APPMOBILIEN · WEB.CLOUD.APPS. GMBH

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung

Stand: Oktober 2026

Web.Cloud.Apps. GmbH · Dorfstraße 8 · 71636 Ludwigsburg
www.appmobilien.de · support@appmobilien.de

1. Allgemeines

(1) Diese Auftragsverarbeitungsvereinbarung („AVV“) wird zwischen der Web.Cloud.Apps. GmbH, Dorfstraße 8, 71636 Ludwigsburg (nachstehend „Auftragnehmer“ genannt) und dem Kunden (nachstehend „Auftraggeber“ genannt) geschlossen.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(3) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt. Zudem wird auf die Allgemeinen Geschäftsbedingungen (https://www.appmobilien.de/rechtliches/allgemeine-geschaeftsbedingungen/) und die Leistungsbeschreibung von AppMobilien verwiesen.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, teilt der Auftraggeber diese dem Auftragnehmer in Textform mit. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verarbeitet die Daten grundsätzlich in Mitgliedstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR). Eine Übermittlung in ein Drittland erfolgt nur, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind – insbesondere auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission oder geeigneter Garantien i.S.d. Art. 46 DSGVO. Die eingesetzten Unterauftragnehmer und der Ort ihrer Verarbeitung ergeben sich aus Anlage 3.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Über Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, unterrichtet der Auftragnehmer den Auftraggeber im Voraus in Textform. Im Übrigen gilt Ziffer 14 Abs. 2.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Der Auftragnehmer darf die Verarbeitung auch außerhalb seiner Betriebsstätte durchführen (mobiles Arbeiten, Telearbeit), sofern die technischen und organisatorischen Maßnahmen nach Anlage 2 auch dort eingehalten werden. Der Auftragnehmer stellt insbesondere sicher, dass

- der Zugriff ausschließlich über eine verschlüsselte Verbindung erfolgt;
- die eingesetzten Geräte verschlüsselt sowie durch Kennwort und Bildschirmsperre geschützt sind;
- personenbezogene Daten nicht dauerhaft auf diesen Geräten gespeichert werden;
- Dritte, einschließlich Angehöriger, keine Kenntnis von den Daten nehmen können;
- Unterlagen in Papierform außerhalb der Betriebsstätte nicht verwendet werden.

Eine Verlagerung der Verarbeitung in ein Drittland i.S.d. Kapitels V DSGVO findet dabei nicht statt. Die Beauftragung von Unterauftragnehmern richtet sich ausschließlich nach Ziffer 9.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, teilt der Auftragnehmer diese dem Auftraggeber in Textform mit. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter und Kontaktstelle des Auftragnehmers

(1) Der Auftragnehmer benennt einen Datenschutzbeauftragten, sofern und sobald er hierzu nach Art. 37 DSGVO oder § 38 BDSG verpflichtet ist. Besteht keine Benennungspflicht, stellt der Auftragnehmer sicher, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger Weisungen des Auftraggebers gewährleisten.

(2) Der Auftragnehmer benennt dem Auftraggeber eine Kontaktstelle für Fragen des Datenschutzes und für Meldungen nach Ziffer 6. Diese ist erreichbar unter support@appmobilien.de. Änderungen teilt der Auftragnehmer in Textform mit.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten der Anlaufstelle des Auftragnehmers für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Stehen die vorgenannten Informationen nicht vollständig zur Verfügung, teilt der Auftragnehmer dem Auftraggeber die verfügbaren Angaben unverzüglich mit und reicht die übrigen Angaben ohne unangemessene weitere Verzögerung nach.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen. Der Auftragnehmer kann die Einsichtnahme insoweit beschränken, als ihr die Vertraulichkeit der Daten anderer Auftraggeber, der Schutz von Geschäfts- und Betriebsgeheimnissen oder Rechte Dritter entgegenstehen; in diesem Fall stellt er dem Auftraggeber die zur Beurteilung erforderlichen Angaben in anderer geeigneter Weise zur Verfügung.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftraggeber kann die Kontrolle nach den Absätzen 1 bis 4 auch durch einen von ihm beauftragten Prüfer durchführen lassen. Der Prüfer ist zur Verschwiegenheit zu verpflichten. Der Auftragnehmer kann einem Prüfer widersprechen, der Wettbewerber des Auftragnehmers ist; in diesem Fall benennt der Auftraggeber einen anderen Prüfer.

(6) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Der Auftragnehmer bedient sich zur Vertragserfüllung der in Anlage 3 genannten Unterauftragnehmer.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung i.S.d. Art. 28 Abs. 2 DSGVO, die in Anlage 3 aufgeführten Unterauftragnehmer mit der Verarbeitung personenbezogener Daten zu betrauen.

(3) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung eines weiteren oder Ersetzung eines bestehenden Unterauftragnehmers mindestens zwei Wochen vor deren Wirksamwerden in Textform. Die Information kann auch durch Nachricht innerhalb der Anwendung oder an die vom Auftraggeber hinterlegte E-Mail-Adresse erfolgen. Der Auftraggeber kann der Änderung binnen zwei Wochen ab Zugang der Information aus einem nachvollziehbaren datenschutzrechtlichen Grund widersprechen. Widerspricht der Auftraggeber nicht innerhalb dieser Frist, gilt die Änderung als genehmigt.

(4) Im Fall eines fristgerechten Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung. Kommt eine solche nicht innerhalb von vier Wochen ab Zugang des Widerspruchs zustande, ist der Auftraggeber berechtigt, diesen Vertrag sowie den zugrunde liegenden Hauptvertrag mit einer Frist von einem Monat zu kündigen.

(5) Ist die Hinzuziehung oder Ersetzung eines Unterauftragnehmers erforderlich, um den Betrieb aufrechtzuerhalten oder eine unmittelbare Gefahr für die Sicherheit der Daten abzuwenden, können die Frist nach Absatz 3 Satz 1 und die Widerspruchsfrist nach Absatz 3 Satz 3 auf das aufgrund der Dringlichkeit erforderliche und angemessene Maß verkürzt werden. Der Auftragnehmer informiert den Auftraggeber so früh wie möglich, in jedem Fall aber vor der Beauftragung, in Textform über den vorgesehenen Zeitpunkt des Einsatzes und den Grund der Dringlichkeit. Bis zu diesem Zeitpunkt kann der Auftraggeber aus einem nachvollziehbaren datenschutzrechtlichen Grund widersprechen. Absatz 4 gilt entsprechend.

(6) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(7) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO bzw. § 38 BDSG benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(8) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(9) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln. Angaben, die Geschäftsgeheimnisse des Auftragnehmers oder des Unterauftragnehmers betreffen und für die Beurteilung der datenschutzrechtlichen Pflichten nicht erforderlich sind, dürfen dabei unkenntlich gemacht werden.

(10) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(11) Nicht als Unterauftragsverhältnisse im Sinne dieser Ziffer sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Anwendungen stellt ein Unterauftragsverhältnis und eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar und unterliegt den Regelungen dieser Ziffer, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtungen der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftragnehmer darf die technischen und organisatorischen Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau dadurch nicht unterschritten wird. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, teilt der Auftragnehmer dem Auftraggeber im Voraus in Textform mit. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

(1) Dieser Vertrag ist Bestandteil des Hauptvertrages über die Nutzung von AppMobilien und kommt mit diesem zustande, insbesondere mit der Registrierung unter Einbeziehung der Allgemeinen Geschäftsbedingungen. Er gilt für die Dauer des Hauptvertrages. Die Schriftform i.S.d. Art. 28 Abs. 9 DSGVO wird durch das elektronische Format gewahrt. Auf Wunsch erhält der Auftraggeber ein vom Auftragnehmer unterzeichnetes Exemplar.

(2) Die Kündigungsfristen ergeben sich aus den AGB von AppMobilien bzw. aus der Leistungsvereinbarung.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung erstreckt sich auf sämtliche vorhandenen Kopien. Daten, die in turnusmäßigen Datensicherungen enthalten sind, werden mit dem Ablauf des jeweiligen Sicherungszyklus gelöscht; bis dahin bleiben sie von der weiteren Verarbeitung ausgenommen und werden ausschließlich zur Wiederherstellung im Störungsfall verwendet. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Änderungen und Ergänzungen dieses Vertrages sowie Nebenabreden bedürfen der Textform.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(4) Es gilt dieser Vertrag, sofern die Parteien nicht ausdrücklich etwas anderes vereinbaren.

Anlage 1 – Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber die Software AppMobilien als Cloud-Dienst bereit, mit der dieser die Verwaltung von Immobilien organisiert. Der Funktionsumfang richtet sich nach den vom Auftraggeber genutzten Modulen und umfasst insbesondere:

- **Objektbetreuung** – Verwaltung von Gebäuden, Wohnungen, Räumen, Schlüsseln und Zählern; Wohnungsübergaben und -abnahmen mit Protokoll, Fotos, Zählerständen und Unterschrift; Begehungen mit Prüfpunkten; Mängelverwaltung; Dokumentenablage mit Volltextsuche
- **Kontakte** – Mieter, Eigentümer, Interessenten, Dienstleister und sonstige Kontakte des Auftraggebers mit Notizen, Terminen und Kontaktverlauf
- **Mietverwaltung** – Mietverträge, Sollstellung und Mietkonten, Kautionen, Mietanpassungen und Kündigungen, Zahlungseingang einschließlich des Abrufs von Kontoumsätzen, Lastschriften und Mahnwesen
- **Abrechnungen** – Betriebs- und Heizkostenabrechnungen, Bescheinigungen nach § 35a EStG und Anpassung der Vorauszahlungen
- **WEG-Verwaltung** – Wirtschaftspläne, Hausgeld, Hausgeldabrechnungen, Erhaltungsrücklagen, Eigentümerversammlungen und Beschlusssammlung

Der Zugriff erfolgt über eine Weboberfläche sowie mobile Anwendungen für Android und iOS.

Ergänzend wird auf die Allgemeinen Geschäftsbedingungen (https://www.appmobilien.de/rechtliches/allgemeine-geschaeftsbedingungen/) und die Leistungsbeschreibung von AppMobilien verwiesen.

2. Art der Verarbeitung

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung bzw. andere Formen der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen und Vernichtung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO).

3. Art(en) der personenbezogenen Daten

- Stamm- und Kontaktdaten (Name, Firma, Anschrift einschließlich neuer Anschrift nach Auszug, Telefon, E-Mail, Umsatzsteuer-Identifikationsnummer, Steuernummer)
- Vertragsdaten (Mietverhältnisse und Vertragsparteien, Miete und Nebenkosten, Kautionen und Bürgschaften, Mietanpassungen, Mietminderungen, Kündigungen einschließlich ihrer Gründe)
- Zahlungs- und Bankdaten (Kontoinhaber, IBAN, BIC, SEPA-Mandate, Kontoumsätze mit Gegenpartei und Verwendungszweck, Forderungen, Zahlungen und Mahnungen) sowie die Zugangsdaten zum Online-Banking, soweit der Auftraggeber den Abruf von Kontoumsätzen nutzt
- Objekt- und Verbrauchsdaten mit Personenbezug (Zuordnung von Wohnungen, Schlüsseln und Zählern, Zählerstände, Abrechnungsergebnisse, Miteigentumsanteile, Hausgeld)
- Inhalte von Übergabe- und Abnahmeprotokollen, Begehungen und Mängelmeldungen einschließlich Notizen
- Fotos, die bei Übergaben, Begehungen und Ablesungen aufgenommen werden
- Unterschriften, die auf dem Gerät geleistet werden
- Inhalte der vom Auftraggeber hochgeladenen Dokumente und Dateien einschließlich des daraus gewonnenen Volltexts
- Angaben zu Eigentümerversammlungen und Beschlüssen
- Notizen, Termine und Kontaktverlauf einschließlich Anrufdaten (Rufnummer, Zeitpunkt, Dauer), soweit der Auftraggeber die entsprechenden Funktionen nutzt
- Nutzerdaten der Beschäftigten des Auftraggebers (Name, E-Mail-Adresse, Rolle, Berechtigungen, Zeitpunkt der letzten Anmeldung)

Besondere Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Der Auftraggeber stellt sicher, dass solche Daten nicht in Freitextfeldern, Notizen, Mängelbeschreibungen, Dokumenten oder Bildaufnahmen erfasst werden. Werden sie gleichwohl erfasst, beschränkt sich die Verarbeitung durch den Auftragnehmer auf Speicherung und Bereitstellung; eine inhaltliche Auswertung findet nicht statt.

Genetische Daten sowie biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person werden nicht verarbeitet. Unterschriften werden als Bild gespeichert und nicht zur Identifizierung ausgewertet.

4. Kategorien betroffener Personen

- Mieter, ehemalige Mieter und Mietinteressenten sowie Mitbewohner, soweit erfasst
- Eigentümer, insbesondere Wohnungseigentümer, und deren Vertreter
- Bürgen und sonstige Sicherungsgeber
- Beschäftigte und sonstige Nutzer des Auftraggebers
- Hausmeister, Handwerker, Messdienste, Lieferanten und sonstige Dienstleister und Vertragspartner des Auftraggebers
- sonstige Personen, die in Freitexten, Notizen, Dokumenten oder Bildaufnahmen genannt oder abgebildet werden

Anlage 2 – Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Rechenzentrum und Serversysteme

- Einbruchmeldeanlage
- Automatisches Zugangskontrollsystem
- Legitimationsprüfung der zugriffsberechtigten Personen
- Schließsysteme mit Codesperre, Chipkarten- bzw. Transponder-Schließsystem, Sicherheitsschlösser
- Sorgfältig ausgewähltes Reinigungspersonal
- Protokollierung der Besucher, Ausweiskontrollen
- Videoüberwachung der Zugänge (Innen- und Außenkameras) sowie der Regale und Schränke

Büroräume

- Schließanlage für Gebäude, Etagen und Büroräume
- Zutrittsberechtigung nur für Mitarbeiter und Reinigungskräfte
- Unternehmensfremde, Gäste und Besucher nur in Begleitung eines Mitarbeiters
- Namentliche Dokumentation von Ein- und Ausgangszeit
- Sorgfältig ausgewähltes Reinigungspersonal

1.2 Zugangskontrolle

Rechenzentrum und Serversysteme

- Authentifizierung mit Benutzername und Passwort
- Benutzerprofile werden erstellt
- Hardware-Firewall
- VPN, SSH, SFTP und TLS für alle Verbindungen
- Unterteilung der IT-Systeme in separate logische Netze (VLAN)

Büroräume

- Firmennetzwerk durch Hardware-Firewall geschützt
- VPN, SSH, SFTP und TLS für alle Verbindungen
- Virenschutz mit automatischer Signaturaktualisierung auf allen Arbeitsplatzrechnern
- Authentifizierung mit Benutzername und Passwort
- Passwortrichtlinie: mindestens 12 Zeichen; ein Wechsel wird nur bei Verdacht auf Kompromittierung verlangt
- Automatische Bildschirmsperre nach 15 Minuten
- Regelmäßige und automatisierte Einspielung von Software-Aktualisierungen
- Datenträger in Laptops und Notebooks sind verschlüsselt

1.3 Zugriffskontrolle

- Berechtigungskonzept mit Zuordnung von Benutzerrechten und Benutzerprofilen zu IT-Systemen
- Der Auftraggeber vergibt die Rollen und Berechtigungen seiner Nutzer innerhalb der Anwendung selbst, einschließlich der Freigabe einzelner Dokumentenordner
- Der Zugriff auf Kundendaten durch den Auftragnehmer ist auf einen eng begrenzten, namentlich dokumentierten Personenkreis beschränkt
- Rechteverwaltung durch Systemadministratoren
- Mitarbeiter werden sorgfältig ausgewählt und schriftlich auf die Einhaltung der Vertraulichkeit verpflichtet
- Sichere Aufbewahrung und ordnungsgemäße Vernichtung von Datenträgern; Aktenvernichter im Einsatz
- Physische Löschung von Datenträgern vor deren Wiederverwendung

1.4 Trennung

- Daten, die zu verschiedenen Zwecken verarbeitet werden, werden logisch voneinander getrennt gespeichert
- Kunden haben ausschließlich Zugriff auf ihr eigenes Konto (Mandantenfähigkeit); kein Kunde hat Zugang zu internen oder administrativen Systemen
- Jede Datenabfrage der Anwendung ist an das Kundenkonto gebunden, sodass ein Kunde nur die eigenen Daten abrufen kann
- Test- und Produktivsysteme sind voneinander getrennt und verwenden unterschiedliche Zugänge
- Für Fehlersuche und Versionsmigration können Produktivdaten auf ein gesondertes, gleich geschütztes System übernommen werden; der Zugriff hierauf ist auf einen eng begrenzten Personenkreis beschränkt

2. Verschlüsselung und Pseudonymisierung

- Die Übertragung zwischen Browser bzw. mobiler App und Server erfolgt ausschließlich über verschlüsselte Verbindungen (TLS)
- Passwörter der Nutzer werden nicht im Klartext, sondern als kryptografischer Hash gespeichert
- Datenträger mobiler Geräte des Auftragnehmers sind verschlüsselt
- Auswertungen und Fehleranalysen erfolgen, soweit möglich, ohne Personenbezug

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Die Unternehmensleitung hat die Verantwortung für Datenschutz und Informationssicherheit übernommen (Leitlinie)
- Beschäftigte werden bei Antritt und bei Wechsel des fachlichen Aufgabenbereichs zum Datenschutz geschult
- Beschäftigte werden im Rahmen des Arbeitsvertrages zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet
- Beschäftigte werden jährlich für den Datenschutz sensibilisiert und angehalten, Datenschutzverstöße unverzüglich zu melden
- Keine Massenexportmöglichkeiten
- Regelmäßige Überprüfung und Aktualisierung der Datenschutzmaßnahmen

4. Integrität

4.1 Eingabekontrolle

- Die Systemdienste (Konsole, Datenbanken, Webserver) werden protokolliert
- Direkter schreibender Zugriff auf Datenbanken, Konsole und Serversysteme steht ausschließlich Administratoren zur Verfügung; Nutzer wirken auf die Daten allein über die Anwendung und im Rahmen ihrer Berechtigungen ein
- Protokolle der Systemdienste werden 30 Tage aufbewahrt und anschließend gelöscht
- Abgeschlossene Übergabe- und Abnahmeprotokolle werden als PDF mit den geleisteten Unterschriften festgehalten

4.2 Weitergabekontrolle

- Webbasierte Datenübertragung ausschließlich über HTTPS
- Verbindungen zwischen Büro und Rechenzentrum sind über VPN, SSH und TLS abgesichert
- Sicherungen werden auf Maschinen ohne externen Zugriff aus dem Internet aufbewahrt
- E-Mail-Verschlüsselung wird angeboten
- Der Abruf von Kontoumsätzen erfolgt verschlüsselt unmittelbar beim Kreditinstitut des Auftraggebers (FinTS)

5. Verfügbarkeit und Belastbarkeit

Verfügbarkeit

- Anfertigung von Sicherungskopien, Aufbewahrung an einem sicheren Ort
- Backup- und Recovery-Konzept, Notfallplan
- Blitzableiter, Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in Serverräumen
- Klimaanlage in Serverräumen; Serverräume liegen nicht unter sanitären Anlagen
- Unterbrechungsfreie Stromversorgung (USV)
- Redundanz von Hard- und Software sowie Infrastruktur
- Vertretungsregelungen für abwesende Mitarbeiter

Belastbarkeit

- Last- und Performancetests
- RAID-Systeme (RAID 1, RAID 5, RAID 1+0)
- Skalierende Systeme

Wiederherstellung

- Backup-Systeme, Notfallkonzept, Notstromversorgung
- Integration des Notfallmanagements in die Geschäftsprozesse
- Redundante Server

Anlage 3 – Unterauftragnehmer

Aufgabe	Unterauftragnehmer	Ort der Verarbeitung
Rechenzentrum, Hosting, E-Mail-Server	active 1 GmbH (Rechenzentrum iNTERWERK), Kritenbarg 66, 22391 Hamburg	Deutschland
Support- und Telefonservice	MWC – Mobile World Communications GmbH, Kollwitzstraße 76, 10435 Berlin	Deutschland
Telefonanlage	Gamma Placetel GmbH, Lothringer Straße 56, 50677 Köln	Deutschland

Der Abruf von Kontoumsätzen erfolgt unmittelbar bei dem vom Auftraggeber angebundenen Kreditinstitut. Das Kreditinstitut handelt dabei im Rahmen seines eigenen Vertragsverhältnisses mit dem Auftraggeber und ist nicht Unterauftragnehmer des Auftragnehmers.

Die vorstehende Aufstellung gibt den Stand bei Vertragsschluss wieder. Änderungen teilt der Auftragnehmer dem Auftraggeber nach Ziffer 9 Abs. 3 mit.