Bedingungen zur Auftragsverarbeitung „immoprofessional“

Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem Kunden als Verantwortlichem (nachfolgend „Kunde“)

und der WebsitesCreator GmbH, Lindenbreede 72, 49124 Georgsmarienhütte, als Auftragsverarbeiter (nachfolgend „Auftragnehmer“).

1. Gegenstand und Dauer

1.1 Der Auftragnehmer stellt dem Kunden die Immobiliensoftware immoprofessional als Online-Dienst bereit (Hauptvertrag). Dabei verarbeitet er personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag gilt auch für einen kostenlosen Testzugang.

1.2 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

2.1 Zweck der Verarbeitung ist die Erbringung der Leistungen nach dem Hauptvertrag. Dazu gehören insbesondere Objektverwaltung, CRM mit E-Mail-Client, Exposé-Erstellung, Portalschnittstellen, die Website des Kunden mit Anfrageformularen, KI-Funktionen und Support sowie auf Wunsch Domains und Exchange-Postfächer. Die Verarbeitung umfasst insbesondere das Erheben, Speichern, Sichern, Abfragen, Verarbeiten mit KI-Funktionen, Übermitteln an vom Kunden bestimmte Empfänger (z. B. Immobilienportale) und Löschen.

2.2 Art der Daten: Kontakt- und Stammdaten (z. B. Name, Anschrift, Telefonnummer, E-Mail-Adresse), Such- und Interessentenprofile, Kommunikationsinhalte (E-Mails, Anfragen, Notizen), Termine, Einwilligungsnachweise, Objektdaten mit Personenbezug einschließlich Bildern und Dokumenten, Zugangs- und Protokolldaten der Nutzer sowie Verbindungsdaten der Websitebesucher (z. B. IP-Adresse).

2.3 Betroffene Personen: Interessenten, Käufer, Mieter und Feriengäste, Eigentümer, Verkäufer und Vermieter, sonstige Kontakte und Geschäftspartner des Kunden, Besucher der Website des Kunden sowie Beschäftigte und sonstige Nutzer des Kunden.

3. Weisungen

3.1 Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung in ein Drittland, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats dazu verpflichtet. In diesem Fall teilt er dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Weisungen sind dieser Vertrag, der Hauptvertrag und die Nutzung der Funktionen von immoprofessional durch den Kunden. Einzelweisungen erteilt der Kunde in Textform.

3.3 Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Kunden unverzüglich.

3.4 Der Auftragnehmer verarbeitet die Daten nicht für eigene Zwecke, insbesondere nicht zum Training oder zur Verbesserung von KI-Modellen. Er setzt nur KI-Dienste ein, deren Anbieter die Daten weder für eigene Zwecke, insbesondere zum Training, verwenden noch über die Bearbeitung der jeweiligen Anfrage hinaus speichern. Mit KI-Funktionen werden Daten nur

verarbeitet, wenn ein Nutzer des Kunden eine solche Funktion auslöst oder der Kunde sie in den Einstellungen aktiviert hat.

4. Vertraulichkeit und Sicherheit

4.1 Der Auftragnehmer setzt nur Personen ein, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.2 Er trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen gemäß Anlage 1. Er darf sie an den technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird.

5. Unterauftragsverarbeiter

5.1 Der Kunde erteilt die allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Unterauftragsverarbeiter). Die in Anlage 2 genannten Unterauftragsverarbeiter gelten als genehmigt.

5.2 Der Auftragnehmer informiert den Kunden mindestens 30 Tage vorher in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Kunde kann der Änderung innerhalb von 14 Tagen nach Zugang der Information in Textform widersprechen. Widerspricht er nicht fristgerecht, gilt die Änderung als genehmigt. Widerspricht er, kann jede Partei den Hauptvertrag zum Zeitpunkt der beabsichtigten Änderung kündigen.

5.3 Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Kunden für deren Einhaltung.

5.4 Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

6. Unterstützung des Kunden

6.1 Der Auftragnehmer unterstützt den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III DSGVO. Anträge, die sich an ihn richten, leitet er unverzüglich an den Kunden weiter.

6.2 Er unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO. Eine Verletzung des Schutzes personenbezogener Daten meldet er dem Kunden unverzüglich, nachdem sie ihm bekannt wurde.

7. Löschung und Rückgabe

Nach Abschluss der Leistungen löscht der Auftragnehmer alle personenbezogenen Daten des Kunden oder gibt sie nach Wahl des Kunden zurück, sofern nicht nach dem Recht der Union oder eines Mitgliedstaats eine Pflicht zur Speicherung besteht. Der Kunde kann seine Daten bis zum Vertragsende mit den Exportfunktionen der Software sichern oder die Rückgabe in Textform verlangen. Im Übrigen löscht der Auftragnehmer die Daten innerhalb von 30 Tagen nach Vertragsende. Datensicherungen werden mit Ablauf ihrer Aufbewahrungsfrist überschrieben.

8. Nachweise und Überprüfungen

8.1 Der Auftragnehmer stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen einschließlich Inspektionen, die vom Kunden oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer durchgeführt werden, und trägt dazu bei.

8.2 Anstelle einer Inspektion kann der Auftragnehmer die Einhaltung seiner Pflichten durch geeignete andere Nachweise belegen, insbesondere durch aktuelle Prüfberichte oder Testate unabhängiger Stellen, Zertifizierungen nach Art. 42 DSGVO, die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder einen schriftlichen Bericht seines Datenschutzbeauftragten. Eine Inspektion ist dann nur zulässig, soweit diese Nachweise im Einzelfall nicht ausreichen, insbesondere bei konkreten Anhaltspunkten für einen Verstoß gegen diesen Vertrag.

8.3 Inspektionen sind vorher anzukündigen und während der üblichen Geschäftszeiten ohne vermeidbare Störung des Betriebs durchzuführen.

9. Vertragsschluss und Vorrang

9.1 Dieser Vertrag kommt zustande, indem der Kunde ihn im Bestell- oder Registrierungsprozess durch Anklicken der vorgesehenen Checkbox bestätigt. Er ist damit in elektronischer Form nach Art. 28 Abs. 9 DSGVO abgeschlossen. Der Auftragnehmer stellt ihn zum Abruf und Speichern bereit.

9.2 Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.

10. Änderungen dieser Bedingungen

10.1 Der Auftragnehmer kann diese Bedingungen ändern, soweit dies wegen einer Änderung der Rechtslage, der Rechtsprechung oder behördlicher Vorgaben oder wegen einer Änderung der Leistungen nach dem Hauptvertrag erforderlich ist. Die Änderung darf das Schutzniveau für die personenbezogenen Daten nicht absenken und die Rechte des Kunden aus Art. 28 DSGVO nicht einschränken.

10.2 Der Auftragnehmer teilt dem Kunden die Änderungen mindestens vier Wochen vor ihrem Wirksamwerden in Textform mit. Sie gelten als genehmigt, wenn der Kunde nicht bis zu ihrem Wirksamwerden in Textform widerspricht. Auf diese Folge weist der Auftragnehmer in der Mitteilung besonders hin. Widerspricht der Kunde, gelten die bisherigen Bedingungen fort und jede Partei kann den Hauptvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

10.3 Für den Wechsel von Unterauftragsverarbeitern gilt Ziffer 5.2, für die Anpassung der technischen und organisatorischen Maßnahmen Ziffer 4.2.

11. Schlussbestimmungen

11.1 Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung tritt die gesetzliche Regelung.

11.2 Ist der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag der Sitz des Auftragnehmers.

Anlagen

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 2: Unterauftragsverarbeiter

Stand: 03.11.2026

ANLAGE 1 zu den Bedingungen zur Auftragsverarbeitung „immoprofessional“

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 03.11.2026

1. Vertraulichkeit

Maßnahme	Ausführung
Postfachzugänge	Verschlüsselt und authentifiziert gespeichert (XSalsa20-Poly1305). Der Schlüssel liegt außerhalb der Datenbank und der Versionsverwaltung. Die Zugangsdaten werden nicht angezeigt und nicht protokolliert.
Kennwörter	Ausschließlich als nicht umkehrbarer Prüfwert (Argon2id). Neue Benutzer setzen ihr Kennwort selbst über einen Einmal-Link.
Anmeldung	Fehlgeschlagene Anmeldeversuche werden begrenzt, nach Fehlversuchen wird die Anmeldung vorübergehend gesperrt. Zwei-Faktor-Authentifizierung steht allen Nutzern zur Verfügung.
Transportverschlüsselung	HTTPS für Anwendung und KI-Dienste, IMAP und SMTP über TLS zum Postfach. Die Datenbankverbindung ist auf TLS gezwungen und wird nach dem Verbindungsaufbau überprüft.
Speicherverschlüsselung	Datenbank und Dateien liegen auf verschlüsselten Datenträgern
Rechteprüfung	Berechtigungen werden in der Verarbeitung selbst geprüft, nicht nur in der Bildschirmmaske. Sitzungscookies mit HttpOnly, Secure und SameSite im strengen Modus.
Administrativer Zugang	Zugang zu Servern und Datenbank haben nur namentlich festgelegte Administratoren, ausschließlich über Schlüsselverfahren oder mit zweitem Faktor. Administrative Zugriffe werden protokolliert und 90 Tage aufbewahrt.
Supportzugriff	Beschäftigte des Auftragnehmers greifen auf Daten eines Kunden nur zu, soweit dies zur Bearbeitung einer Anfrage des Kunden oder zur Behebung einer Störung erforderlich ist. Jeder solche Zugriff wird mit Anlass protokolliert.
Verpflichtung der Personen	Schriftliche Verpflichtung jeder Person mit Zugriffsmöglichkeit vor Einrichtung des Zugangs (Art. 28 Abs. 3 lit. b DSGVO).
Physischer Schutz	Die Anwendungsserver stehen in Rechenzentren der IONOS SE in Deutschland, die über eigene Zutrittskontrollen verfügen.

2. Trennung

Maßnahme	Ausführung
Mandantentrennung als Sperre	Die Datenbankzugriffsschicht weist jede Abfrage auf eine Tabelle mit Kundenbezug ab, die nicht auf die Kundennummer filtert. Kommentare werden vor der Prüfung entfernt. Ein kundenübergreifender Zugriff muss ausdrücklich und mit hinterlegter Begründung angemeldet werden.

Maßnahme	Ausführung
Nachweis	Automatisierte Prüfsammlung zu Mandantentrennung, Rechteprüfung und Löschung. Der Löschtest prüft jede Anweisung gegen die Sperre, sodass eine nicht eingetragene Tabelle auffällt.

3. Integrität, Verfügbarkeit und Belastbarkeit

Maßnahme	Ausführung
Datenbankzugriff	Ausschließlich vorbereitete Abfragen.
Aufspielen neuer Fassungen	Über Schlüsselverfahren mit Prüfsummenvergleich. Zugangsdaten außerhalb der Versionsverwaltung.
Aktualisierungen	Sicherheitsupdates für Betriebssystem, Webserver, Datenbank und Programmbibliotheken werden zeitnah eingespielt, kritische Lücken unverzüglich. Die Programmbibliotheken werden automatisiert auf bekannte Schwachstellen geprüft.
Netzwerkschutz	Von außen sind nur die für den Betrieb erforderlichen Dienste erreichbar, alle übrigen Zugänge sind durch eine Firewall gesperrt. Administrative Zugänge sind auf feste IP-Adressen oder VPN beschränkt.
Schutz vor Schadsoftware	Die Arbeitsplatzrechner der Beschäftigten erhalten automatische Sicherheitsupdates und sind mit Schadsoftwareschutz ausgestattet.
Sicherungen	Nächtlich und automatisiert auf zwei bei der IONOS SE gemietete Root-Server, auf die ausschließlich der Auftragnehmer Zugriff hat. Sie stehen in Berlin, in einem anderen Rechenzentrum als die Anwendungsserver, sodass der Ausfall eines Rechenzentrums die Sicherungen nicht miterfasst. Verschlüsselt übertragen und verschlüsselt gespeichert. Aufbewahrung sieben Tage, danach Überschreiben. Wiederherstellung erprobt und dokumentiert.
Monatssicherungen	Einmal im Monat wird zusätzlich eine Sicherung heruntergeladen und auf einer gesonderten Festplatte mit vollständiger Laufwerksverschlüsselung (BitLocker) gespeichert, die im Tresor der Hausbank des Auftragnehmers verwahrt wird. Aufbewahrung höchstens 12 Monate, danach endgültige Löschung.
Belastbarkeit	Erreichbarkeit und Auslastung der Server werden laufend überwacht, bei Störungen erfolgt eine automatische Benachrichtigung. Schutz gegen Überlastangriffe durch den Infrastrukturanbieter.
Fehlerprotokoll	Außerhalb des über das Netz erreichbaren Verzeichnisses. Enthält Kennzahlen und Meldungen, keine Inhalte aus Nachrichten oder Dokumenten.

4. Überprüfung, Fristen und Organisation

Maßnahme	Ausführung
Prüfläufe	Prüfsammlungen zu Mandantentrennung, Rechteprüfung, Löschfristen und Datenausleitung laufen bei jeder Änderung.
Fristensteuerung	Ein täglicher Vorgang entfernt, was seine Frist überschritten hat. Der Tagesmerker wird erst nach fehlerfreiem Lauf gesetzt. Für Tabellen mit gesetzlicher Aufbewahrungspflicht lässt sich keine Frist eintragen.
Löschfristen der Protokolle	Anmeldeversuche mit IP-Adresse 90 Tage, Versandprotokoll der Systemnachrichten 365 Tage, Einmal-Links 7 Tage, Zugriffsprotokolle der Webserver einschließlich der Websites der Kunden 30 Tage.

Maßnahme	Ausführung
KI-Modelle	Eingaben und Ergebnisse werden beim Anbieter der KI-Dienste nicht über die Bearbeitung der Anfrage hinaus gespeichert und nicht zum Training verwendet. Eine Protokollierung der Modellaufrufe mit Inhalten ist nicht eingerichtet. Vor einem Wechsel des KI-Modells wird geprüft, ob diese Zusagen unverändert gelten.
Organisation	Dokumentiertes Berechtigungskonzept, Verfahren für Betroffenenanfragen (Weiterleitung an den Kunden), Meldeverfahren nach Art. 33 Abs. 2 DSGVO und schriftliches Löschkonzept.

ANLAGE 2 zu den Bedingungen zur Auftragsverarbeitung „immoprofessional“

Unterauftragsverarbeiter

Stand: 03.11.2026

Der Auftragnehmer setzt die folgenden Unterauftragsverarbeiter ein (Ziffer 5.1):

Nr.	Unterauftragsverarbeiter	Gegenstand der Leistung	Ort der Verarbeitung
1	IONOS SE Elgendorfer Straße 57 56410 Montabaur Deutschland	Bereitstellung der Serverinfrastruktur für den Betrieb von immoprofessional (Anwendung, Datenbanken, Dateien und Websites der Kunden) sowie der Server für die Datensicherungen	Deutschland
2	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg Luxemburg	Bereitstellung von KI-Diensten für die KI-Funktionen von immoprofessional (insbesondere Texterstellung, Übersetzung und Bildanalyse)	Deutschland (Region Frankfurt am Main)
3	QualityHosting GmbH Uferweg 40-42 63571 Gelnhausen Deutschland	Betrieb von Microsoft-Exchange-Servern (E-Mail-Postfächer, Kalender und Kontakte) für Kunden, die diese Leistung buchen	Deutschland
4	InterNetX GmbH Johanna-Dachs-Straße 55 93055 Regensburg Deutschland	Registrierung und Verwaltung der Domains der Kunden	Deutschland
5	Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown, Dublin 18 Irland	Microsoft 365 für E-Mail, Kommunikation und Büroanwendungen des Auftragnehmers, insbesondere bei der Bearbeitung von Supportanfragen	EU
6	Google Cloud EMEA Limited 70 Sir John Rogerson's Quay Dublin 2 Irland	Bereitstellung von KI-Diensten über Google Cloud Vertex AI für die KI-Funktionen von immoprofessional (insbesondere Texterstellung, Übersetzung und Bildanalyse)	EU

Die Unterauftragsverarbeiter zu Nr. 2, Nr. 5 und Nr. 6 gehören zu Konzernen mit Sitz in den USA. Soweit dadurch ein Zugriff aus einem Drittland möglich ist, erfolgt er nur unter den Voraussetzungen der Art. 44 ff. DSGVO.