ImmoInvent GmbH
Sommerrain 1/1
72631 Aichtal
Deutschland

Vertrag über die Verarbeitung von Daten im Auftrag

gemäß Art. 28 DSGVO

Zwischen Auftraggeber

Ihre Firma
Ihre Strasse/Hausnummer
Ihre PLZ/Ort

und Auftragnehmer

ImmoInvent GmbH
Sommerrain 1/1
72631 Aichtal

Vorschau-Version

Unterschriften

Dieser Vertrag wurde online geschlossen und ist ohne Unterschriften gültig.

Zeitstempel: Der Vertragsschluss erfolgte elektronisch am 28.04.2026 - 15:45:27 Uhr (MEZ) über die Internetseite "immobilien-wertermittlung.de". Genutze IP Adresse des Auftraggebers zu diesem Zeitpunkt: xxx.xxx.xxx.xxx

1. Allgemeines
(1) 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.
(2) 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
(1) 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.

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 Betroffenen Rechte gegenüber dem Auftragnehmer geltend machen.
(3) Der Auftraggeber hat die Möglichkeit, die gespeicherten Daten selbst zu ändern oder vollständig zu löschen. Eine Weisung zur Löschung ist in begründeten Ausnahmefällen möglich, diese muss schriftlich erfolgen.
(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
(5) Der im Rahmen der Anmeldung / Registrierung benannte Ansprechpartner ist gleichzeitig die weisungsberechtigte Person des Auftraggebers.
(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. Weisungen sind stets in Textform zu erteilen und vom Auftragnehmer unverzüglich in Textform zu bestätigen, sowie durch den Auftragnehmer zu dokumentieren. Mündliche Weisungen sind unverzüglich nachzudokumentieren. 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 verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Übermittlung in ein Drittland bedarf der vorherigen dokumentierten Weisung der verantwortlichen Stelle (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 - 49 GDPR erfüllt sind.
(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.
(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.

5. Datenschutzbeauftragter des Auftragnehmers
(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen.

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, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs 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;
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.

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.
(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 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. Unterauftragnehmer / Unterauftragsverhältnisse
(1) Als Unterauftragnehmer im Sinne dieser Bestimmung gelten die vom Auftragnehmer beauftragten Verarbeiter, deren Leistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Dazu gehören nicht die vom Auftragnehmer in Anspruch genommenen Nebendienstleistungen, z. B. Telekommunikationsdienste, Post-/Transportdienste und Reinigung. 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 Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, 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.
(2) Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 2 zu diesem Vertrag angeben.
(3) Die Vergabe an Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:
- der Auftraggeber vom Auftragnehmer mit einer angemessenen Frist von mindestens 14 Tagen im Voraus schriftlich oder in Textform über die Auslagerung an Unterauftragnehmer informiert wird, und
- der Auftragnehmer bis zum Zeitpunkt der Übergabe der Daten an den Auftragnehmer keinen schriftlichen Widerspruch gegen die geplante Auslagerung durch den Auftraggeber erfährt.
Bei Widerspruch gegen einen neuen Unterauftragnehmer oder Wechsel eines bestehenden Unterauftragnehmers besteht ein außerordentliches Kündigungsrecht des Auftraggebers hinsichtlich der betroffenen Leistungsteil(e) des Vertrages, sofern keine zumutbare Alternative angeboten wird.
(4) 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. Schwärzungen von Geschäftsgeheimnissen sind hierbei zulässig.
(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, hat der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch geeignete Maßnahmen sicherzustellen.
(6) Weitere Auslagerungen durch den Unterauftragnehmer bedürfen der ausdrücklichen Zustimmung der verantwortlichen Stelle. Alle vertraglichen Regelungen in der Vertragskette müssen auch den anderen Unterauftragnehmern auferlegt 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 Verpflichtung 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 unterstützten. 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(Einschränkung der Verarbeitung) oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers unverzüglich, jedoch spätestens

innerhalb von 14 Tagen 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 von Unterstützungsleistungen und Mehraufwänden
(1) Unterstützungsleistungen im Sinne dieser Regelung sind insbesondere Mitwirkungen des Auftragnehmers nach Art. 28 Abs. 3 lit. e-f DSGVO sowie Art. 32-36 DSGVO, darunter die Unterstützung bei Betroffenenanträgen (Art. 12-23 DSGVO), bei Meldungen/Benachrichtigungen zu Datenschutzverletzungen (Art. 33, 34 DSGVO), bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO), bei Konsultationen mit Aufsichtsbehörden (Art. 36 DSGVO), bei der Führung/Ergänzung von Verzeichnissen und Nachweisen sowie bei Audits und Auskunftsersuchen.
(2) Unentgeltliche Basisleistungen sind:
a) die Bereitstellung vorhandener Standardnachweise und -unterlagen (z. B. aktuelle TOMs, Subunternehmerliste) einmal pro Kalenderjahr;
b) die Entgegennahme und Bestätigung des Eingangs von Betroffenenanträgen sowie deren interne Zuordnung;
c) die Erstmeldung an den Auftraggeber bei Verdacht auf eine Verletzung des Schutzes personenbezogener Daten und die Übermittlung der dem Auftragnehmer bereits vorliegenden Basisinformationen;
d) die Beantwortung allgemeiner Rückfragen des Auftraggebers mit einem Gesamtaufwand von bis zu 60 Minuten je Kalendermonat.
(3) Vergütungspflichtige Unterstützungsleistungen (Mehraufwände)
Vergütungspflichtig sind Unterstützungsleistungen, die über die in Abs. 2 genannten Basisleistungen hinausgehen, insbesondere:
a) Recherche-, Prüf-, Extraktions-, Lösch-, Sperr- und Exporttätigkeiten in Systemen des Auftragnehmers oder seiner Unterauftragnehmer zur Bearbeitung von Betroffenenanträgen, einschließlich Anonymisierung/Pseudonymisierung, Aufbereitung in kundenspezifischen Formaten und Dokumentation;
b) die Erstellung individueller Stellungnahmen, Risiko- und Folgenabschätzungen, TIAs, Sicherheits- oder Compliance-Bewertungen, die nicht auf vorhandenen Standardunterlagen beruhen;
c) die Unterstützung bei Datenschutz-Folgenabschätzungen und behördlichen Konsultationen, einschließlich Workshops, Fragebögen, Nachweisen und ergänzenden technischen Prüfungen;
d) die Beantwortung individueller Audit- und Fragekataloge des Auftraggebers sowie die Mitwirkung bei Vor-Ort- oder Remote-Audits; darüber hinausgehende Folgemaßnahmen (z. B. Tests, Nachbesserungsberichte), soweit sie nicht auf einem Verstoß des Auftragnehmers beruhen;
e) die Umsetzung individueller Weisungen des Auftraggebers, soweit sie mit zusätzlichem Aufwand verbunden sind (z. B. Sonderberichte, besondere Lösch- oder Aufbewahrungsanforderungen, abweichende Protokollierungen);
f) Datenbereitstellungen in besonderen, nicht standardmäßig unterstützten Formaten, inklusive Mapping und Verifikation;
g) Leistungen außerhalb der üblichen Geschäftszeiten des Auftragnehmers.
(4) Vergütungssätze und Abrechnung
a) Unterstützungsleistungen nach Abs. 3 werden nach Aufwand zu einem Stundensatz von 100.- EUR zzgl. gesetzlicher Umsatzsteuer vergütet. Abrechnung in Einheiten von 15 Minuten; Mindestabrechnung 15 Minuten je Vorgang.
b) Übliche Geschäftszeiten sind Montag-Freitag, 8:00-16:00 Uhr, lokale Zeit des Auftragnehmers, gesetzliche Feiertage ausgenommen. Einsätze außerhalb dieser Zeiten werden mit einem Zuschlag von 25 % (Nacht/Wochenende 50%) berechnet.
c) Reisezeiten werden mit 50% des Stundensatzes berechnet; Reise- und Nebenkosten (z. B. Bahn/Flug, Hotel, Verpflegungspauschalen) werden gegen Nachweis erstattet. Vor-Ort-Einsätze erfolgen nur nach vorheriger Abstimmung.
d) Dritt- und Durchlaufkosten (z. B. Gebühren externer Gutachter, Übersetzungen, spezielle Zertifikate) trägt der Auftraggeber

nach vorheriger Freigabe.
(5) Kostenvoranschlag, Freigabe und Eilfälle
a) Vor Beginn vergütungspflichtiger Unterstützungsleistungen übermittelt der Auftragnehmer dem Auftraggeber einen Kostenvoranschlag mit Leistungsbeschreibung und voraussichtlichem Aufwand. Der Auftragnehmer beginnt erst nach Freigabe durch den Auftraggeber.
b) Eilfälle: Soweit zur Einhaltung gesetzlicher Fristen (insb. Art. 33/34 DSGVO) sofortiges Handeln erforderlich ist und eine rechtzeitige Freigabe nicht eingeholt werden kann, ist der Auftragnehmer berechtigt, ohne vorherige Freigabe Unterstützungsleistungen bis zu einem Aufwand von maximal 2 Stunden zu erbringen. Der Auftragnehmer informiert den Auftraggeber unverzüglich und holt die Freigabe für weiteren Aufwand nach.
c) Der Auftragnehmer informiert den Auftraggeber, sobald absehbar ist, dass der freigegebene Aufwand überschritten wird, und holt eine Nachfreigabe ein.
(6) Auditspezifische Regelungen
a) Der Auftragnehmer darf zur Reduzierung des Aufwands zunächst aktuelle unabhängige Prüfberichte/Zertifikate (z. B. ISO 27001, SOC 2) sowie standardisierte Nachweise bereitstellen.
b) Ein vom Auftraggeber initiierter Vor-Ort-Audit pro Kalenderjahr und Standort ist zulässig; der dabei beim Auftragnehmer entstehende Aufwand wird gemäß Abs. 4 vergütet, sofern keine Abweichungen/Verstöße des Auftragnehmers festgestellt werden. Bei festgestellten wesentlichen Verstößen trägt der Auftragnehmer den eigenen Aufwand zur Abhilfe.
(7) Kein Entgelt bei Verursachung durch den Auftragnehmer
Aufwendungen, die ausschließlich dadurch entstehen, dass der Auftragnehmer gegen diesen Vertrag, gegen dokumentierte Weisungen des Auftraggebers oder gegen anwendbare Datenschutzvorschriften verstoßen hat, sind vom Auftragnehmer zu tragen. Gleiches gilt für Unterstützungsleistungen zur Behebung von vom Auftragnehmer zu vertretenden Sicherheitsmängeln.
(8) Zahlungsbedingungen
Vergütungspflichtige Unterstützungsleistungen werden monatlich nachträglich abgerechnet. Rechnungen sind innerhalb von 14 Tagen nach Zugang ohne Abzug zur Zahlung fällig.
(9) Keine Einschränkung gesetzlicher Pflichten
Die vorstehenden Vergütungsregelungen lassen die Pflicht des Auftragnehmers unberührt, den Auftraggeber im gesetzlich erforderlichen Umfang und fristgerecht zu unterstützen. Eine gesetzlich gebotene Unterstützung wird nicht wegen offener Vergütungen zurückgehalten; die Abrechnung erfolgt in diesem Fall nachträglich.
(10) Transparenz und Nachweis
Der Auftragnehmer dokumentiert Art, Umfang und Dauer der erbrachten Unterstützungsleistungen nachvollziehbar und stellt dem Auftraggeber auf Anforderung geeignete Tätigkeitsnachweise zur Verfügung.

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 3 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. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. 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) Der Vertrag beginnt mit Unterzeichnung bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.
(2) 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 ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren.

17. Meldung von Verletzungen des Schutzes personenbezogener Daten (Vorfallmeldung)
(1) Eine Verletzung des Schutzes personenbezogener Daten (Datenpanne) ist ein Verstoß gegen die Sicherheit, der zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO). Diese Regelung gilt auch bei entsprechenden Vorfällen bei Unterauftragnehmern sowie bei Sicherheitsvorfällen, die voraussichtlich Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit der im Auftrag verarbeiteten personenbezogenen Daten haben.
(2) Meldefristen und Kommunikationswege
a) Der Auftragnehmer informiert den Auftraggeber unverzüglich und ohne unangemessene Verzögerung, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung vom Vorfall.
b) Meldungen erfolgen an die vom Auftraggeber benannte Email-Adresse.
c) Ist der Auftragnehmer aufgrund gesetzlicher Vorgaben vorübergehend an der Information gehindert, informiert er den Auftraggeber, sobald das rechtlich zulässig ist, und teilt den Grund der Verzögerung mit.
(3) Mindestinhalte der Erstmeldung nach Art. 33 Abs. 3 DSGVO
Die Erstmeldung enthält mindestens:
- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Zeitpunkt der Entdeckung und, soweit feststellbar, den mutmaßlichen Zeitpunkt/Zeitraum des Vorfalls;
- den betroffenen Verarbeitungsprozess/die betroffenen Systeme und etwaig involvierte Unterauftragnehmer;
- den Namen und die Kontaktdaten der Ansprechperson bzw. des Datenschutzbeauftragten beim Auftragnehmer;
- die wahrscheinlichen Folgen der Verletzung für die betroffenen Personen und für den Auftraggeber;
- eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen, einschließlich Sofortmaßnahmen zur Eindämmung.
(4) Fortlaufende Information und Nachmeldungen
a) Soweit zum Zeitpunkt der Erstmeldung noch nicht alle Informationen vorliegen, übermittelt der Auftragnehmer fehlende Informationen unverzüglich nach, sobald sie verfügbar sind.
b) Der Auftragnehmer informiert den Auftraggeber bis zur Eindämmung des Vorfalls in angemessenen Intervallen über den Status (z. B. täglich oder nach wesentlichen Erkenntnissen/Meilensteinen).
c) Spätestens innerhalb von 10 Werktagen nach Eindämmung übermittelt der Auftragnehmer einen Abschlussbericht mit Ursachenanalyse, getroffenen Abhilfemaßnahmen und Maßnahmen zur Vermeidung künftiger gleichartiger Vorfälle.
(5) Untersuchungs-, Mitwirkungs- und Abhilfepflichten
a) Der Auftragnehmer nimmt unverzüglich eine Untersuchung des Vorfalls vor, ergreift alle angemessenen Maßnahmen zur Eindämmung, Behebung und Verhinderung weiterer Beeinträchtigungen und arbeitet eng mit dem Auftraggeber zusammen.
b) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO, einschließlich der Bereitstellung aller hierfür erforderlichen Informationen, der Formulierung behördlicher Meldungen und von Benachrichtigungen an betroffene Personen sowie der Beantwortung von Rückfragen der Aufsichtsbehörden.

c) Der Auftragnehmer stellt auf Anfrage Details zur Art der betroffenen Daten (einschließlich etwaiger besonderer Kategorien nach Art. 9 DSGVO), eingesetzter Schutzmechanismen (z. B. Verschlüsselung, Pseudonymisierung), betroffenen Datenmengen, Exfiltrationsindikatoren und Logdaten zur Verfügung, soweit rechtlich zulässig.
(6) Unterauftragnehmer
a) Tritt der Vorfall bei einem Unterauftragnehmer auf, stellt der Auftragnehmer sicher, dass der Unterauftragnehmer den Auftragnehmer unverzüglich informiert und alle zur Vorfallbearbeitung erforderlichen Informationen bereitstellt.
b) Der Auftragnehmer bleibt gegenüber dem Auftraggeber zentraler Ansprechpartner und koordiniert die Kommunikation.
(7) Behörden- und Betroffenenkommunikation
a) Der Auftragnehmer nimmt in seiner Rolle als Auftragsverarbeiter ohne dokumentierte Weisung des Auftraggebers keine Meldung an Aufsichtsbehörden und keine Benachrichtigung betroffener Personen vor, es sei denn, er ist hierzu zwingend gesetzlich verpflichtet. In diesem Fall informiert er den Auftraggeber vorab, soweit rechtlich zulässig, oder unverzüglich danach.
b) Presse- und Öffentlichkeitsarbeit zum Vorfall erfolgt nur in Abstimmung mit dem Auftraggeber, soweit rechtlich zulässig.
(8) Beweissicherung, Vertraulichkeit und Minimierung
a) Der Auftragnehmer trifft angemessene Maßnahmen zur Beweissicherung (z. B. Sicherung relevanter Log- und Systemdaten) und stellt sicher, dass die Untersuchung die Integrität der Beweise wahrt.
b) Alle im Zusammenhang mit dem Vorfall erhaltenen Informationen behandelt der Auftragnehmer vertraulich und nutzt sie ausschließlich zur Vorfallbearbeitung und zur Erfüllung gesetzlicher Pflichten.
c) Offenlegungen an Dritte erfolgen ausschließlich, soweit zur Vorfallbearbeitung erforderlich oder gesetzlich vorgeschrieben, und nach vorheriger Information des Auftraggebers, soweit zulässig.
(9) Dokumentation und Aufbewahrung
a) Der Auftragnehmer dokumentiert jeden Vorfall gemäß Art. 33 Abs. 5 DSGVO so, dass dem Auftraggeber die Überprüfung der Einhaltung seiner Pflichten ermöglicht wird. Die Dokumentation umfasst insbesondere den Hergang, die Auswirkungen, die ergriffenen Maßnahmen und die Kommunikationsschritte.
b) Die Vorfalldokumentation wird für mindestens 3 Jahre oder länger, sofern gesetzlich erforderlich oder vertraglich vereinbart, aufbewahrt und dem Auftraggeber auf Anfrage zur Einsicht bereitgestellt.
(10) Keine Einschränkung gesetzlicher Pflichten
Diese Regelung lässt strengere gesetzliche Meldefristen oder -inhalte unberührt. Der Auftragnehmer wird Informationen nicht wegen offener Vergütungsfragen zurückhalten; eine etwaige Vergütung richtet sich nach der gesonderten Vergütungsregelung.

18. 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.

19. Haftung
(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 und 4 DSGVO gemeinsam für den materiellen und immateriellen Schaden, den eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind für einen solchen Schaden sowohl der Auftraggeber als auch der Auftragnehmer verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung für den Schaden entspricht.

20. 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) Für Nebenabreden ist die Schriftform erforderlich.
(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlagen

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung
Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Verarbeitung und Speicherung von personenbezogenen Daten, die im Rahmen von Wertermittlungen erhoben werden, die durch den Auftraggeber über die Internetplattform des
Auftragnehmers erfolgen. Dabei werden Daten wie Anschriften, Wohnorte oder Daten zu Immobilien erhoben, die in direktem oder indirekten Zusammenhang mit einer natürlichen Person stehen.

2. Art(en) der personenbezogenen Daten
Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:
- Personenbezogene Daten des Auftraggebers (Vor- und Zuname, Straße, Hausnummer, Postleitzahl, Ort, Land, Telefon, Fax, Email, Vertragsverhältnis, Kundenhistorie, Vertragsabrechnungs- und Zahlungsinformationen)
- Personenbezogene Daten von Dritten, die in direktem oder indirekten Zusammenhang mit der Bewertung einer Immobilien stehen (Vor- und Zuname, Straße, Hausnummer, Postleitzahl, Ort, Land, Telefon, Fax, Email)
- Objektdaten wie Anschrift oder Wohnflächen, Fotos und ggf. andere Medien, die direkt oder indirekt einer natürlichen oder juristischen Person zuzuordnen sind.

3. Kategorien betroffener Person
Kreis der von der Datenverarbeitung betroffenen Personen:
Auftraggeber und Dritte.

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten ("Unterauftragnehmer").
Dabei handelt es sich um nachfolgende Unternehmen:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Standort der Verarbeitung: Deutschland
Art der erbringenden Leistung: Zurverfügungstellung von IT Infrastruktur und Hardware

Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Standort der Datenresidenz: Deutschland (Microsoft Rechenzentrum)
Standort der Verarbeitung: Europäische Union (Microsoft Rechenzentren innerhalb der EU Datenzone)
Art der erbringenden Leistung: Zurverfügungstellung von Anwendungen zur Verarbeitung mittels künstlicher Intelligenz im Rahmen der Azure Plattform. Verbot der Eigennutzung/Modelltrainings der übermittelten Daten.

Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

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

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

- mechanisches Schließsystem
- Protokollierung der Besucher (z.B. Besucherbuch)
- Besucherkontrolle am Eingang
- verschlossene Türen bei Abwesenheit

Zugangskontrolle
(Maßnahmen, die geeignet sind, unbefugten Personen die Benutzung von Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

- Authentifikation mit Benutzername + Passwort
- Verschlüsselung der Kommunikation mittels SSL-Verschlüsselung
- Verwaltung von Benutzerberechtigungen (z.B. bei Eintritt, Änderung, Austritt)
- Einsatz von Firewalls zum Schutz des Netzwerkes
- Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)
- Begrenzung von Fehlversuchen bei Anmeldungen
- Systemverwalterbefugnisse und -protokollierung
- Dunkelschaltung der Bildschirme mit Passwortschutz
- Einsatz von Anti-Viren-Software

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

- sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- sichere Aufbewahrung von Datenträgern
- Verwaltung der Rechte durch einen Systemadministrator

Trennungskontrolle
(Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

- softwareseitige, logische Mandantentrennung
- Trennung von Produktiv- und Testsystemen
- Datentrennung über Datenbankrechte

2. Integrität
Eingabekontrolle
(Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.)

- Verwendung von individuellen Benutzernamen zur Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen von Daten
- individuelle, personenbezogene Rechtevergabe zur Eingabe, Änderung und Löschung von Daten
- Protokollierung

Weitergabekontrolle
(Maßnahmen die 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 Einrichtungen zur Datenübertragung vorgesehen ist.)

- Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- Kryptographische Verschlüsselung der übertragenen Daten

3. Verfügbarkeit und Belastbarkeit
(Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- Einsatz von Firewalls sowie Antivirensoftware zum Schutz vor Viren/Malware
- Nutzung eines Backup- & Wiederherstellungskonzepts
- Nutzung/Verwendung eines Notfallplanes bei IT Ausfällen ganzer oder einzelner Komponenten
- Feuer- und Rauchmeldeanlagen
- CO2 Feuerlöschgeräte in Serverräumen
- Klimatisierung in Serverräumen
- Überwachung von Feuchtigkeit und Temperatur in Serverräumen
- Mehrfachanbindung der Server über verschiedene Peeringpoints
- redundante Datenhaltung (z.B. durch RAID1 gespiegelte Festplatten und gespiegelte Server)
- redundante USV Stromversorgung in Serverräumen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Verpflichtung aller Mitarbeiter auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO
- Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Durchführung regelmäßiger interner Audits