

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO · Stand: Juli 2026

Vertragsparteien

Verantwortlicher (Auftraggeber – nachfolgend „Verantwortlicher“)

Firma / Name: _____
Anschrift: _____
PLZ, Ort: _____
Vertreten durch: _____
E-Mail des Nutzerkontos: _____

Auftragsverarbeiter (Auftragnehmer – nachfolgend „Auftragsverarbeiter“)

HausHirsch GmbH
Hauptstraße 44
40789 Monheim am Rhein
Vertreten durch den Geschäftsführer Christian Wanderer
Telefon: +49 800 000 1244 · E-Mail: info@haushirsch.de
Betrieb des Dienstes maklerunterlagen.de

Der Auftragsverarbeiter hat einen externen Datenschutzbeauftragten bestellt: PROLIANCE GmbH, Leopoldstraße 21, 80802 München, info@proliance.ai.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Bereitstellung und der Betrieb der Web-Anwendung maklerunterlagen.de, mit der der Verantwortliche Dokumentvorlagen ausfüllt, speichert, als PDF exportiert und über zeitlich begrenzte Links teilt. Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen.

(2) Einzelheiten zu Art, Umfang und Zweck der Verarbeitung, den Datenkategorien und dem Kreis der betroffenen Personen ergeben sich aus **Anlage 1**.

(3) Die Dauer dieses Auftrags entspricht der Laufzeit des Nutzungsverhältnisses nach den Nutzungsbedingungen von maklerunterlagen.de. Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.

(4) Die Verarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem Drittland erfolgt nicht und bedürfte der vorherigen Zustimmung des Verantwortlichen sowie der Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO.

§ 2 Rechte und Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich (Art. 24 DSGVO).

(2) Der Verantwortliche entscheidet allein darüber, welche personenbezogenen Daten er in den Dienst eingibt. Er stellt sicher, dass für die Erhebung und Eingabe eine Rechtsgrundlage besteht und dass er zur Übermittlung an den Auftragsverarbeiter befugt ist.

(3) Weisungen erteilt der Verantwortliche in Textform an info@haushirsch.de. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Die Bedienung des Dienstes im Rahmen seiner Funktionen gilt als erteilte Weisung.

(4) Der Verantwortliche benennt für Fragen des Datenschutzes eine ansprechbare Stelle; sofern er einen Datenschutzbeauftragten bestellt hat, teilt er dessen Kontaktdaten mit.

(5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrages und nach dokumentierten Weisungen des Verantwortlichen. Eine Verarbeitung zu eigenen Zwecken – insbesondere zu Werbezwecken, zur Profilbildung oder zum Training von Modellen künstlicher Intelligenz – findet nicht statt.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, teilt er dies dem Verantwortlichen unverzüglich mit. Er ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

(3) Der Auftragsverarbeiter ist verpflichtet, den Dienst so einzurichten, dass die im Rahmen der Auftragsdurchführung verarbeiteten Daten von den Daten anderer Verantwortlicher getrennt bleiben. Die Trennung erfolgt logisch durch die Zuordnung sämtlicher Datensätze zum jeweiligen Nutzerkonto.

(4) Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(5) Der Auftragsverarbeiter benennt dem Verantwortlichen auf Anfrage die Kontaktdaten seines Datenschutzbeauftragten.

§ 4 Vertraulichkeit

(1) Der Auftragsverarbeiter setzt zur Durchführung der Arbeiten ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet und mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht wurden (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

(2) Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung der Tätigkeit fort.

(3) Ein Zugriff auf Inhalte des Verantwortlichen durch Beschäftigte des Auftragsverarbeiters erfolgt nur, soweit dies zur Störungsbeseitigung unumgänglich ist oder der Verantwortliche im Rahmen einer Supportanfrage ausdrücklich darum bittet.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und weist deren Einhaltung auf Verlangen nach.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und werden hiermit genehmigt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens **30 Tage** vor der Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters in Textform. Der Verantwortliche kann hiergegen innerhalb von 14 Tagen nach Zugang aus wichtigem, datenschutzrechtlichem Grund Einspruch erheben. Wird der Einspruch nicht ausgeräumt, kann der Verantwortliche das Nutzungsverhältnis zum geplanten Zeitpunkt der Änderung außerordentlich kündigen.

(3) Der Auftragsverarbeiter wählt Unterauftragsverarbeiter sorgfältig aus und verpflichtet sie vertraglich auf Datenschutzpflichten, die denen dieses Vertrages entsprechen (Art. 28 Abs. 4 DSGVO).

(4) Nicht als Unterauftragsverhältnis gelten Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt und die keinen Zugriff auf die Auftragsdaten eröffnen (z. B. Telekommunikationsleistungen, Reinigung, Wartung).

§ 7 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Erfüllung von Anfragen betroffener Personen nach Art. 12 bis 23 DSGVO. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

(2) Auskunft, Berichtigung, Einschränkung, Löschung und Datenübertragbarkeit kann der Verantwortliche für die von ihm eingegebenen Daten weitgehend selbst über die Funktionen des Dienstes ausüben: Dokumente lassen sich jederzeit einsehen, bearbeiten, als PDF exportieren und löschen; das gesamte Konto samt aller Dokumente kann selbständig gelöscht werden.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen des Schutzes personenbezogener Daten und bei Datenschutz-Folgenabschätzungen.

(4) Für Unterstützungsleistungen, die über die Bereitstellung der Funktionen des Dienstes hinausgehen und nicht auf einem Verschulden des Auftragsverarbeiters beruhen, kann dieser eine angemessene Vergütung verlangen; er weist auf die Entgeltlichkeit vorher hin.

§ 8 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Kenntniserlangung, über Verletzungen des Schutzes personenbezogener Daten, die die Auftragsdaten betreffen.

(2) Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die betroffenen

Datenkategorien und die ungefähre Zahl der betroffenen Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen.

(3) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich hierzu mit dem Verantwortlichen ab.

§ 9 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter weist die Einhaltung der Pflichten aus diesem Vertrag auf Anforderung nach – vorrangig durch Selbstauskunft, Übersendung der Dokumentation der technischen und organisatorischen Maßnahmen oder durch Vorlage geeigneter Zertifikate oder Prüfberichte.

(2) Der Verantwortliche ist berechtigt, sich von der Einhaltung zu überzeugen, auch durch Kontrollen vor Ort. Solche Kontrollen sind mit angemessener Vorlaufzeit von mindestens 14 Tagen, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs durchzuführen; sie werden auf eine Kontrolle pro Kalenderjahr beschränkt, sofern kein besonderer Anlass besteht.

(3) Kontrollen durch Beauftragte des Verantwortlichen setzen voraus, dass diese nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen und zur Verschwiegenheit verpflichtet sind.

§ 10 Löschung und Rückgabe

(1) Nach Beendigung des Auftrags löscht der Auftragsverarbeiter sämtliche im Auftrag verarbeiteten personenbezogenen Daten, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Löscht der Verantwortliche sein Konto über die Funktion „Konto löschen“, werden das Konto, das Firmenprofil samt Logo, alle Dokumente, Feldwerte, Versionen, erzeugten PDF-Dateien und Freigabelinks unwiderruflich entfernt. Eine Wiederherstellung ist danach nicht mehr möglich.

(3) Der Verantwortliche ist gehalten, benötigte Dokumente vor der Löschung selbst als PDF zu exportieren. Eine darüber hinausgehende Herausgabe in einem strukturierten Format kann er bis zur Beendigung des Auftrags verlangen.

(4) Sicherungskopien werden im Rahmen der üblichen Aufbewahrungszyklen automatisch überschrieben.

§ 11 Haftung

(1) Für die Haftung im Verhältnis der Parteien gelten die Regelungen der Nutzungsbedingungen von maklerunterlagen.de.

(2) Art. 82 DSGVO bleibt unberührt.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Bei Widersprüchen zwischen diesem Vertrag und den Nutzungsbedingungen gehen die Regelungen dieses Vertrages vor, soweit die Verarbeitung personenbezogener Daten im Auftrag betroffen ist.

(3) Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

Ort, DatumOrt, Datum

VerantwortlicherHausHirsch GmbH

Anlage 1: Gegenstand, Art und Zweck der Verarbeitung

1. Gegenstand

Bereitstellung einer Web-Anwendung zum Ausfüllen, Speichern, Versionieren und Exportieren von Dokumentvorlagen für die Immobilienvermittlung sowie zum Teilen dieser Dokumente über zeitlich begrenzte Links.

2. Art der Verarbeitung

Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Verwenden (Zusammenführen zu Dokumenten), Übermitteln durch Bereitstellung (Freigabelinks), Einschränken und Löschen.

3. Zweck

Erstellung, Verwaltung und Bereitstellung von Vertrags- und Formulardokumenten für die Geschäftstätigkeit des Verantwortlichen als Immobilienmakler. Eine über diesen Zweck hinausgehende Verwendung findet nicht statt.

4. Kategorien betroffener Personen

- Eigentümerinnen und Eigentümer sowie Verkäuferinnen und Verkäufer
- Kauf- und Mietinteressentinnen und -interessenten
- Mieterinnen und Mieter sowie Vermieterinnen und Vermieter
- Ansprechpartnerinnen und Ansprechpartner der vorgenannten Personen
- Beschäftigte des Verantwortlichen, die den Dienst nutzen

5. Kategorien personenbezogener Daten

- **Stammdaten:** Vor- und Nachname, Anschrift
- **Kontaktdaten:** Telefonnummer, E-Mail-Adresse
- **Vertragsdaten:** Kaufpreis, Miethöhe, Provision, Laufzeiten, Fristen, Ort und Datum des

Abschlusses

- **Objektbezogene Daten:** Anschrift und Merkmale der Immobilie, Zählerstände, Schlüsselanzahl, dokumentierte Mängel
- **Daten aus Selbstauskünften,** soweit der Verantwortliche entsprechende Vorlagen nutzt: Angaben zu Beschäftigung, Einkommen und Bonität sowie erklärte Angaben zu Haushalt und Wohnverhältnissen
- **Nutzungsdaten** des Kontos des Verantwortlichen: Anmeldezeitpunkte, Bearbeitungszeitpunkte, Versionsverlauf

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Der Verantwortliche sieht davon ab, solche Daten in den Dienst einzugeben.

6. Ort der Verarbeitung

Ausschließlich Rechenzentren in der Bundesrepublik Deutschland.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

Zutrittskontrolle. Der Betrieb erfolgt in Rechenzentren des in Anlage 3 genannten Hosting-Anbieters in Deutschland. Dort bestehen Zutrittssicherung, Videoüberwachung, Vereinzelungsanlagen und dokumentierte Besucherverwaltung. Eigene Serverräume werden nicht betrieben.

Zugangskontrolle. Der Zugang zur Anwendung setzt ein persönliches Nutzerkonto mit bestätigter E-Mail-Adresse voraus. Passwörter unterliegen einer serverseitig geprüften Mindestkomplexität und werden ausschließlich als nicht umkehrbarer Hash nach dem Verfahren Argon2id gespeichert. Anmeldeversuche sind nach IP-Adresse und E-Mail-Adresse gedrosselt; nach mehreren Fehlversuchen greift eine zeitlich ansteigende Sperre. Sitzungen werden bei der Anmeldung erneuert (Schutz vor Session-Fixation), sind an eine Sitzungs-Epoche gebunden und werden nach einer Passwortänderung sämtlich ungültig.

Zugriffskontrolle. Jeder Datensatz ist einem Nutzerkonto zugeordnet; sämtliche Abfragen prüfen diese Zuordnung. Erzeugte PDF-Dateien und hochgeladene Logos liegen außerhalb des über das Internet erreichbaren Verzeichnisses und werden nur über geprüfte Anwendungsrouten ausgeliefert. Administrative Funktionen sind einer gesonderten Rolle vorbehalten.

Trennungskontrolle. Die Daten verschiedener Verantwortlicher werden logisch über die Kontozuordnung getrennt verarbeitet. Produktiv- und Testumgebungen sind getrennt; Tests erfolgen nicht mit Produktivdaten.

Pseudonymisierung. In den Sicherheitsprotokollen werden IP-Adressen, E-Mail-Adressen und Browserkennungen ausschließlich als Hashwert gespeichert.

2. Integrität

Weitergabekontrolle. Sämtliche Verbindungen zur Anwendung sind mit TLS verschlüsselt; die Auslieferung erfolgt mit HTTP Strict Transport Security. Der E-Mail-Versand erfolgt über eine

verschlüsselte SMTP-Verbindung. Eine Übermittlung in Drittländer findet nicht statt. Freigabelinks sind zufällig erzeugt, werden nur als Hashwert gespeichert, laufen automatisch ab (Standard 72 Stunden), können auf eine Anzahl von Abrufen begrenzt und jederzeit widerrufen werden.

Eingabekontrolle. Jede Speicherung eines Dokuments erzeugt eine Version mit Zeitstempel, Nutzerbezug und Prüfsumme des Inhalts. Sicherheitsrelevante Vorgänge – Passwortänderung, Kontolöschung, Verwendung ungültiger Links – werden protokolliert.

Datenintegrität. Alle Datenbankzugriffe erfolgen über vorbereitete Anweisungen. Vom Nutzer eingegebenes HTML wird serverseitig gegen eine strenge Positivliste bereinigt. Zustandsverändernde Anfragen sind durch sitzungsgebundene CSRF-Merkmale geschützt. Schreibende Vorgänge, die mehrere Tabellen betreffen, laufen in Datenbanktransaktionen; gleichzeitige Bearbeitung wird über eine Versionsnummer erkannt.

3. Verfügbarkeit und Belastbarkeit

Der Betrieb erfolgt in Rechenzentren mit unterbrechungsfreier Stromversorgung, Netzersatzanlagen, Brandfrüherkennung und redundanter Netzanbindung. Der Auftragsverarbeiter führt regelmäßige Sicherungen der Datenbank und des Dokumentenspeichers durch und prüft die Wiederherstellbarkeit. Ein automatisierter Bereinigungslauf entfernt abgelaufene Zugangsmerkmale und verwaiste Dateien. Anfragehäufigkeiten sind begrenzt, um Überlastung durch automatisierte Zugriffe zu vermeiden.

4. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management. Es besteht ein Verzeichnis der Verarbeitungstätigkeiten. Ein externer Datenschutzbeauftragter ist bestellt. Beschäftigte sind auf Vertraulichkeit verpflichtet.

Auftragskontrolle. Mit Unterauftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO. Weisungen werden in Textform dokumentiert.

Überprüfung. Änderungen an der Anwendung werden vor Veröffentlichung durch automatisierte Tests geprüft, die auch sicherheitsrelevantes Verhalten abdecken (Zugriffsschutz fremder Dokumente, Bereinigung eingegebenen HTML-Codes, Wirksamkeit der Anmeldesperre). Sicherheitsaktualisierungen der eingesetzten Komponenten werden zeitnah eingespielt.

Datenschutz durch Voreinstellung. Der Dienst setzt keine Analyse-, Tracking- oder Werbedienste ein, bindet keine externen Schriftarten oder Skripte ein und erhebt nur die für den Betrieb erforderlichen Daten.

Anlage 3: Genehmigte Unterauftragsverarbeiter

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Hosting der Anwendung, der Datenbank und des Dokumentenspeichers; Betrieb des Mailservers	Deutschland

Stand: Juli 2026. Änderungen werden nach § 6 Abs. 2 dieses Vertrages mitgeteilt.