

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Stand 19.10.2026.

zwischen

dem Kunden der Profi-Immobilienwebsite, benannt in der Auftragsbestätigung, nachstehend „Auftraggeber“ genannt

und der

InnoBrain GmbH, Theaterstraße 26, 97070 Würzburg, nachstehend „Auftragnehmer“ genannt,

nachstehend gemeinsam die „Parteien“ genannt.

Präambel

Der Auftragnehmer stellt dem Auftraggeber nach den Allgemeinen Geschäftsbedingungen für die Profi-Immobilienwebsite (nachstehend „Hauptvertrag“) eine gehostete Website bereit. Dabei verarbeitet er im Auftrag des Auftraggebers weisungsgebunden personenbezogene Daten. Dies stellt eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO dar. Dieser liegen die Regelungen der DSGVO und des Bundesdatenschutzgesetzes (BDSG) zugrunde. Die vorliegende Vereinbarung regelt die ordnungsgemäße Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers. Der Verantwortliche für die Verarbeitung im Sinne des Art. 4 Nr. 7 sowie Art. 28 DSGVO ist der Auftraggeber. Die Anlage 1 „Weisungen, Weitere Auftragsverarbeiter, Art der Verarbeitung, Kreis der Betroffenen“ und die Anlage 2 „Technische und organisatorische Maßnahmen“ sind Bestandteil dieser Vereinbarung.

Diese Vereinbarung kommt mit dem Hauptvertrag in Textform zustande (Art. 28 Abs. 9 DSGVO). Sie ist Anlage 3 des Hauptvertrags.

1. Gegenstand und Dauer des Auftrags

a) Gegenstand des Auftrags

Gegenstand des Auftrags ist das Hosting und der Betrieb der Website des Auftraggebers auf der Plattform des Auftragnehmers nach dem Hauptvertrag. Dies umfasst die Speicherung und Auslieferung der vom Auftraggeber eingestellten Inhalte, die Verwaltung der Benutzerkonten des Redaktionssystems, die Übernahme von Objekt- und Ansprechpartnerdaten aus dem vom Auftraggeber angebundenen Immobilien-Verwaltungssystem, die Verarbeitung technischer Daten der Besucher der Website beim Abruf, die Datensicherung sowie die Wartung und Störungsbeseitigung. Nicht Gegenstand des Auftrags sind der Betrieb von E-Mail-Postfächern oder Mailservern des Auftraggebers, der Versand von E-Mails im Namen des Auftraggebers, die Verarbeitung durch den KI-Assistenten des Auftraggebers oder dessen Anbieter (Hauptvertrag § 4) sowie das Produktfeedback, das Benutzer des Redaktionssystems dem Auftragnehmer senden (Hauptvertrag § 18 Abs. 2). Die Verarbeitung der personenbezogenen Daten erfolgt durch den Auftragnehmer im Auftrag des Auftraggebers gemäß Art. 4 Nr. 2 und Art. 28 DSGVO.

b) Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags. Eine Kündigung oder sonstige Beendigung des Hauptvertrags bewirkt automatisch eine Beendigung der vorliegenden Vereinbarung. Das Recht zur fristlosen Kündigung dieser Vereinbarung aus wichtigem Grund bleibt für beide Parteien unberührt. Spätestens mit Beendigung dieses Auftrags werden sämtliche personenbezogenen Daten nach Wahl des Auftraggebers zurückgegeben oder gelöscht (Ziffer 9); die Fristen für Abruf und Löschung regelt der Hauptvertrag § 10.

2. Konkretisierung des Auftragsinhalts, Verantwortlichkeit

- a) Der Umfang, die Art und der Zweck der Verarbeitung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen sind in Anlage 1 beschrieben.
- b) Die Erbringung der vertraglich vereinbarten Datenverarbeitung durch den Auftragnehmer findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Die in Anlage 1 bezeichneten Drittlandbezüge der dort genannten Subunternehmer gelten als genehmigt.
- c) Der Auftraggeber ist im Rahmen dieses Vertrages insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie der Datenverarbeitung als solcher verantwortlich, also für die Frage, ob bestimmte Daten überhaupt rechtmäßig verarbeitet werden dürfen. Das gilt insbesondere für die Inhalte, die der Auftraggeber oder sein KI-Assistent auf der Website einstellt, für die Objekt- und Ansprechpartnerdaten aus seinem Immobilien-Verwaltungssystem sowie für die Informationspflichten gegenüber den Besuchern der Website.

3. Technisch-organisatorische Maßnahmen

- a) Die technischen und organisatorischen Maßnahmen des Auftragnehmers sind in Anlage 2 dokumentiert und mit Abschluss dieser Vereinbarung Grundlage des Auftrags. Ergibt eine Prüfung oder ein Audit des Auftraggebers Anpassungsbedarf, setzen die Parteien ihn einvernehmlich um.
- b) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten hierzu in Anlage 2).
- c) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

- a) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Der Auftraggeber kann Inhalte und Benutzerkonten seiner Website im Redaktionssystem selbst berichtigen, einschränken und löschen; insoweit bedarf es keiner Weisung an den Auftragnehmer.
- c) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen nachzukommen. Das gilt insbesondere für Anträge auf Auskunft,

Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch (Art. 15 bis 22 DSGVO). Anträge betroffener Personen leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter und beantwortet sie nur nach dessen dokumentierter Weisung.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Sofern der Auftragnehmer nach Art. 37 DSGVO zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, hat dieser seine Tätigkeit gemäß Art. 38 und 39 DSGVO auszuüben. Gemäß § 38 Abs. 1 Satz 1 BDSG ist der Auftragnehmer zum Zeitpunkt des Zustandekommens dieser Vereinbarung nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Die Benennung eines Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- b) Zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO: Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten hierzu in Anlage 2).
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages.
- i) Sollte eine Änderung der gesetzlichen Bestimmungen und/oder sollten Vorgaben von Regulierungsbehörden, wie z. B. der Europäischen Kommission oder der Datenschutzaufsichtsbehörden, eine Anpassung dieser vertraglichen Vereinbarungen erfordern, insbesondere im Hinblick auf die Vereinbarung von Bestimmungen zur Informationssicherheit, wie z. B. Meldepflichten, Schutzbedarfsfeststellungen etc., werden die Vertragsparteien sich umgehend zusammensetzen und bis spätestens zum Zeitpunkt des geplanten Inkrafttretens der geänderten gesetzlichen Bestimmung(en) den Vertrag einvernehmlich anpassen. Können sich die

Parteien nicht einigen und kann eine Anpassung des Vertrages oder die Erbringung der erforderlichen Leistung innert nützlicher Frist nicht gewährleistet oder erbracht werden, bleibt jeder Partei die außerordentliche Kündigung vorbehalten.

6. Kontrollrechte des Auftraggebers

- a) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner vertraglichen und gesetzlichen Pflichten als Auftragsverarbeiter zur Verfügung. Er gestattet und ermöglicht dem Auftraggeber und von ihm beauftragten Prüfern entsprechende Überprüfungen (einschließlich Inspektionen) in der Regel innerhalb der Servicezeiten nach Anlage 2 des Hauptvertrags und unterstützt hierbei. Sollte der von dem Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, steht dem Auftragnehmer ein Einspruchsrecht zu, das er jedoch nur unverzüglich ausüben kann.
- b) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Inspektion, hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber die Verpflichtungsvereinbarung mit dem Dritten unverzüglich vorzulegen.
- c) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- d) Faktoren für einen Nachweis für die Maßnahmen nach dem vorstehenden Absatz, die nicht nur den konkreten Auftrag betreffen, können insbesondere sein:
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).
- e) Der Nachweis für die Maßnahmen soll vorrangig durch die im vorstehenden Absatz aufgeführten Nachweise erbracht werden.

7. Unterstützung des Auftraggebers bei der Einhaltung datenschutzrechtlicher Verpflichtungen, Mitteilung bei Verstößen des Auftragnehmers

- a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Insbesondere verpflichtet sich der Auftragnehmer,
 - ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen, sicherzustellen;
 - den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen;
 - den Auftraggeber bei dessen Datenschutz-Folgenabschätzung zu unterstützen;
 - den Auftraggeber im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde zu unterstützen.

- b) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziffer 8 dieses Vertrages durchführen.

8. Weisungsbefugnis des Auftraggebers

- a) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (mind. Textform) bestätigen. Die Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

Die Weisungsberechtigten, Weisungsempfänger und die für Weisungen zu verwendenden Kommunikationsmittel ergeben sich aus Anlage 1. Die Nutzung der Website und des Redaktionssystems durch den Auftraggeber und seinen KI-Assistenten innerhalb des vertraglich vereinbarten Leistungsumfangs gilt als Weisung im Rahmen dieser Vereinbarung.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

- b) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung von Daten und Rückgabe von Datenträgern

- a) Der Auftragnehmer verarbeitet die Daten nur wie in dieser Vereinbarung beschrieben und nur zu den dort genannten Zwecken. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- b) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber (spätestens mit Beendigung dieser Vereinbarung) hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Die Aushändigung erfolgt durch den Datenexport nach dem Hauptvertrag § 10 und Anlage 1 Ziffer 10 des Hauptvertrags; ruft der Auftraggeber den Export innerhalb des Abrufzeitraums nicht ab, gilt die Löschung als gewählt. Die Löschung einschließlich der Sicherungskopien erfolgt innerhalb der dort genannten Fristen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über

das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10. Informationspflichten, Schriftformklausel, Rechtswahl

- a) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.
- b) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile (einschließlich etwaiger Zusicherungen des Auftragnehmers) bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann. Die Vereinbarung muss ausdrücklich darauf hinweisen, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Änderungen nach § 20 des Hauptvertrags und Änderungen der Subunternehmer nach Ziffer 11 g bleiben unberührt.
- c) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit dieser Vereinbarung im Übrigen nicht.
- d) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- e) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.
- f) Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist Würzburg. Als Ausnahme hierzu ist der Auftragnehmer auch berechtigt, den Auftraggeber an seinem allgemeinen Gerichtsstand in Anspruch zu nehmen.

11. Unterauftragsverhältnisse mit Subunternehmern

- a) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung der weisungsberechtigten Personen des Auftraggebers gestattet. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- b) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- c) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.
- d) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

- e) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den auferlegten Datenschutzpflichten nachkommt.
- f) Zurzeit sind für den Auftragnehmer die in Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
- g) Der Auftragnehmer ist berechtigt, weitere Subunternehmer hinzuzuziehen oder bestehende zu ersetzen. Er teilt jede beabsichtigte Änderung mindestens vier Wochen vor deren Wirksamwerden mit, entweder durch Veröffentlichung der aktualisierten Subunternehmerliste auf seiner Website oder in Textform gegenüber den weisungsberechtigten Personen des Auftraggebers. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus einem datenschutzrechtlich begründeten Anlass in Textform widersprechen. Widerspricht er nicht und nutzt er die Leistungen des Auftragnehmers nach Ablauf der Frist weiter, gilt die Genehmigung im Sinne von Art. 28 Abs. 2 Satz 1 DSGVO als erteilt. Im Fall eines Widerspruchs suchen die Parteien eine einvernehmliche Lösung; kommt sie nicht zustande, kann der Auftraggeber den betroffenen Leistungsteil mit einer Frist von vier Wochen kündigen.
- h) Nicht als Subunternehmer im Sinne dieser Ziffer gelten der Anbieter des KI-Assistenten, den der Auftraggeber mit seiner Website verbindet, der Betreiber des Immobilien-Verwaltungssystems des Auftraggebers sowie Drittanbieter, deren Dienste der Auftraggeber selbst in seine Website einbettet (etwa Video-, Karten- oder Bewertungsdienste). Diese Anbieter beauftragt der Auftraggeber selbst; der Auftragnehmer hat auf sie keinen Einfluss.

Unterschriften

Diese Vereinbarung wird mit dem Abschluss des Hauptvertrags im Bestellvorgang wirksam (AGB § 2 Abs. 3) und liegt damit in elektronischem Format vor (Art. 28 Abs. 9 DSGVO). Wünscht der Auftraggeber eine unterzeichnete Fassung, unterzeichnen die Parteien nachstehend; die Wirksamkeit hängt davon nicht ab.

Auftraggeber	Auftragnehmer
Ort, Datum:	Würzburg, den
Unterschrift:	Unterschrift (InnoBrain GmbH):
Name, Funktion:	Name, Funktion:

Anlage 1: Weisungen, Weitere Auftragsverarbeiter, Art der Verarbeitung, Kreis der Betroffenen

1. Weisungsberechtigte, Weisungsempfänger, Kommunikationsmittel für Weisungen

Weisungsberechtigte Personen des Auftraggebers sind die in der Auftragsbestätigung benannte Ansprechperson sowie jede Person, die der Auftraggeber dem Auftragnehmer in Textform als weisungsberechtigt benennt. Bis zu einer abweichenden Mitteilung gilt der Inhaber des Administratorkontos der Website als weisungsberechtigt.

Weisungsempfänger beim Auftragnehmer ist der Support der InnoBrain GmbH, support@inno-brain.de, Telefon 0931 61423986.

Für Weisungen zu nutzende Kommunikationskanäle: InnoBrain GmbH, Theaterstraße 26, 97070 Würzburg, E-Mail support@inno-brain.de, Telefon 0931 61423986. Mündliche Weisungen bestätigt der Auftraggeber in Textform.

2. Auftragsverarbeiter

Folgende Auftragsverarbeiter dürfen durch den Auftragnehmer im Rahmen der Tätigkeit, die in dem zu dieser Anlage gehörenden Vertrag zur Auftragsverarbeitung beschrieben ist, hinzugezogen werden:

Auftragsverarbeiter Nr. 1 Name: Hetzner Online GmbH Anschrift inklusive Land: Industriestraße 25, 91710 Gunzenhausen, Deutschland Umfang, Art und Zweck der Tätigkeit: Rechenzentrum (Standort Falkenstein), Bereitstellung der Server-Infrastruktur, Hosting der Website; Objektspeicher (Standort Nürnberg) für die fortlaufende Datensicherung der Website

Auftragsverarbeiter Nr. 2 Name: Microsoft Ireland Operations Limited Anschrift inklusive Land: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland Umfang, Art und Zweck der Tätigkeit: Microsoft 365 (Outlook/Exchange, Teams, OneDrive, SharePoint, Entra ID) für die Support- und Geschäftskommunikation mit dem Auftraggeber, soweit darin personenbezogene Daten aus dem Auftrag enthalten sind. Verarbeitung in Rechenzentren in der EU; Unterauftragnehmer des Anbieters können Daten auch in Drittländern (insbesondere USA) verarbeiten, Grundlage sind die EU-Standardvertragsklauseln im Vertrag mit dem Anbieter

Auftragsverarbeiter Nr. 3 Name: Atlassian B.V. Anschrift inklusive Land: Hoogoorddreef 5, 1101 BA Amsterdam, Niederlande Umfang, Art und Zweck der Tätigkeit: Jira Service Management für die Bearbeitung von Support-Anfragen des Auftraggebers. Verarbeitung in Rechenzentren in der EU; Unterauftragnehmer des Anbieters können Daten auch in Drittländern (insbesondere USA) verarbeiten, Grundlage sind die EU-Standardvertragsklauseln im Vertrag mit dem Anbieter

[Baustein bei Mailversand durch die Plattform: Sobald die Website E-Mails versendet (etwa Benachrichtigungen aus Kontaktformularen), wird der Versanddienstleister als Auftragsverarbeiter Nr. 4 mit Name, Anschrift und dem Zweck „Versand von E-Mails der Website im Auftrag des Auftraggebers“ ergänzt. Bis dahin versendet die Website keine E-Mails.]

Nicht aufgeführt und bewusst nicht Auftragsverarbeiter: die Scaleway SAS (Container-Registry des Auftragnehmers; dort liegen nur Programmpakete ohne Daten des Auftraggebers), der Anbieter des KI-Assistenten des Auftraggebers, der Betreiber des Immobilien-Verwaltungssystems des Auftraggebers sowie die Zertifizierungsstelle Let's Encrypt (verarbeitet nur Domainnamen).

3. Umfang, Art und Zweck der Verarbeitung

Der Auftragnehmer speichert die vom Auftraggeber eingestellten Inhalte, liefert sie an Besucher der Website aus, verwaltet die Benutzerkonten des Redaktionssystems, übernimmt Objekt- und Ansprechpartnerdaten aus dem angebundenen Immobilien-Verwaltungssystem, protokolliert den technischen Betrieb, sichert die Daten fortlaufend und stellt sie bei Störungen wieder her. Zweck ist der Betrieb der Website des Auftraggebers nach dem Hauptvertrag.

4. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Daten der Benutzer des Redaktionssystems: Name, E-Mail-Adresse, Rolle, Passwort (nur als Hashwert), Geheimnisse der Zwei-Faktor-Authentifizierung und Passkeys, Zeitpunkte der Anmeldung, Bearbeitungsverlauf (Versionen);
- Inhalte der Website, soweit sie personenbezogen sind: Namen, Fotos, Positionen und Kontaktdaten von Mitarbeitern und Ansprechpartnern des Auftraggebers; Namen und Aussagen in Kundenstimmen; Angaben in Texten, Bildern und Dokumenten, die der Auftraggeber einstellt;
- Objektdaten aus dem Immobilien-Verwaltungssystem: Objektbeschreibungen, Bilder, Lage und Adresse des Objekts, soweit freigegeben, sowie der zugeordnete Ansprechpartner (Name, Foto, Kontaktdaten);
- technische Daten der Besucher der Website: IP-Adresse, Zeitpunkt des Abrufs, abgerufene Adresse, Browser- und Geräteerkennung und Referrer werden beim Abruf verarbeitet, aber nicht dauerhaft protokolliert; Fehlerprotokolle der Website werden kurzfristig vorgehalten; die Plattform verdichtet Abrufe zu Zählwerten ohne Personenbezug; dazu eine Sitzungskennung in technisch notwendigen Cookies.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags; der Auftraggeber stellt sicher, dass er solche Daten nicht auf der Website einstellt.

5. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst: Mitarbeiter, Inhaber und Ansprechpartner des Auftraggebers; Besucher der Website; Kunden, Interessenten und Eigentümer des Auftraggebers, soweit sie in Inhalten der Website (Kundenstimmen, Referenzen, Objektdaten) genannt werden; sonstige Personen, deren Daten der Auftraggeber in Inhalte der Website aufnimmt.

Anlage 2: Technische und organisatorische Maßnahmen nach Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO

Stand 19.10.2026. Beschrieben sind die Maßnahmen für die Plattform, auf der die Website des Auftraggebers betrieben wird, sowie für die Organisation des Auftragnehmers.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Zutrittskontrolle

Die Website und ihre Daten werden ausschließlich in Rechenzentren der Hetzner Online GmbH (Falkenstein, Nürnberg) verarbeitet. Für den Zutritt zu diesen Rechenzentren gelten die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters Nr. 1, die der Auftragnehmer auf Anfrage vorlegt. In den Geschäftsräumen des Auftragnehmers werden keine Daten des Auftraggebers dauerhaft gespeichert; Geräte, über die der Auftragnehmer auf die Plattform zugreift, sind verschlüsselt und mit Bildschirmsperre versehen.

b) Zugangskontrolle

- Der administrative Zugriff auf die Plattform ist auf die mit dem Betrieb betrauten Personen des Auftragnehmers beschränkt und erfolgt mit persönlichen kryptografischen Schlüsseln.
- Benutzer des Redaktionssystems melden sich mit persönlichem Konto und Passwort an. Passwörter werden ausschließlich als Hashwert gespeichert. Zwei-Faktor-Authentifizierung und Passkeys stehen allen Benutzern zur Verfügung.
- Anmeldeversuche werden begrenzt; die Schnittstelle für KI-Assistenten ist über ein OAuth-Verfahren an das Benutzerkonto gebunden und auf 60 Anfragen je Minute begrenzt.
- Die Anmeldung am Redaktionssystem erfolgt über eine nicht indexierte Adresse; die Plattform-Adresse der Website ist für Suchmaschinen gesperrt.

c) Zugriffskontrolle

- Benutzer des Redaktionssystems erhalten Rollen mit abgestuften Rechten; der Auftraggeber verwaltet die Benutzer seiner Website selbst.
- Die Schnittstelle für KI-Assistenten kann Inhalte nicht löschen, nur anlegen, ändern und unveröffentlichen.
- Mitarbeiter des Auftragnehmers greifen auf Inhalte des Auftraggebers nur zur Störungsbeseitigung, zur Wiederherstellung oder auf Weisung zu.

d) Trennungskontrolle

- Jede Website läuft in einem eigenen Container mit eigener Datenbank und eigenem Dateibestand. Container verschiedener Kunden teilen keine Daten.
- Netzwerkrichtlinien unterbinden jede Verbindung zwischen den Containern verschiedener Websites; erlaubt sind nur Namensauflösung, der Zugriff des Lastverteilers auf die Website und ausgehende Verbindungen ins Internet.
- Container laufen ohne Administratorrechte, mit eingeschränkten Systemrechten und ohne Zugangsdaten zur Plattformsteuerung.
- Die Zugangsdaten zum Objektspeicher sind nur dem Sicherungsprozess zugänglich, nicht den Website-Containern.

e) Pseudonymisierung

Abrufe der Website werden zu Zählwerten ohne Personenbezug verdichtet (Fünf-Minuten-Fenster, Vorhaltezeit sieben Tage); Zugriffsprotokolle mit IP-Adressen werden nicht dauerhaft gespeichert. Produktfeedback enthält keine Besucherdaten.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a) Weitergabekontrolle

Alle Verbindungen zur Website, zum Redaktionssystem, zur Schnittstelle und zum Objektspeicher sind transportverschlüsselt (TLS). Zertifikate werden automatisch beantragt und erneuert. Datenträger werden nicht transportiert.

b) Eingabekontrolle

Das Redaktionssystem führt für Seiten und Einträge Versionen mit Benutzer und Zeitpunkt. Änderungen über die Schnittstelle werden dem angemeldeten Benutzer zugeordnet. Administrative Eingriffe des Auftragnehmers werden dokumentiert.

c) Datenintegrität bei Fehlfunktionen

Updates von Template und Plattform durchlaufen vor dem Einspielen automatisierte Tests und werden versioniert ausgerollt; jede Website wird einzeln auf eine neue Version umgestellt. Die Datenbank jeder Website wird fortlaufend gesichert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, lit. c DSGVO)

a) Verfügbarkeitskontrolle

- Fortlaufende Replikation der Datenbank jeder Website bei jeder Änderung in den Objektspeicher des Auftragsverarbeiters Nr. 1 an einem zweiten Standort.
- Überwachung des Zustands jeder Website; bei Ausfall eines Containers wird er automatisch ersetzt und aus der Sicherung wiederhergestellt.
- Speicher- und Ressourcengrenzen je Website, damit eine Website die anderen nicht beeinträchtigt; die Schnittstelle für KI-Assistenten ist auf 60 Anfragen je Minute begrenzt.
- Patch-Management für Plattform und Template; sicherheitsrelevante Updates werden ohne Verzögerung eingespielt.

b) Rasche Wiederherstellbarkeit

Wiederherstellung einer Website auf einen Zeitpunkt innerhalb der letzten sieben Tage; Wiederherstellungspunkt nach Anlage 2 des Hauptvertrags.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO)

a) Auftragskontrolle

Die Verantwortlichkeiten von Auftraggeber und Auftragnehmer ergeben sich aus dem Hauptvertrag. Der Auftragnehmer verarbeitet die Daten nur im Rahmen des vereinbarten Leistungsumfangs und der Weisungen nach Ziffer 8.

b) Datenschutz-Management, Incident-Response-Management, datenschutzfreundliche Voreinstellungen

- Die Plattform wird regelmäßig einer Sicherheitsprüfung unterzogen; festgestellte Schwachstellen werden nach Schwere priorisiert und behoben.
- Sicherheitsvorfälle werden nach einem festgelegten Ablauf erfasst, bewertet, behoben und dem Auftraggeber nach Ziffer 7 gemeldet.

- Datenschutzfreundliche Voreinstellungen des Templates: keine Analyse- oder Marketing-Werkzeuge im Auslieferungszustand, selbst gehostete Schriften, externe Einbettungen erst nach Klick, Plattform-Adresse nicht indexiert.
- Beschäftigte des Auftragnehmers sind auf die Vertraulichkeit verpflichtet und werden zu Datenschutz und Informationssicherheit unterwiesen.