Vertrag zur Auftrags-verarbeitung

Stand 14.11.2026 immoGenio GmbH, Offenbach am Main

Lesezeit rund 8 Minuten

Fassung: 2026-11-1 vom 14. November 2026

zwischen dem **Kunden**, der das immoGenio Cockpit nutzt („Verantwortlicher“), und der **immoGenio GmbH**, Am Park 10, 63075 Offenbach am Main („Auftragsverarbeiter“).

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen das immoGenio Cockpit als Software zur Verwaltung von Immobilien bereit, samt den Zugängen für Eigentümer, Mieter, Hausmeister und Dienstleister des Verantwortlichen.

(2) Der Vertrag gilt, solange der Verantwortliche das Cockpit nutzt, einschließlich der Testphase, des Lesezugriffs und der Sperre nach Vertragsende (AGB § 4 Abs. 4), bis zur Löschung nach § 7.

§ 2 Art der Daten und Kreis der Betroffenen

(1) Betroffen sind Eigentümer, Mieter und Bewohner, Interessenten, Dienstleister und Hausmeister, Beiräte, Mitarbeiter des Verantwortlichen sowie Personen, die dem Verantwortlichen schreiben oder ihn anrufen.
(2) Verarbeitet werden insbesondere Namen, Anschriften und Kontaktdaten; Vertrags-, Objekt- und Einheitsdaten; Bankverbindungen, Kontoumsätze, Sollstellungen und Zahlungen; Verbrauchs- und Zählerdaten; Belege, Dokumente und Fotos; E-Mails, Nachrichten und Gesprächsmitschriften; Beschlüsse und Abstimmungen; Zugangs- und Protokolldaten.

§ 3 Zweck

Die Daten werden ausschließlich verarbeitet, um dem Verantwortlichen die Funktionen des Cockpits bereitzustellen: Stammdaten, Buchhaltung, Abrechnungen, Wirtschaftspläne, Versammlungen, Vermietung, Kommunikation, Aufgaben, Dokumente, Zähler und die Zugänge der Beteiligten.

§ 4 Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung in ein Drittland, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten dazu verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet. Als Weisung gelten die Einstellungen und Handlungen des Verantwortlichen und seiner Nutzer in der Anwendung.
(2) Hält der Auftragsverarbeiter eine Weisung für einen Verstoß gegen Datenschutzvorschriften, informiert er den Verantwortlichen unverzüglich.

§ 5 Pflichten des Auftragsverarbeiters

(1) Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.
(2) Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.
(3) Die Daten werden auf Servern in der Europäischen Union gespeichert (Rechenzentrum „Hub Europe“ der Contabo GmbH in Lauterbourg, Frankreich). Eine Übermittlung in Drittländer findet nur bei den in Anlage 2 so gekennzeichneten Diensten statt; sie stützt sich auf die Standarddatenschutzklauseln der Europäischen Kommission (Art. 46 Abs. 2 lit. c DSGVO).
(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei Anträgen betroffener Personen nach Kapitel III DSGVO — insbesondere mit Auskunft, Berichtigung, Löschung und Export in der Anwendung — sowie bei den Pflichten nach Art. 32 bis 36 DSGVO.
(5) Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er sie dem Verantwortlichen unverzüglich.

§ 6 Weitere Auftragsverarbeiter

(1) Der Verantwortliche genehmigt die in Anlage 2 genannten weiteren Auftragsverarbeiter. Der Auftragsverarbeiter erlegt ihnen vertraglich dieselben Datenschutzpflichten auf; kommt ein weiterer Auftragsverarbeiter ihnen nicht nach, haftet der Auftragsverarbeiter dem Verantwortlichen für dessen Pflichten.
(2) Über jede beabsichtigte Hinzuziehung oder Ersetzung unterrichtet der Auftragsverarbeiter den Verantwortlichen vorab per E-Mail und auf www.immogenio.de/sicherheit/; der Verantwortliche kann innerhalb von 30 Tagen Einspruch erheben.
(3) Dienste, mit denen der Verantwortliche selbst einen Vertrag schließt und deren Zugang er in der Anwendung hinterlegt (etwa SMS-, Brief-, Video- oder

Signaturdienste, ein eigener Bankzugang oder ein eigener KI-Assistent), sind keine weiteren Auftragsverarbeiter dieses Vertrags.

§ 7 Löschung und Rückgabe

(1) Nach Ende des Vertrags kann der Verantwortliche seine Daten einen Monat lang einsehen und exportieren; danach ist der Zugang gesperrt. Wählt der Verantwortliche binnen drei Monaten nach Vertragsende keinen Tarif, löscht der Auftragsverarbeiter die Daten, soweit keine gesetzliche Aufbewahrungspflicht besteht, und bestätigt dies auf Verlangen. Auf Verlangen löscht er früher. Der Verantwortliche kann sein Konto jederzeit selbst löschen; die Löschung wirkt sofort.

(2) Verschlüsselte Datensicherungen, die vor einer Löschung entstanden sind, enthalten die Daten bis zum Ablauf ihrer Aufbewahrung — tägliche Stände 30 Tage, wöchentliche 12 Wochen, monatliche 120 Monate. Sie werden nur zur Wiederherstellung nach einem Ausfall verwendet; gelöschte Daten werden daraus nicht zurückgespielt.

§ 8 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind, und ermöglicht Überprüfungen — einschließlich Inspektionen — durch den Verantwortlichen oder einen von ihm beauftragten Prüfer, nach Anmeldung mit angemessener Frist.

§ 9 Schlussbestimmungen

(1) Dieser Vertrag geht bei der Verarbeitung personenbezogener Daten den AGB vor.

(2) Er wird elektronisch geschlossen (Art. 28 Abs. 9 DSGVO).

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Ziel	Maßnahme
Verschlüsselung	Datenträger mit Datenbank, Dokumenten und Zwischenspeicher verschlüsselt (LUKS2, AES-256); der Schlüssel kommt beim Start von einem zweiten Server. Verbindungen nach außen nur per HTTPS mit HSTS; zwischen den Servern WireGuard. Zugangsdaten zu Banken und Schnittstellen einzeln verschlüsselt (AES-256-GCM).
Vertraulichkeit, Zugang	Anmeldung über einen selbst betriebenen Anmeldedienst mit Passkey oder Passwort, zweiter Faktor wählbar, begrenzte Fehlversuche; Anmeldelinks 15 Minuten gültig und einmalig. Serverzugang nur per SSH-Schlüssel. Zugriffsprotokolle des Webservers ohne IP-Adresse.
Trennung	Trennung je Mandant in der Datenbank (Row-Level-Security); Rollen, Rechte und Objektgrenzen je Mandant; ein angebundener KI-Assistent höchstens mit den Rechten des Nutzers. Testumgebung getrennt, mit bereinigter Kopie (E-Mail-Adressen, Telefonnummern und Bankverbindungen ersetzt, Zugangsdaten geleert).
Integrität	Änderungen werden protokolliert; das Protokoll der Buchhaltung ist unveränderlich. Hochgeladene Dateien werden vor dem Ablegen auf Schadsoftware geprüft. Neue Fassungen gehen erst nach Prüfung auf der Testumgebung und Freigabe live.
Verfügbarkeit, Wiederherstellung	Tägliche verschlüsselte Sicherung in einen Speicher in der EU, Änderungen der Datenbank alle 15 Minuten; monatlicher automatischer Wiederherstellungstest; Überwachung der Dienste alle 30 Minuten; Messung der Verfügbarkeit jede Minute von einem zweiten Server aus.
Überprüfung	Sicherheitsreview des Programmcodes (zuletzt November 2026); diese Anlage wird bei jeder Änderung der Technik überprüft.

Anlage 2 — Weitere Auftragsverarbeiter

Auftragsverarbeiter	Leistung	Drittland
Top Gear Brains EOOD, 19 „27th July“ Str., 9000 Warna, Bulgarien	Betrieb der Plattform	nein
Contabo GmbH, München	Rechenzentrum „Hub Europe“ in Lauterbourg, Frankreich	nein
Cloudflare, Inc., San Francisco, USA	verschlüsselte Datensicherung in einem Speicher in der EU (Schlüssel nur beim Auftragsverarbeiter); Auslieferung der Oberflächen	ja — Standarddatenschutzklauseln, EU-US Data Privacy Framework
Mistral AI SAS, Paris, Frankreich	Lesen von Belegen, Zählerständen und Mängelfotos; Spracherkennung und -ausgabe des Telefonassistenten	nur über deren Unterauftragsverarbeiter, Standarddatenschutzklauseln
OpenRouter, Inc., New York, USA, mit TypeSafe AI, Inc., San Francisco, USA, und Anthropic, PBC, San Francisco, USA	Einordnung von E-Mails, Suche mit KI, Kontovorschlag und Beleglesung (AGB § 6 Abs. 4 bis 8); Gesprächsführung und Zusammenfassung des Telefonassistenten	ja — Standarddatenschutzklauseln
BANKSapi Technology GmbH, München; Enable Banking Oy, Espoo, Finnland	Abruf von Kontoumsätzen, wenn der Verantwortliche ein Bankkonto über diese Dienste verbindet	nein
easybell GmbH, Berlin	Telefonleitung des Telefonassistenten, wenn eingerichtet	nein

Auftragsverarbeiter	Leistung	Drittland
Meta Platforms Ireland Ltd., Dublin, Irland	WhatsApp-Nachrichten, wenn der Verantwortliche WhatsApp einschaltet	ja — Standarddatenschutzklauseln
apilayer GmbH, Wien, Österreich (OpenIBAN)	Bankname und BIC zu einer eingegebenen IBAN	nein
Descartes Technologies GmbH, Berlin (OpenRegister)	Suche nach Firmen im Handelsregister bei der Eingabe	nein
komoot GmbH, Schönefeld (Photon)	Adressvorschläge zu einer eingegebenen Anschrift, ohne IP-Adresse des Nutzers	nein
Push-Dienste der Browser (etwa Apple, Google, Mozilla)	Zustellung von Benachrichtigungen; ihr Inhalt ist Ende-zu-Ende verschlüsselt	Inhalt nicht lesbar