Version 3.0 vom 18. April 2024

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen **dem Kunden**

im Folgenden: **Auftraggeber**

und der **ThinkImmo GmbH**

im Folgenden: **Auftragnehmer**

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Gegenstand der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten bestimmen sich nach der Leistungsvereinbarung und dieser Vereinbarung zur Auftragsverarbeitung. Die allgemeinen Nutzungsbedingungen (https://connect.thinkimmo.com/terms) stellen die Leistungsvereinbarung dar und werden bei der Registrierung durch den Verantwortlichen ausdrücklich zugestimmt.

2.2 Dauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung. Ist die Leistungsvereinbarung ordentlich kündbar, gelten die Bestimmungen der Leistungsvereinbarung. Im Zweifel gilt eine Kündigung der Leistungsvereinbarung auch als Kündigung dieser Vereinbarung und eine Kündigung dieser Vereinbarung als Kündigung der Leistungsvereinbarung.

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Umfang, Art und Zweck der Datenverarbeitung

Eine elektronische Verarbeitung von personenbezogenen Daten gem. Absatz 3.2 findet unter Einsatz der Dienste des Auftragsverarbeiters durch den Verantwortlichen statt. Der Einsatz der Dienste des Auftragsverarbeiters richtet sich nach der Nutzung durch den Verantwortlichen und dieser Auftragsverarbeitungsvereinbarung und stellt dessen grundsätzlich abschließende Weisung an den Auftragsverarbeiter dar. Der Einsatz der Dienste des Auftragsverarbeiters durch den Verantwortlichen führt – je nach Nutzung - zu mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgängen oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten gem. Absatz 3.2, die insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung umfassen können. Die Datenverarbeitung folgt dem der jeweiligen Dienstnutzung durch den Verantwortlichen zugrundeliegenden Zweck, insbesondere zum Management von Geschäftsbeziehungen mit Kontakt- und Empfängerpersonen, zur Kommunikation mit Kontakt- und Empfängerpersonen, zum Direktmarketing sowie zur Transaktionskommunikation mit Kontakt- und Empfängerpersonen. Um einen sicheren und effizienten Dienst bereitzustellen, implementiert der

Auftragsverarbeiter eine Reihe von Maßnahmen, um die personenbezogenen Daten zu verarbeiten. Diese Maßnahmen dienen dazu, Betrug, Phishing, unerwünschte Kommunikation oder jegliches anderes unerlaubtes Verhalten gegenüber der Plattform, der Infrastruktur oder dem Dienst des Auftragsverarbeiters zu erkennen, zu überwachen und zu verhindern. Die Maßnahmen werden in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften und gemäß der Datenschutzrichtlinie des Auftragsverarbeiters durchgeführt.

Zu den konkreten Maßnahmen gehören:

1. **Verschlüsselungstechnologien:** Der Auftragsverarbeiter verwendet fortschrittliche Verschlüsselungstechnologien, um die Daten während der Übertragung und bei der Speicherung zu schützen. Dies stellt sicher, dass die Daten vor unerlaubtem Zugriff geschützt sind.

2. **Anwendung von Firewalls und Intrusion-Detection-Systemen:** Diese Technologien dienen dazu, unerwünschten Verkehr zu blockieren und Angriffsversuche zu erkennen und zu verhindern.

3. **Zugriffskontrollmechanismen:** Der Zugang zu den Daten ist streng kontrolliert. Nur autorisiertes Personal hat Zugang zu den Daten, und es werden regelmäßige Überprüfungen durchgeführt, um sicherzustellen, dass die Zugriffsrechte aktuell und angemessen sind.

4. **Antiviren- und Antimalware-Software:** Die Infrastruktur des Auftragsverarbeiters ist mit Antiviren- und Antimalware-Software ausgestattet, um Schadsoftware zu erkennen und zu entfernen, die die Sicherheit der Daten beeinträchtigen könnte.

5. **Datensicherung und Disaster-Recovery-Plan:** Der Auftragsverarbeiter hat robuste Backup-Verfahren und einen Disaster-Recovery-Plan implementiert, um sicherzustellen, dass die Daten im Falle eines Datenverlusts oder einer Katastrophe wiederhergestellt werden können.

Diese Maßnahmen sind integraler Bestandteil der Verpflichtung des Auftragsverarbeiters, einen sicheren und effizienten Dienst bereitzustellen und gleichzeitig die personenbezogenen Daten der Nutzer zu schützen.

3.2 Art der Daten

Es werden folgende Daten verarbeitet:

Arten von Daten

i. Verantwortlicher und Personen, die vom Verantwortlichen zur Nutzung des Accounts berechtigt sind (zusammenfassend "Nutzer"): Identifikations- und Kontaktdaten (Name, Adresse, Titel, Kontaktdaten, Benutzername, Unternehmens-/Organisationsdaten); Beschäftigungs-/Organisationsdaten (geografischer Standort, Website), Sendeinformationen (E-Mail-Adresse, IP-Adresse, Datum und Uhrzeit).

ii. Kontaktpersonen/Empfängerperson des Verantwortlichen: Identifikations- und Kontaktdaten, wie sie vom Nutzer hochgeladen wurden (Name, E-Mail-Adresse,

Telefonnummer, Notizen); IT-Informationen (IP-Adressen, Öffnungs-/Klickrate, Online-Navigationsdaten).

Es ist wichtig zu betonen, dass in der Verarbeitung dieser Daten keine besonders schützenswerten Daten gemäß der Datenschutz-Grundverordnung (DSGVO) erhoben werden. Besonders schützenswerte Daten sind Kategorien personenbezogener Daten, die eine höhere Stufe an Schutz erfordern, da ihre Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen könnte. Dazu gehören Daten über Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Der Auftragsverarbeiter stellt sicher, dass bei der Verarbeitung der oben genannten Datenarten keine besonders schützenswerten Daten erhoben werden und die Verarbeitung in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften erfolgt. Diese Verpflichtung umfasst die Implementierung angemessener technischer und organisatorischer Maßnahmen, um die Sicherheit und Integrität der verarbeiteten Daten zu gewährleisten.

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

<u>Personenkategorien</u>

i. Nutzer und

ii. Jede Person,

- deren E-Mail-Adresse oder Telefonnummer in der Kundenverteilerliste enthalten ist;
- deren Informationen über die Funktionalitäten der Plattform („Dienste des Auftragsverarbeiters“) gespeichert oder gesammelt werden,
- an die Nutzer E-Mails senden oder mit denen sie auf andere Weise über die Dienste des Auftragsverarbeiters in Kontakt treten oder kommunizieren (zusammenfassend "Abonnenten").

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen, regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

5 Sicherheit der Verarbeitung

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Der Auftragsverarbeiter hat alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vertragliche oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren. Der Auftraggeber und der Auftragnehmer vereinbaren, dass Endkunden (Verbraucher) des Auftraggebers eine technische Möglichkeit eingeräumt wird, damit diese Endkunden ihre jeweiligen Daten bzw. den dafür zugrundeliegenden Account beim Auftragnehmer selbst löschen können.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter hat zwar die allgemeine Erlaubnis, weitere Auftragsverarbeiter (Subunternehmen) hinzuzuziehen, jedoch ist dies an strenge Bedingungen geknüpft, um die Sicherheit Ihrer Daten zu gewährleisten. Alle derzeit beteiligten Subunternehmen sind in Anhang 2 "Unterauftragsverarbeiter" klar und transparent aufgelistet. Falls sich Änderungen ergeben und wir einen neuen Subunternehmer hinzuziehen müssen, werden wir Sie umgehend informieren. Sie haben dann die Möglichkeit, gemäß Art. 28 Abs. 2 S. 2 DSGVO Einspruch gegen diesen neuen Subunternehmer zu erheben, wenn Sie Bedenken haben. Dies kann innerhalb von zwei Wochen nach unserer Mitteilung erfolgen. Bitte beachten Sie, dass wir nur Subunternehmer in Anspruch nehmen, die dieselben strengen Datenschutzstandards erfüllen, die wir auch einhalten. Sollten Sie jedoch trotzdem ernsthafte datenschutzrechtliche Bedenken haben, haben Sie das Recht, die Auftragsverarbeitung außerordentlich innerhalb von 30 Tagen nach dem Einspruch zu kündigen. Umgekehrt könnten wir auch die Auftragsverarbeitung kündigen, falls ein Einspruch eingelegt wird. Allerdings wollen wir Sie versichern, dass wir stets im besten Interesse Ihrer Datensicherheit handeln und alle notwendigen Maßnahmen treffen, um Ihre Daten zu schützen. Alle Mitteilungen im Zusammenhang mit diesen Prozessen erfolgen gemäß Anhang 3 "Kontakt und Kommunikation", um sicherzustellen, dass die Kommunikation klar und transparent ist. Unser Hauptziel ist es, Ihnen einen sicheren, zuverlässigen und effizienten Service zu bieten.

(2) Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als reine Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt und die sich daher nicht unmittelbar auf die Erbringung der Hauptleistung beziehen. Hierzu gehören – ohne abschließend zu sein – beispielsweise Post-, Transport- und Versanddienstleistungen, Reinigungsdienstleistungen, Bewachungsdienste, Telekommunikationsleistungen, Benutzerservice, Wartung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit personenbezogener Daten des Verantwortlichen

auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem neuen Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung. Sofern Subunternehmer in Drittländern eingeschalten werden, stellt der Auftragsverarbeiter sicher, dass die zusätzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens.

8 Mitteilungspflichten

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach 8 vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

9 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch

den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

11 Schlussbestimmungen

(1) Der Auftragsverarbeiter kann diese Vereinbarung mit einer Vorlaufsfrist von zwei Wochen ändern oder ersetzen. Auf Änderungen oder Ersetzungen der Vereinbarung wird der Verantwortliche per E-Mail oder in seinem Account hingewiesen. Dem Verantwortlichen steht ein außerordentliches Kündigungsrecht zu, welches er innerhalb 30 Tage ab Hinweis ausüben kann. Die außerordentliche Kündigung hat gem. Anhang 3 „Kontakt und Kommunikation“ zu erfolgen.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare 10 Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(3) Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Berlin.

Anlage 1 – technische und organisatorische Maßnahmen

(1) Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der personenbezogenen Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

(2) Der Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

(3) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Vertraulichkeit	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	- Zutritt zu den Büroräumen nur durch oder in Begleitung von berechtigten Personen, - Zutrittskontrollsystem zu Büroräumen mithilfe von Schlüsselkonzept (Türsicherung, Eintritt nur mit Schlüssel, dokumentierte Schlüsselvergabe), - Lagerung von vertraulichen Dokumenten ausschließlich unter Verschluss in abschließbaren Räumen.
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	- Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, - Kennwortverfahren und Passwortschutz durch verpflichtenden Einsatz eines webbasierten Passwortmanager, - Zwei-Faktoren-Authentifizierung, - Berechtigungskonzept für digitale Zugriffsmöglichkeiten.
3.	**Zugriffskontrolle** Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und diese bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	- Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte, - Logging, - regelmäßige Auswertung der Logfiles, - automatisierte 24/7 Überwachung der Logs, - Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch	- Übertragung und Übermittlung unter 256-Bit-SSL sowie TLS 1.2 und TLS 1.3 Verschlüsselung, - Firewall, - Virenschutz, - Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, - Nachweis über Versand, Kennzeichnung und Inventarisierung von Datenträgern, - sowie bei der nachträglichen Überprüfung: Protokollieren, wer personenbezogenen Daten an dritte Stellen übermittelt und zu welchem Zweck.

	Einrichtungen zur Datenübertragung vorgesehen ist.	
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	- Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung wird durch Protokollierungssysteme gewährleistet.
Nr.	**Verfügbarkeit und Belastbarkeit**	**Umsetzung der Maßnahme**
6.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogenen Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	tägliches Backup-Verfahren, - Spiegeln von Festplatten beim Unterauftragsverarbeiter (RAID-Verfahren), - unterbrechungsfreie Stromversorgung beim Unterauftragsverarbeiter (USV), - Firewall und Virenschutz bei Auftragsverarbeiter sowie Unterauftragsverarbeiter, - Notfallplan, - Brandmeldeanlage.
Nr.	**Verfügbarkeit und Belastbarkeit**	**Umsetzung der Maßnahme**
7.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.	- Mandantenfähigkeit der Software, - Funktionstrennung zwischen Produktion/Test, - Entwicklungs- und Testsysteme werden ausschließlich mit Testdaten betrieben.
8.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	- Abgrenzung der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter durch eindeutige Vertragsgestaltung mit Abgrenzung der Verantwortlichkeiten zwischen Verantwortlichem und Auftragsverarbeiter, - klare Festlegung von Weisungen durch Textformerfordernis, - Regelung des Einsatzes von Unterauftragsverarbeitung, - Verpflichtung der Beschäftigten auf das Datengeheimnis, - Bestellung eines Datenschutzbeauftragten, Schulung der Mitarbeiter bzgl. Einhaltung von Datenschutz und Datensicherheit.

In Übereinstimmung mit Art. 32 Abs. 1 lit. d) DSGVO haben wir ein strukturiertes Verfahren etabliert, das die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit unserer technischen und organisatorischen Maßnahmen ermöglicht. Dieses Verfahren umfasst:

1. **Halbjährliche Überprüfungen:** Wir haben einen festen Zeitplan festgelegt, der eine Überprüfung unserer Datenschutzmaßnahmen alle sechs Monate vorsieht.
2. **Interne Audits:** Wir führen systematische interne Audits durch, um sicherzustellen, dass unsere Datenschutzmaßnahmen angemessen und effektiv sind. Diese Audits umfassen die Überprüfung von Systemprotokollen, um mögliche Schwachstellen zu identifizieren.
3. **Risikobewertungen:** Wir führen regelmäßig Risikobewertungen durch, um potenzielle Bedrohungen und Schwachstellen zu identifizieren und zu bewerten. Diese Bewertungen helfen uns, unsere Datenschutzmaßnahmen gezielt anzupassen und zu verbessern.
4. **Aktualisierung der Maßnahmen:** Basierend auf den Ergebnissen unserer Überprüfungen und Risikobewertungen passen wir unsere technischen und organisatorischen Maßnahmen

kontinuierlich an, um sicherzustellen, dass sie weiterhin wirksam und den aktuellen Anforderungen entsprechen.

5. **Schulung der Mitarbeiter:** Wir legen großen Wert darauf, dass alle unsere Mitarbeiter, die mit personenbezogenen Daten umgehen, regelmäßig geschult werden. Diese Schulungen helfen uns sicherzustellen, dass jeder im Team die Bedeutung des Datenschutzes versteht und unsere Datenschutzmaßnahmen effektiv umsetzt.

Wir sind uns bewusst, dass der Datenschutz ein dynamisches Feld ist und dass ständige Verbesserungen und Anpassungen notwendig sind. Daher überprüfen wir unser Verfahren regelmäßig, um sicherzustellen, dass es weiterhin effektiv ist und den neuesten regulatorischen Anforderungen entspricht.

Anlage 2.1 – Zugelassene Subdienstleister

Firma	Serverstandort	Anschrift	Auftragsinhalt
DigitalOcean	Deutschland, Frankfurt am Main	101 6th Ave New York, NY 10013	Hosting
HubSpot Germany GmbH	Deutschland, Frankfurt am Main	Am Postbahnhof 17 10243 Berlin Deutschland	CRM System
Mailjet GmbH	Deutschland, Frankfurt am Main	Alt-Moabit 2, 10557 Berlin, Germany	E-Mail Versand
Amazon Web Services (AWS)	Deutschland, Frankfurt am Main	Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109-5210, USA	E-Mail Versand
Custify SRL	Europa	Strada Zăgazului 4E, București 014262, Rumänien	CRM System
Chargebee	US East (N. Virginia)	Piet Heinkade 55 1019GM Amsterdam Netherlands	Zahlungsabwicklung

"Bei einigen der aufgeführten Subdienstleister, wie DigitalOcean und Amazon Web Services, erfolgt eine Datenübermittlung in Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, insbesondere in die USA. Wir weisen darauf hin, dass nach Meinung des Europäischen Gerichtshofs derzeit kein angemessenes Schutzniveau für den Datentransfer in die USA besteht. Dies kann mit verschiedenen Risiken für die Rechtmäßigkeit und Sicherheit der Datenverarbeitung einhergehen.

Um einen angemessenen Schutz der übermittelten personenbezogenen Daten sicherzustellen, haben wir Vorkehrungen getroffen, insbesondere durch den Abschluss von Standardvertragsklauseln (SCCs), die von der Europäischen Kommission genehmigt wurden. Durch diese Klauseln verpflichten sich die

Subdienstleister, bei der Verarbeitung Ihrer relevanten Daten, das europäische Datenschutzniveau einzuhalten, selbst wenn die Daten in Drittländern gespeichert, verarbeitet und verwaltet werden.

Weitere Informationen zur Datenverarbeitung durch DigitalOcean finden Sie in deren Datenschutzbedingungen unter https://www.digitalocean.com/legal. Informationen zur Datenverarbeitung durch Amazon Web Services finden Sie unter https://aws.amazon.com/de/compliance/data-privacy-faq/.

Anlage 2.2 – Funktionsspezifische Unterauftragsverarbeiter

Einige unserer Funktionen und Integrationen erfordern die Unterstützung durch zusätzliche Unterauftragsverarbeiter. Einige Unterauftragsverarbeiter werden standardmäßig eingesetzt, andere kommen nur dann zum Einsatz, wenn Sie dem zustimmen.

Firma	Serverstandort	Anschrift	Auftragsinhalt
Mixpanel, Inc. ZUSTIMMUNG ERFORDERLICH	* Europa	Avenida Diagonal, 442 – P. 3 PTA. 1 08037, Barcelona, Spain.	Datenanalyse
Europace AG ZUSTIMMUNG ERFORDERLICH	* Deutschland	Heidestraße 8, 10557 Berlin	Zinsvorschau, #Passt System
LinkedIn Inc. ZUSTIMMUNG ERFORDERLICH	* Drittländer	605 W Maude Ave, Sunnyvale, CA 94085, USA	Werbung
Meta Platforms Inc. ZUSTIMMUNG ERFORDERLICH	* Drittländer	1 Hacker Way Menlo Park, California 94025	Werbung
Alphabet Inc. ZUSTIMMUNG ERFORDERLICH	* Drittländer	1600 Amphitheater Parkway Mountain View, CA 94043 USA	Werbung
Stripe Inc. ZUSTIMMUNG ERFORDERLICH	* Drittländer	Stripe Payments Europe, Limited (SPEL) 1 Grand Canal Street Lower Grand Canal Dock Dublin D02 H210 Ireland	Zahlungsabwicklung (Kreditkarte, Lastschrift)

* Bei den oben genannten durch Unterauftragsverarbeiter bereitgestellten Funktionen, die mit einem Sternchen markiert sind, besteht die Möglichkeit, auf die Nutzung zu verzichten.

Anlage 3 – Weisungsberechtige Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung von Weisungen befugt:

Branko Hajduk

branko@thinkimmo.com

ThinkImmo GmbH

Karl-Marx-Allee 108, 10243 Berlin

Anlage 4 – Datenschutzbeauftragter

Wir haben einen internen Mitarbeiter als Datenschutzbeauftragten bestellt. Bei Fragen zum Datenschutz oder zur Meldung von Datenschutzverletzungen wenden Sie sich bitte an:

Branko Hajduk

branko@thinkimmo.com

ThinkImmo GmbH

Domagkstraße 34, 80807 München