	Pascalstraße 10, 10587 Berlin +49 (0) 30 300 146-0	Deutsches Hochleistungsrechenzentrum https://www.strato.de/
4	ALL-INKL.COM - Neue Medien Münnich	Hauptstraße 68, 02742 Friedersdorf +49 (0) 35872 353-10	Deutsches Hochleistungsrechenzentrum https://www.all-inkl.com/
5	Alfahosting GmbH	Ankerstraße 3b, 06108 Halle (Saale) +49 (0) 345 279 58 0	Deutsches Hochleistungsrechenzentrum https://alfahosting.de

Anlage 4 zum AVV – Technische und organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO.

Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Es erfolgt keine Verarbeitung personenbezogener Daten in den Geschäftsräumen des Auftragsverarbeiters. Dennoch sind die Räume nicht frei zugänglich. Sie sind bei Abwesenheit der Mitarbeiter verschlossen. Die Zutrittsberechtigungen sind in einem geregelten Verfahren nach dem „need to know Prinzip“ vergeben und werden regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht. Das Gebäude kann nur mit einem entsprechenden RFID-Chip betreten werden. Die Büroflächen werden morgens und abends mit einem Sicherheitsschloss verriegelt. Der Zugang tagsüber erfolgt über einen RFID-Chip.

Räume, in denen Datenverarbeitungsanlagen (Rechenzentrum, Server, Netzwerkverteiler usw.) untergebracht sind, sind besonders zutrittsgeschützt und sind nur für Beschäftigte der IT-Administration zugänglich. Besucher und unternehmensfremde Personen sind in einem dokumentierten Verfahren registriert und werden innerhalb der Geschäftsräume beaufsichtigt. Diese Kontrollen werden allerdings von unseren Unterauftragnehmern gewährleistet und sind vertraglich geregelt, da alle Datenverarbeitungsanlagen von unseren Unterauftragnehmern bereitgestellt werden. Entsprechende Dokumente können auf Anfrage eingesehen bzw. zur Verfügung gestellt werden.

1.2. Zugangskontrolle

Wie in 1.1. bereits erläutert, erfolgt in den Geschäftsräumen des Auftragsverarbeiters keine Verarbeitung personenbezogener Daten. Alle Maßnahmen, die geeignet sind zu verhindern, dass

Datenverarbeitungssysteme von Unbefugten genutzt werden können, werden von unseren Unterauftragnehmern gewährleistet. Entsprechende Dokumente können auf Anfrage eingesehen bzw. zur Verfügung gestellt werden.

Darüber hinaus sind alle Zugänge passwortgeschützt. Ein Zugriff besteht nur für autorisierte Mitarbeiter des Auftragsverarbeiters. Alle Passwörter müssen eine Mindestlänge haben und werden in regelmäßigen Abständen erneuert.

1.3 Zugriffskontrolle

Es wurden Maßnahmen getroffen, 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.

Getroffene Maßnahmen sind z.B.:

- Berechtigungskonzept
    - Berechtigungsgruppen
        - Systemadministrator
        - Kanzleiadministrator
        - Kanzleimitarbeiter
        - Mandant
    - Berechtigungen
        - Mandantendaten können nur vom Mandanten selbst oder durch die Kanzleimitarbeiter gelesen, verändert oder entfernt werden
        - Mandantenzugänge können nur durch den Kanzleiadministrator gelöscht werden
        - Kanzleimitarbeiter können nur durch Kanzleiadministratoren erstellt, bearbeitet oder entfernt werden
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren sind auf das „Notwendigste“ reduziert
- Eine Mindestpasswortlänge, sowie das Vorkommen von mindestens einer Zahl und einem Buchstaben sind vom System vorgegeben
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung der personenbezogenen Daten in der Datenbank
- Verschlüsselung der hochgeladenen Dokumente

- Wartungen der Online-Plattform werden mit eindeutiger Benutzerkennung vorgenommen und protokolliert
- Fernwartungen auf den Systemen des Auftraggebers bedürfen immer einer Einzelfreigabe durch den Auftraggeber. Es erfolgt kein Dauerzugriff oder eine Aufschaltung ohne Zustimmung des Auftraggebers.

1.4 Pseudonymisierung

Auswertungen werden pseudonymisiert, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

1.5 Trennungskontrolle

Die Trennung von personenbezogenen Daten wird durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt.

Getroffene Maßnahmen sind z.B.:

- Logische Mandantentrennung (softwareseitig)
- Einzelne Instanzen der Online-Plattform sind entweder logisch oder physikalisch voneinander getrennt
- Trennung von Produktiv- und Testsystem

2. Integrität

2.1 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle ist sichergestellt, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail greifen entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern). Mobile Geräte oder mobile Speichermedien werden verschlüsselt, wenn auf ihnen personenbezogene Daten gespeichert werden.

Getroffene Maßnahmen sind z.B.:

- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Die Kommunikation zwischen dem Kreis der Betroffenen und der Online-Plattform erfolgt ausschließlich verschlüsselt
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung

2.2 Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten kann dem durchführenden Beschäftigten zugeordnet werden. Die Änderungen und Löschungen von Datensätzen ist systemseitig eingeschränkt, damit ein versehentliches Ändern oder Löschen wirksam verhindert wird.

Getroffene Maßnahmen sind z.B.:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (*siehe Zugriffskontrolle*)

2.3 Auftragskontrolle

Im Rahmen der Auftragskontrolle ist sichergestellt, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu sind die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen. Die Auftragsverarbeitung wird durch interne Kontrollen überwacht. Die Ergebnisse der Kontrollen werden dokumentiert.

Unterauftragnehmer dürfen nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt werden. Die Übermittlung oder der Zugriff auf personenbezogene Daten darf erst dann erfolgen, wenn der Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO unterzeichnet hat und die Einhaltung der Regelungen des Datenschutzkonzeptes bestätigt hat. Die Prüfpflicht des Auftragsverarbeiters gegenüber seinem Unterauftragnehmer ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit

Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es sind im Netz keine Systeme verbunden, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches werden innerhalb von 72 Stunden nach Bekanntgabe eingespielt. Die durchgängige Verfügbarkeit von personenbezogenen Daten wird mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet. Rechenzentren und Serverräume entsprechen dem Stand der Technik (Temperaturregelung, Brandschutz, Wassereinbruch etc.). Die Server verfügen über eine unterbrechungsfreie Stromversorgung (USV), die ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es ist ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert. Dieses beinhaltet die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regemäßige Auditierung der Datenverarbeitungsverfahren. Ebenso erfolgt die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens vor Aufnahme der Datenverarbeitung. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte ist ein durchgängiger Meldeprozess und Bearbeitungsprozess eingeführt. Dieser beinhaltet auch die Information des Auftraggebers.

Anlage 3 zum Vertrag Nummer Vertragsnummer:

Ersteinrichtung kanzlei.land

Umfang der Ersteinrichtung

Es wird das Grundsystem des kanzlei.land eingerichtet.

Bereitstellung über die folgende Domain:	**https://**
Orientierung des Designs:	**Homepage / Logo**
Kanzleiname kurz:	**Kanzlei Kurz**
Kanzleiname lang:	**Kanzlei Lang**

X

Ort, Datum, Kanzlei (Unterschrift Vertretungsberechtigter)

Anlage 4 zum Vertrag Nummer Vertragsnummer:

SEPA-Lastschriftmandat (wiederkehrende Zahlungen)

Gläubiger-Identifikationsnummer: **DE53ZZZ00001791866**

Mandatsreferenz: **Vertragsnummer**

Kanzlei

Kanzleizusatz

Strasse Nr

PLZ ORT

Bitte leserlich ausfüllen:

Kreditinstitut:

Inhaber:

IBAN:

BIC:

Ich ermächtige die TrustStone Software GmbH, Zahlungen mittels Lastschrift von obigem Konto einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von TrustStone Software GmbH auf mein Konto gezogenen Lastschriften einzulösen. Die Frist für die Vorabinformation des Lastschrifteinzuges (Pre-Notification) wird auf 5 Kalendertage verkürzt.

Hinweis: Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

X

Ort, Datum, Kanzlei (Unterschrift Vertretungsberechtigter)

Anlage 5 zum Vertrag Nummer Vertragsnummer:

Allgemeine Geschäftsbedingungen

Allgemeines, Geltungsbereich

Die nachstehend aufgeführten allgemeinen Geschäftsbedingungen gelten für sämtliche Geschäftsbeziehungen zwischen Kunden und der TrustStone Software GmbH, nachfolgend auch als „TSS“ bezeichnet. Die allgemeinen Geschäftsbedingungen sind Vertragsbestandteil. Es gilt die im Zeitpunkt des Vertragsschlusses gültige Fassung.

Leistungen, Vertragsverhältnis

TSS bietet seinen Kunden cloudbasierte Softwarelösungen zum Austausch und zur Verarbeitung von Daten an. Über das Internetportal kanzlei.land wird die Software auch von Kunden (Mandanten) der Kunden von TSS verwendet. Der Kunde kann die gewünschten Leistungen für seine Mandanten im kanzlei.land individuell beauftragen. TSS gewährleistet eine Erreichbarkeit des kanzlei.land von 99% im Jahresmittel. Ausgenommen sind Zeiten die nicht im Einflussbereich von TSS liegen (Höhere Gewalt, Verschulden Dritter etc.) und vorab angekündigte Wartungsarbeiten, welche in der Regel zwischen 22:00 Uhr und 09:00 Uhr stattfinden.

Datensicherheit

Daten und Belege, die vom Kunden oder von seinen Mandanten in das kanzlei.land übermittelt werden, liegen sicher verschlüsselt auf den Servern von TSS. Der Kunde kann für seine Mandanten jeweils Zugänge für das kanzlei.land freischalten und Passwörter vergeben. Der Kunde bzw. seine Mandanten haften für jeden Missbrauch, der sich aufgrund unberechtigter Verwendung der Passwörter ergibt.

Datensicherungen werden von TSS täglich durchgeführt. Für die verschlüsselte Übertragung von Daten zwischen Eingabegerät und dem kanzlei.land wird für den Kunden ein SSL-Zertifikat bereitgestellt.

Datenschutz

TSS erhebt, verarbeitet und nutzt personenbezogene Daten von Kunden nur, soweit sie für die Vertragsabwicklung erforderlich sind.

Die E-Mail-Adresse des Kunden nutzt TSS nur für Support-Benachrichtigungen, Rechnungen und Preisanpassungen.

Trotz aller Anstrengungen von TSS ist sich der Kunde darüber bewusst, dass Daten, die er oder seine Mandanten ins Internet übermitteln und auf Servern speichern unter Umständen von anderen Teilnehmern im Internet unbefugt eingesehen werden können. Insofern kann TSS hierfür keine Haftung für daraus entstehende Schäden übernehmen.

Urheberrechte, Eigentumsvorbehalt

Für die Dauer des Vertrages erhält der Kunde das uneingeschränkte Recht das kanzlei.land bei seinen Mandanten und darüber hinaus zu bewerben.

Preise und Zahlungsbedingungen

Die nutzungsabhängigen Entgelte werden dem Kunden monatlich in Rechnung gestellt. Zahlungen erfolgen durch Bankeinzug mittels SEPA-Basislastschrift. Für sämtliche Leistungen gilt die jeweils gültige Preisliste. TSS kann die Preise jeweils zum Beginn des Monats anpassen und den Kunden vorab darüber per Email informieren. Die Preisanpassung gilt als genehmigt, wenn der Kunde nicht innerhalt einer angemessenen Frist von 4 Wochen widerspricht. Gerät der Kunde in Zahlungsverzug kann TSS ihre Leistungen und Dienste für den Kunden und dessen Mandanten sperren.

Pflichten des Kunden

Das kanzlei.land wird von Mandanten des Kunden zum Austausch von Belegen und Daten genutzt. Für die Einrichtung des kanzlei.land stellt der Kunde TSS ggf. eine Domain bzw. Subdomain zur Verfügung über die das kanzlei.land zur Verfügung gestellt wird.

Der Kunde ist verpflichtet seine Mandanten über mögliche Risiken bei der Übermittlung von Daten im Internet zu unterrichten.

Die Plattform kanzlei.land darf ausschließlich zum Austausch von Dateien oder Daten genutzt werden, die im Rahmen des Vertragsverhältnisses zwischen Kunde und Mandant erforderlich sind.

Haftung von TSS

Für die Dauer des Vertrages können der Kunde und insbesondere seine Mandanten jederzeit auf seine Daten zugreifen. Für die Langzeitverfügbarkeit der Belege ist alleinig der Mandant des Kunden verantwortlich. TSS tritt nicht für gesetzliche Aufbewahrungspflichten ein. TSS übernimmt keine Haftung für Datenverluste und ggf. daraus entstehende Schäden.

Vertrag, Erfüllungsort, Kündigung

Der Vertrag läuft auf unbestimmte Zeit und kann vom Kunden und von TSS jeweils zum Monatsende gekündigt werden.

Nach Beendigung des Vertrages wird TSS sämtliche Mandantenzugänge des Kunden zunächst sperren. Der Kunde kann nach Beendigung während einer Frist von 4 Wochen bei Bedarf Mandantendaten sichern. Nach einer weiteren Frist von 4 Wochen wird TSS sämtliche Daten des Kunden und seiner Mandanten unwiederbringlich löschen.

Schlussbestimmungen

Die AGB, der Vertrag und die Preisliste umfassen sämtliche Abreden der Parteien. Nebenabreden und Änderungen bedürfen der Schriftform. Email und Telefax erfüllen die Schriftform. Gerichtsstand und Erfüllungsort ist Hamburg.

Sollten einzelne Bestimmungen des Vertrages oder dieser AGB unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen nicht. Die Parteien verpflichten sich, die unwirksame Regelung durch eine Regelung zu ersetzen, die der unwirksamen am nächsten kommt.