

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (AVV) nach Art. 28 DSGVO

Telesherpa GmbH · Version 1.0 · Stand 21.10.2026 · <https://www.telesherpa.com/avv>

Dieser AVV ist Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) der Telesherpa GmbH und gilt für alle Verarbeitungen personenbezogener Daten, die Telesherpa im Auftrag des Kunden vornimmt. Mit der Annahme der AGB bei der Registrierung (im Web oder über ein Agentenkonto mit `accept_terms`) ist auch dieser AVV angenommen; Telesherpa protokolliert Version, Zeitpunkt, Konto und Annahmeweg (Art. 28 Abs. 9 DSGVO). Frühere Versionen sind unter <https://www.telesherpa.com/avv> abrufbar.

Vertragsparteien

Verantwortlicher: der Kunde im Sinne der AGB, einschließlich des Betreibers eines Agentenkontos nach AGB Ziffer 4 (nachfolgend „**Kunde**“). Der Kunde ist Unternehmer, öffentliche Stelle, Verein oder eine vergleichbare Organisation; eine rein private Nutzung ist nicht Gegenstand dieses AVV.

Auftragsverarbeiter: Telesherpa GmbH, Barbaraweg 8, 53125 Bonn, Amtsgericht Bonn HRB 31107, vertreten durch die Geschäftsführung (nachfolgend „**Telesherpa**“).

§ 1 Gegenstand und Dauer

- 1. Gegenstand.** Telesherpa stellt dem Kunden die Ontologie-Plattform „Telesherpa“ als Software-as-a-Service bereit: Web-Anwendung (app.telesherpa.com), Progressive Web App, native Apps für iOS und Android, Programmierschnittstellen und MCP-Server (mcp.telesherpa.com). Mit ihr erfasst, verknüpft und wertet der Kunde Geschäftsobjekte aus, etwa Standorte, Gebäude, Anlagen, Fahrzeuge, Personen, Aufträge und Prüfungen, selbst, durch seine Nutzer und durch von ihm betriebene KI-Agenten. Dabei verarbeitet Telesherpa personenbezogene Daten im Auftrag des Kunden (§ 2).
- 2. Dauer.** Der AVV gilt für die Laufzeit des Nutzungsverhältnisses nach den AGB und darüber hinaus, solange Telesherpa personenbezogene Daten des Kunden verarbeitet, insbesondere bis zum Abschluss von Löschung oder Rückgabe nach § 12.
- 3. Abgrenzung.** Nicht Gegenstand dieses AVV sind Verarbeitungen in eigener Verantwortung von Telesherpa: Verwaltung des Kundenkontos als Vertragspartner, Abrechnung von Credits einschließlich Zahlungsabwicklung, inhaltsfreie technische Nutzungs- und Abrechnungsmetriken, Missbrauchsabwehr nach AGB Ziffer 5 und 9, Erfüllung gesetzlicher Pflichten sowie der Betrieb der Website www.telesherpa.com. Darüber informiert die Datenschutzerklärung von Telesherpa.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen, Ort

- 1. Art der Verarbeitung:** Erheben, Erfassen, Speichern, Organisieren, Ordnen, Verknüpfen, Auslesen, Abfragen, Auswerten, Verwenden, Übermitteln an vom Kunden berechnigte Nutzer, Agenten und Empfänger, Einschränken, Löschen und Vernichten, jeweils über die Plattform.

2. **Zweck:** Bereitstellung, Betrieb, Sicherung, Wartung und Fehlerbehebung der Plattform für den Kunden, insbesondere:

- Speicherung und Verwaltung von Objekten, Eigenschaften, Verknüpfungen, Dateien, Bildern, Kommentaren und Zeitreihen in den Datenbereichen (Scopes) des Kunden;
- Formulare und Formularantworten einschließlich Fotos, Dokumenten und Unterschriften, Erzeugung von PDF-Dokumenten;
- Aufträge (ServiceOrders) an Mitarbeitende, QR-Scan- und Kontrollpunkt-Abläufe, Benachrichtigungen in der Plattform, per E-Mail und per Push;
- Automatisierung über Regeln und Funktionen, Reports und Auswertungen (CSV, JSON, Kartendaten), Geocodierung von Adressen und Koordinaten;
- Bereitstellung der Daten an die KI-Agenten des Kunden über den MCP-Server im Rahmen der vom Kunden vergebenen Rechte;
- Datenimporte und Service-Anfragen des Kunden, etwa zur Ergänzung von Objekttypen;
- Einladungen und Mitgliederverwaltung (Einladungs_codes, Allowlists);
- auf ausdrückliche Weisung des Kunden: Freigabe von Datenbereichen als öffentlich (PUBLIC).

3. **Art der personenbezogenen Daten** (je nach Konfiguration durch den Kunden):

Kategorie	Beispiele
Konto- und Identitätsdaten	E-Mail-Adresse bzw. Benutzername, Passwort (nur als Hash), Profilangaben, Sprache, Rollen, Scope-Mitgliedschaften und Rechte; bei Agentenkonten die generierte Adresse <code>agent- <hex>@agents.telesherpa.com</code>
Authentifizierungs- und Sitzungsdaten	Access- und Refresh-Tokens, MCP-Session-IDs, Passkey-Daten, OAuth-Client-Registrierungen, User-Agent, IP-Adressen
Protokolldaten	Änderungs- und Aktionsprotokolle einschließlich Payload, Zeitpunkte, ausführendes Konto (Mensch oder Agent)
Inhaltsdaten in Objekten	Namen, Kontaktdaten, Anschriften, Funktionen von Personen; Kunden-, Mieter- oder Mitgliedsbezüge, die der Kunde anlegt; Kommentare; freie Texte
Standort- und Bewegungsdaten	Adressen, Geokoordinaten, Zeitreihen (z. B. Fahrzeugrouten), Scan-Zeitpunkte an Kontrollpunkten mit ausführender Person
Bild-, Dokument- und Unterschriftsdaten	Fotos (auch mit abgebildeten Personen), hochgeladene Dokumente, elektronische Unterschriften, erzeugte PDFs
Arbeits- und Einsatzdaten	Aufträge, Zuweisungen, Bearbeitungsstatus, Dienstpläne, Stundenzettel, Prüfprotokolle
Kommunikationsdaten	Benachrichtigungen, Push-Abonnements, E-Mail-Adressen in Einladungen und Allowlists
Besondere Kategorien (Art. 9 DSGVO)	Ausgeschlossen. Gesundheitsdaten und andere besondere Kategorien personenbezogener Daten sind nicht Gegenstand dieses AVV. Der Kunde verpflichtet sich, solche Daten nicht in die Plattform einzubringen und dies auch seinen Nutzern und Agenten vorzugeben (§ 5 Abs. 3).

4. **Betroffene Personen:** Beschäftigte und sonstige Nutzer des Kunden (einschließlich Außendienstkräfte); Betreiber von Agentenkonten; Kunden, Mieter, Mitglieder, Gäste und Besucher des Kunden; Ansprechpartner von Lieferanten, Dienstleistern und Partnern; sonstige Personen, die der Kunde in Objekten, Fotos oder Dokumenten erfasst; eingeladene Personen.
5. **Ort der Verarbeitung.** Plattform und Daten des Kunden werden ausschließlich im Rechenzentrum der OVH GmbH am Standort Limburg, Deutschland, betrieben und gespeichert, einschließlich der Datensicherungen (Anlage 2 Teil A). Eine Spiegelung an andere Standorte findet derzeit nicht statt. **Hinweis:** Weil Produktivdaten und Datensicherungen am selben Standort liegen, kann ein schwerer Schaden an diesem Standort (z. B. Brand) zum Verlust von Daten einschließlich der Sicherungen führen. Abweichungen ergeben sich nur aus den in Anlage 2 Teil B als **Drittlandbezug** gekennzeichneten Leistungen, insbesondere einem möglichen Fernzugriff von Gesellschaften der OVH-Gruppe in Kanada und im Vereinigten Königreich zu Sicherheits- und Wartungszwecken sowie dem E-Mail-Versand über Apple (Anlage 2 Teil B Nr. 2). Nutzt der Kunde die Geocodierung, übermittelt Telesherpa auf seine Weisung Adressangaben an Google als eigenständig Verantwortlichen (§ 7 Abs. 5, Anlage 2 Teil D). Push-Benachrichtigungen werden Ende-zu-Ende-verschlüsselt über die Push-Dienste der Browser zugestellt (Anlage 2 Teil C). Über weitere Standorte in der EU bzw. im EWR entscheidet Telesherpa nach § 6 Abs. 6.

§ 3 Weisungen

1. Telesherpa verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in ein Drittland, es sei denn, Telesherpa ist nach dem Recht der Union oder eines Mitgliedstaats dazu verpflichtet (Art. 28 Abs. 3 UAbs. 1 lit. a DSGVO). Dann teilt Telesherpa dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. **Behörden.** Personenbezogene Daten des Kunden übermittelt Telesherpa an Behörden nur, soweit Telesherpa nach Unions- oder mitgliedstaatlichem Recht dazu verpflichtet ist; Abs. 1 Satz 2 gilt. Freiwillige Meldungen nach AGB Ziffer 9 beschränken sich auf Daten, für die Telesherpa selbst verantwortlich ist. Ersuchen von Behörden aus Drittländern beantwortet Telesherpa nur nach Maßgabe von Art. 48 DSGVO.
3. **Was als Weisung gilt.** Weisungen sind dieser AVV, die AGB und die Konfiguration der Plattform durch den Kunden. Als Weisung gelten außerdem alle Handlungen, die der Kunde, seine Nutzer oder seine Agenten über Web-Anwendung, Apps, API oder MCP-Server vornehmen, etwa Anlegen, Ändern, Freigeben, Exportieren oder Löschen, sowie Service-Anfragen in Textform (ontouser_service_request oder E-Mail an service@telesherpa.com).
4. **Agenten des Kunden.** Handlungen eines Agentenkontos rechnet Telesherpa dem Kunden als Betreiber zu (AGB Ziffer 4). Der Kunde ist dafür verantwortlich, dass Konfiguration und Steuerung seiner Agenten mit dem Datenschutzrecht vereinbar sind.
5. **Erklärungen und Weisungen über Agenten.** Telesherpa ist eine Plattform, die in erster Linie von KI-Agenten genutzt wird. Für Erklärungen und Weisungen gilt daher:

- a) **Annahme.** Der Kunde kann diesen AVV über sein Agentenkonto annehmen (z. B. mit `accept_terms`). Der Agent übermittelt dabei die Erklärung des Betreibers als dessen Bote; formuliert er die Erklärung selbst, handelt er als vom Betreiber eingesetztes Werkzeug, dessen Erklärungen der Betreiber gegen sich gelten lässt (AGB Ziffer 4). Der Betreiber bleibt Verantwortlicher im Sinne der DSGVO.
 - b) **Weisungen.** Weisungen, die ein vom Kunden berechtigtes Konto, einschließlich eines Agentenkontos, über Web-Anwendung, Apps, API, MCP-Server oder Service-Anfrage erteilt, gelten als dokumentierte Weisungen des Kunden im Sinne von Art. 28 Abs. 3 UAbs. 1 lit. a DSGVO. Das gilt auch für weitreichende Weisungen: Löschung ganzer Scopes oder Konten, Veröffentlichung (PUBLIC) und Rückgabe der Daten nach § 12. Telesherpa protokolliert jede Weisung mit Konto und Zeitpunkt (§ 8 Abs. 5). Vor einer weitreichenden Weisung darf Telesherpa eine Bestätigung durch dasselbe Konto verlangen.
 - c) **Verantwortung des Betreibers.** Der Betreiber ist für die Erklärungen und Weisungen seines Agenten verantwortlich, als hätte er sie selbst abgegeben, auch wenn der Agent eigenständig oder infolge manipulierter Eingaben gehandelt hat (§ 5 Abs. 4).
 - d) **Kontaktstelle.** Mitteilungen von Telesherpa nach diesem AVV (insbesondere §§ 6, 9, 10 und 15) gehen an die Kontaktmöglichkeit, die der Betreiber nach AGB Ziffer 4 hinterlegt hat, und zusätzlich in das Plattform-Postfach des Kontos (nachfolgend „**Kontaktstelle**“); sie gelten mit Eingang als zugegangen. Der Kunde kann zusätzlich eine natürliche Person als Ansprechpartner benennen (Anlage 3); erforderlich ist das nicht.
6. **Datenschutzwidrige Weisungen.** Hält Telesherpa eine Weisung für datenschutzwidrig, informiert Telesherpa den Kunden unverzüglich (Art. 28 Abs. 3 UAbs. 2 DSGVO) und darf die Ausführung aussetzen, bis der Kunde sie bestätigt oder ändert.

§ 4 Pflichten von Telesherpa, Vertraulichkeit

1. Telesherpa verarbeitet die Daten ausschließlich für die Zwecke nach § 2, nutzt sie nicht für eigene Zwecke und gibt sie nicht an Dritte weiter, außer nach diesem AVV oder auf Weisung des Kunden. Telesherpa verwendet personenbezogene Daten des Kunden insbesondere nicht für Produktentwicklung, Tests, Experimente, Benchmarks oder Statistiken zu eigenen Zwecken. Erlaubt sind nur inhaltsfreie technische Nutzungs- und Abrechnungsmetriken in eigener Verantwortung (§ 1 Abs. 3). Telesherpa stellt sicher, dass ihm unterstellte Personen sowie von ihm betriebene automatisierte Systeme und KI-Agenten Daten des Kunden nur auf Weisung verarbeiten (Art. 29 DSGVO).
2. **Vertraulichkeit.** Telesherpa setzt nur Personen ein, die auf Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 UAbs. 1 lit. b DSGVO), und macht sie mit den Datenschutzbestimmungen vertraut. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.
3. **Berufsgeheimnisse.** Telesherpa übernimmt keine Verpflichtung als mitwirkende Person nach § 203 Abs. 3 und 4 StGB. Unterliegt der Kunde einer Verschwiegenheitspflicht nach § 203 StGB, bringt er keine Daten ein, die diesem Berufsgeheimnis unterliegen.

4. **Eigene KI-Agenten.** Für KI-Agenten, die Telesherpa für Entwicklung, Betrieb, Sicherheitsprüfung oder Support einsetzt, gilt § 8 Abs. 4.
5. **Ansprechpartner Datenschutz.** Ansprechpartner für den Datenschutz ist die Geschäftsführung (adg@telesherpa.com). Telesherpa hat keinen Datenschutzbeauftragten benannt; der Geschäftsführer übernimmt diese Funktion wegen des Interessenkonflikts nach Art. 38 Abs. 6 DSGVO nicht. Wird ein Datenschutzbeauftragter benannt, teilt Telesherpa dies mit und ergänzt Anlage 3.
6. Telesherpa führt ein Verzeichnis der Verarbeitungstätigkeiten im Auftrag (Art. 30 Abs. 2 DSGVO).
7. Telesherpa arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen und informiert den Kunden unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie diesen AVV betreffen.

§ 5 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Telesherpa trifft die in **Anlage 1** beschriebenen Maßnahmen. Sie berücksichtigen den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie das Risiko für die Rechte und Freiheiten der betroffenen Personen.
2. Telesherpa darf die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen teilt Telesherpa dem Kunden in Textform mit; Anlage 1 wird mit Versionsstand unter <https://www.telesherpa.com/avv> veröffentlicht.
3. **Verantwortung des Kunden.** Der Kunde ist verantwortlich für die Vergabe von Rechten in seinen Scopes, die sichere Aufbewahrung von Zugangsdaten und Tokens seiner Nutzer und Agenten (nicht im Klartext in geteilten Verzeichnissen), Auswahl und Konfiguration seiner KI-Modelle und Agenten sowie die Entscheidung, Daten öffentlich zu machen. Rechte werden je Scope vergeben, nicht je Objekt; ein Schreibrecht gilt für alle Objekte eines Scopes. Der Kunde ordnet seine Daten so auf Scopes auf, dass dies seinen Schutzanforderungen genügt.
4. **Hinweise zu Agenten.** Agenten können durch manipulierte Eingaben (Prompt Injection) zu unerwünschten Aktionen verleitet werden. Telesherpa empfiehlt, Agenten nur die nötigen Rechte zu geben (z. B. nur Lesen), getrennte Scopes für sensible Daten zu nutzen und destruktive Aktionen durch einen Menschen bestätigen zu lassen.

§ 6 Unterauftragsverarbeiter

1. **Genehmigung.** Der Kunde erteilt eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO). Bei Vertragsschluss gelten die in **Anlage 2 Teil B** aufgeführten Unterauftragsverarbeiter als genehmigt.
2. **Vertragliche Bindung.** Telesherpa erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Telesherpa haftet gegenüber dem Kunden für die Pflichterfüllung seiner Unterauftragsverarbeiter.

3. **Änderungen.** Telesherpa informiert den Kunden mindestens 30 Tage vor dem Einsatz eines neuen oder dem Austausch eines bestehenden Unterauftragsverarbeiters per E-Mail an die Kontaktstelle nach § 3 Abs. 5 lit. d und durch Aktualisierung der Liste unter <https://www.telesherpa.com/avv> mit Änderungshistorie. Die Information nennt Name, Anschrift, Leistung, Ort der Verarbeitung und einen etwaigen Drittlandbezug.
4. **Widerspruch.** Der Kunde kann innerhalb von 14 Tagen nach Zugang aus begründetem datenschutzrechtlichem Grund in Textform widersprechen. Telesherpa bemüht sich dann um eine zumutbare Alternative. Gibt es keine, kann jede Partei den Vertrag zum Zeitpunkt des Wechsels kündigen; Telesherpa erstattet nicht verbrauchte, vorausbezahlte Credits anteilig. AGB Ziffer 7 Satz 2 und 3 gilt insoweit nicht.
5. **Notfall.** Fällt ein Unterauftragsverarbeiter aus oder liegt ein Sicherheitsvorfall vor, darf Telesherpa vorübergehend einen gleichwertigen Ersatz mit Sitz und Verarbeitung in der EU bzw. im EWR einsetzen. Telesherpa informiert den Kunden unverzüglich; der Kunde kann innerhalb von 14 Tagen nach Abs. 4 widersprechen.
6. **Künftige Standorte.** Über weitere Rechenzentrumsstandorte entscheidet Telesherpa; eine Wahl des Standorts durch den Kunden besteht nicht. Es gilt:
 - a) Weitere Standorte liegen ausschließlich in der EU bzw. im EWR. Daten und Datensicherungen des Kunden werden nie außerhalb von EU bzw. EWR gespeichert.
 - b) Telesherpa kündigt die Aufnahme eines weiteren Standorts mindestens 30 Tage vorher nach Abs. 3 an und aktualisiert Anlage 2.
 - c) Neuer Standort desselben Unterauftragsverarbeiters: Mitteilung nach Abs. 3. Neuer Anbieter: Verfahren nach Abs. 3 und 4.
7. Keine Unterauftragsverarbeitung sind Nebenleistungen Dritter ohne Zugriff auf personenbezogene Daten des Kunden, etwa Telekommunikation oder Domainregistrierung.

§ 7 Übermittlung in Drittländer

1. Telesherpa verarbeitet die Daten des Kunden ausschließlich an den Orten nach Anlage 2 Teil A in Deutschland und übermittelt sie nicht in Drittländer außerhalb von EU und EWR, außer bei den in Anlage 2 Teil B als **Drittlandbezug** gekennzeichneten Leistungen mit der dort genannten Garantie. Das betrifft insbesondere einen möglichen Fernzugriff durch OVH Hebergement INC (Kanada) und OVH Limited (Vereinigtes Königreich) für Sicherheit und Wartung; für beide Länder besteht ein Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO). Die Daten bleiben dabei am Standort Limburg gespeichert und sind dort von Telesherpa selbst verschlüsselt (Anlage 1). Außerdem betrifft es den Inhalt von E-Mails, die über Apple versandt werden (Anlage 2 Teil B Nr. 2); Garantie EU-U.S. Data Privacy Framework bzw. Standardvertragsklauseln. Zur Geocodierung siehe Abs. 5. Für Push-Benachrichtigungen gilt Anlage 2 Teil C: Die Push-Dienste der Browser erhalten nur verschlüsselte Inhalte.

2. Maßgeblich für eine Drittlandübermittlung ist, wo die Daten verarbeitet werden, insbesondere wo ein KI-Modell ausgeführt wird, nicht, wo Entwickler oder Herausgeber des Modells ihren Sitz haben. Ein KI-Modell, das ohne Verbindung zu einem externen Modellanbieter auf eigener Hardware von Telesherpa in Deutschland läuft, führt zu keiner Drittlandübermittlung.
3. Eine Übermittlung in ein Drittland durch Telesherpa oder einen Unterauftragsverarbeiter ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss einschließlich EU-U.S. Data Privacy Framework, Standardvertragsklauseln mit Transfer Impact Assessment). Für die in Anlage 2 Teil B gekennzeichneten Fälle stimmt der Kunde mit Abschluss dieses AVV zu.
4. Übermittlungen an KI-Agenten und KI-Modelle, die der Kunde verbindet, erfolgen auf Weisung des Kunden (§ 8 Abs. 2). Ob dabei eine Drittlandübermittlung vorliegt und wie sie abgesichert wird, verantwortet der Kunde.
5. **Geocodierung über Google.** Die Geocodierung von Adressen über die Google Maps Geocoding API (onto_object_geocode; ersatzweise Nominatim/OpenStreetMap, wenn Google kein Ergebnis liefert) ist fester Bestandteil der Leistung.
 - a) **Weisung des Kunden.** Mit der Nutzung der Plattform und der Eingabe von Adressen weist der Kunde Telesherpa an, die Adressdaten zur Geocodierung an Google zu übermitteln. Übermittelt wird nur die Adresszeichenfolge bzw. die Koordinaten des Objekts, keine Namen oder sonstigen Objektdaten.
 - b) **Eigenständig Verantwortlicher.** Google handelt dabei nicht als Unterauftragsverarbeiter von Telesherpa, sondern als eigenständig Verantwortlicher nach den Google Controller-Controller Data Protection Terms (Anlage 2 Teil D). Google verarbeitet die Daten in den USA; Grundlage der Übermittlung ist das EU-U.S. Data Privacy Framework, unter dem Google LLC zertifiziert ist.
 - c) **Information der Betroffenen.** Der Kunde ist verpflichtet, die betroffenen Personen, deren Adressen er in die Plattform eingibt, über die Übermittlung an Google als eigenständig Verantwortlichen und die Verarbeitung in den USA zu informieren (Art. 13, 14 DSGVO).

§ 8 Besondere Regelungen für KI-Agenten und KI-Modelle

1. **Kein Training auf Kundendaten.** Telesherpa verwendet personenbezogene Daten und sonstige Inhalte des Kunden nicht zum Training, Feintuning oder sonstigen Verbessern von KI-Modellen, weder eigener noch solcher Dritter, es sei denn, der Kunde hat dem gesondert und ausdrücklich in Textform zugestimmt. Inhaltsfreie Metriken nach § 4 Abs. 1 bleiben zulässig.
2. **Agenten und KI-Modelle des Kunden („Bring your own model“).** Der Kunde arbeitet mit eigenen KI-Agenten und KI-Modellen, die er selbst auswählt, verbindet und betreibt.
 - a) **Verantwortung des Kunden.** Diese Agenten und Modelle liegen in der Verantwortung des Kunden. Ihre Anbieter sind je nach Ausgestaltung durch den Kunden dessen Auftragsverarbeiter oder eigenständig verantwortlich, in keinem Fall

Unterauftragsverarbeiter von Telesherpa. Der Kunde verantwortet die Rechtsgrundlage, den Vertrag mit dem Anbieter einschließlich eines eigenen AVV und die Absicherung etwaiger Drittlandübermittlungen nach Art. 44 ff. DSGVO.

b) **Keine Einflussnahme.** Telesherpa wählt diese Agenten und Modelle nicht aus, konfiguriert sie nicht und überwacht ihre Verarbeitung außerhalb der Plattform nicht. Die Rechte von Telesherpa nach AGB Ziffer 4, 5 und 9 bleiben unberührt.

c) **Rolle von Telesherpa.** Telesherpa verarbeitet die Daten, die der Agent des Kunden an die Plattform sendet oder dort abrufen, im Rahmen der Rechte des Agentenkontos und übermittelt Antworten an den Agenten (Transport und Bereitstellung). Das geschieht auf Weisung des Kunden; als Weisung gilt der Abruf durch ein vom Kunden berechtigtes Agentenkonto (§ 3 Abs. 3, 4). Für diesen Teil gilt dieser AVV.

d) Die Plattform selbst ruft für die Verarbeitung von Kundendaten kein KI-Modell auf.

3. **Agenten nur innerhalb der vergebenen Rechte.** Ein Agentenkonto erhält Zugriff ausschließlich auf die Scopes und Rechte (Lesen, Schreiben, Verwalten), die ihm der Kunde oder ein berechtigter Nutzer über Mitgliedschaften oder EinladungsCodes erteilt hat. Ohne Zuordnung besteht kein Zugriff. Ein selbst registriertes Agentenkonto ohne Einladung ist von fremden Daten isoliert. Lesen und Schreiben sind getrennte Rechte; die Prüfung erfolgt serverseitig. Telesherpa erweitert die Rechte eines Agenten nicht ohne Weisung des Kunden.

4. **Eigene KI-Agenten von Telesherpa.** Telesherpa setzt für Entwicklung, Betrieb, Sicherheitsprüfung und Support eigene, interne KI-Agenten ein. Sie und ihre Modelle sind nicht Teil der Leistung für den Kunden.

a) **Grundsatz: kein Zugriff.** Interne KI-Agenten haben keinen Zugriff auf personenbezogene Daten des Kunden. Telesherpa stellt das technisch sicher: Agenten für Code-Reviews und Konzept-Reviews haben keine Konten und keinen Zugang zu Systemen von Telesherpa und arbeiten nur mit dem Material, das ihnen ein Mensch vorlegt. Der Entwicklungsagent hat technisch keinen Zugriff auf Kundendaten, insbesondere keine Mitgliedschaft in Scopes des Kunden, keine administrative Rolle und keine Zugangsdaten zu Produktivsystemen, Datenbanken, Datensicherungen, Produktivprotokollen oder Service-Anfragen des Kunden; er arbeitet mit Programmcode, Konfiguration und synthetischen Testdaten, überträgt keine personenbezogenen Daten an den Anbieter seines Modells, und Änderungen an der Produktivplattform werden nur nach Freigabe durch die Geschäftsführung eingespielt. Einziger Administrator der Produktivplattform ist ein Mensch (Anlage 1).

b) **Keine Ausnahme.** Kein interner Agent erhält Zugriff auf personenbezogene Daten des Kunden, auch nicht im Einzelfall. Das gilt insbesondere für Agenten, deren KI-Modell außerhalb der EU bzw. des EWR ausgeführt wird, etwa über die Modell-API eines externen Anbieters.

c) **Folge.** Die Anbieter der Modelle interner Agenten sind keine Unterauftragsverarbeiter, weil diese Agenten nach lit. a und b technisch keinen Zugang zu Kundendaten haben. Gelangen

personenbezogene Daten des Kunden entgegen lit. a und b an einen solchen Agenten oder dessen Modellanbieter, behandelt Telesherpa dies als Verletzung nach § 10.

5. **Transparenz und Protokolle.** Aktionen von Agenten und Menschen werden im Änderungs- und Aktionsprotokoll festgehalten. Der Kunde erhält auf Anforderung binnen 5 Werktagen einen maschinenlesbaren Auszug des Protokolls seiner Scopes. Protokolle einschließlich Payload werden 12 Monate aufbewahrt; Zugriff haben nur benannte Administratoren von Telesherpa, Zugriffe auf Protokolle werden protokolliert. Gedankengänge oder Schlussfolgerungen des Kundenmodells speichert die Plattform nicht.
6. **Automatisierte Entscheidungen, KI-Verordnung.** Nutzt der Kunde Agenten oder Regeln für Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung (Art. 22 DSGVO), ist er für deren Zulässigkeit und menschliche Überprüfung verantwortlich. Telesherpa stellt dem Kunden auf Anfrage Informationen über die selbst betriebenen KI-Systeme bereit, soweit er sie für eigene Pflichten nach der Verordnung (EU) 2024/1689 benötigt.
7. **Öffentliche Datenbereiche (Marktplatz).** Macht der Kunde einen Datenbereich öffentlich (PUBLIC), erhalten andere Nutzer Lesezugriff. Das ist eine Offenlegung auf Weisung und in Verantwortung des Kunden. Öffentliche Datenbereiche dürfen keine personenbezogenen Daten enthalten, es sei denn, der Kunde hat dafür eine Rechtsgrundlage und dokumentiert sie bei der Freigabe.
8. **Agenten Dritter.** Betreibt oder vermittelt Telesherpa Agenten Dritter als Teil der Leistung, wird deren Anbieter vorher nach § 6 in Anlage 2 Teil B aufgenommen. Anbieter im Marktplatz werden vertraglich verpflichtet, Daten aus Scopes des Kunden nicht für eigene Zwecke zu verwenden.

§ 9 Unterstützung bei Betroffenenrechten

1. Telesherpa unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei Anträgen betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 UAbs. 1 lit. e DSGVO). Viele Anträge kann der Kunde selbst über die Plattform erfüllen (Suche, Export als CSV/JSON, Ändern oder Löschen von Objekten und Eigenschaften, Entfernen von Mitgliedern).
2. Was der Kunde nicht selbst kann, insbesondere das Löschen ganzer Scopes oder Konten oder einen Protokollauszug, erledigt Telesherpa auf Weisung binnen 5 Werktagen.
3. Wendet sich eine betroffene Person direkt an Telesherpa, leitet Telesherpa den Antrag unverzüglich an die Kontaktstelle nach § 3 Abs. 5 lit. d weiter, soweit eine Zuordnung möglich ist, und beantwortet ihn nicht selbst, außer auf Weisung.
4. Die Unterstützung über die Plattformfunktionen hinaus ist kostenfrei, solange sie im üblichen Rahmen bleibt. Außergewöhnlichen Aufwand kann Telesherpa nach vorheriger Ankündigung zu angemessenen Sätzen berechnen, außer er beruht auf einem Verstoß von Telesherpa.

§ 10 Meldung von Datenschutzverletzungen

1. Telesherpa meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO), die Daten des Kunden betrifft, unverzüglich, spätestens **24 Stunden**, nachdem

Telesherpa von der Verletzung Kenntnis erlangt oder einen begründeten Verdacht hat. Die Meldung geht an die Kontaktstelle nach § 3 Abs. 5 lit. d.

2. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der Personen und Datensätze, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen und eine Ansprechperson. Fehlende Informationen reicht Telesherpa schrittweise nach.
3. Telesherpa ergreift unverzüglich Maßnahmen zur Eindämmung und Behebung, unterstützt den Kunden bei seinen Pflichten nach Art. 33 und 34 DSGVO und stellt die Informationen für die Dokumentation nach Art. 33 Abs. 5 DSGVO bereit. Meldungen an Aufsichtsbehörden oder Betroffene im Namen des Kunden erfolgen nur auf Weisung.
4. Telesherpa informiert den Kunden auch über schwerwiegende Betriebsstörungen und sonstige Unregelmäßigkeiten bei der Verarbeitung seiner Daten.
5. Die Melde- und Incident-Prozesse von Telesherpa sind auch auf die Meldepflichten der Verordnung (EU) 2024/2847 (Cyber Resilience Act) ausgerichtet; Meldungen nach dieser Verordnung erfolgen über die Single Reporting Platform (SRP). Die Meldung an den Kunden nach Abs. 1 bleibt davon unberührt.

§ 11 Weitere Unterstützungspflichten

Telesherpa unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Datenschutz-Folgenabschätzung, vorherige Konsultation), insbesondere durch Bereitstellung von Anlage 1 und Anlage 2. § 9 Abs. 4 gilt entsprechend.

§ 12 Löschung und Rückgabe

1. **Während der Laufzeit** kann der Kunde Daten jederzeit selbst exportieren (Reports als CSV/JSON, Dateien) und löschen. Konten und ganze Scopes löscht Telesherpa auf Weisung nach § 9 Abs. 2. Als gelöscht markierte Daten werden spätestens nach **30 Tagen** endgültig entfernt.
2. **Nach Vertragsende** löscht Telesherpa nach Wahl des Kunden alle personenbezogenen Daten des Kunden oder gibt sie zurück und löscht danach die vorhandenen Kopien, sofern nicht eine Pflicht zur Speicherung nach Unions- oder mitgliedstaatlichem Recht besteht (Art. 28 Abs. 3 UAbs. 1 lit. g DSGVO). Die Rückgabe erfolgt als Export in gängigen, maschinenlesbaren Formaten (CSV/JSON und Originaldateien). Der Kunde teilt seine Wahl innerhalb von 30 Tagen nach Vertragsende mit; ohne Wahl löscht Telesherpa nach Ablauf dieser Frist.
3. **Fristen.** Die Löschung im Produktivsystem erfolgt innerhalb von 30 Tagen nach Fristablauf bzw. Weisung. Datensicherungen werden spätestens nach **35 Tagen** überschrieben; bis dahin sind sie vor Zugriff geschützt und werden nicht für andere Zwecke verwendet.
4. Bei einer Kontolöschung werden Payloads mit Inhaltsdaten aus den Protokollen entfernt; inhaltsfreie Metadaten (Zeitpunkt, Aktion, Konto) bleiben bis zum Ablauf der Frist nach § 8 Abs. 5.

6. Telesherpa bestätigt die Löschung auf Anfrage in Textform.
7. Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, sowie Daten, die Telesherpa aufgrund gesetzlicher Pflichten aufbewahren muss, darf Telesherpa über das Vertragsende hinaus für die Dauer der jeweiligen Pflicht bzw. bis zum Ablauf der Verjährung aufbewahren.
8. **Öffentliche Scopes.** Mit Vertragsende werden vom Kunden öffentlich gemachte Scopes zurückgezogen; Buchungen anderer Nutzer enden zu diesem Zeitpunkt.

§ 13 Nachweise und Kontrollrechte

1. Telesherpa stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO und diesem AVV erforderlich sind.
2. Nachweise sind insbesondere: die Selbstauskunft nach Anlage 1, Testate oder Zertifikate des Rechenzentrumsbetreibers und Ergebnisse von Penetrationstests, soweit vorhanden, sowie genehmigte Verhaltensregeln oder Zertifizierungen (Art. 40, 42 DSGVO).
3. **Inspektionen.** Der Kunde oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der kein Wettbewerber von Telesherpa ist, darf Inspektionen durchführen (Art. 28 Abs. 3 UAbs. 1 lit. h DSGVO). Sie umfassen alle Verarbeitungsorte nach Anlage 2 Teil A. Inspektionen werden mit einer Frist von mindestens 14 Tagen angemeldet, finden während der Geschäftszeiten ohne Störung des Betriebs statt, regelmäßig höchstens einmal pro Kalenderjahr; anlassbezogene Prüfungen, etwa nach einer Datenschutzverletzung, sind jederzeit möglich.
4. Prüfungen beim Rechenzentrumsbetreiber richten sich nach dessen Bedingungen; Telesherpa leitet dessen Nachweise weiter. Reichen diese nicht aus, kann der Kunde eine Prüfung durch einen unabhängigen Prüfer verlangen.
5. Jede Partei trägt ihre eigenen Kosten. Für zusätzliche, nicht anlassbezogene Prüfungen über eine pro Jahr hinaus kann Telesherpa angemessenen Aufwand berechnen.

§ 14 Haftung

1. Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis erfolgt der Ausgleich nach Art. 82 Abs. 5 DSGVO entsprechend dem jeweiligen Verantwortungsanteil.
2. **Unbeschränkte Haftung.** Telesherpa haftet unbeschränkt bei Vorsatz und grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit, nach dem Produkthaftungsgesetz, im Umfang einer übernommenen Garantie sowie gegenüber betroffenen Personen nach Art. 82 DSGVO. Diese Haftung wird durch Abs. 3 nicht beschränkt.
3. **Haftungshöchstsumme.** Im Übrigen haftet Telesherpa bei einfacher Fahrlässigkeit nur für die Verletzung wesentlicher Vertragspflichten; die Pflichten aus diesem AVV sind wesentliche Vertragspflichten im Sinne von AGB Ziffer 10. Die Haftung ist dann auf den vertragstypischen, vorhersehbaren Schaden begrenzt, insgesamt jedoch höchstens auf die Summe aller Entgelte, die der Kunde in den drei Monaten vor dem schadensbegründenden Ereignis tatsächlich an

Telesherpa gezahlt hat (rollierend; einschließlich gekaufter Credits und nutzungsabhängiger Entgelte). Maßgeblich ist der Zeitraum vom gleichen Kalendertag drei Monate vor dem Ereignis bis zum Tag vor dem Ereignis. Mehrere Schäden aus demselben Ereignis gelten als ein Schadensfall. Im Übrigen ist die Haftung bei einfacher Fahrlässigkeit ausgeschlossen.

4. Jede Partei stellt die andere von Ansprüchen Dritter frei, soweit diese auf einem von ihr zu vertretenden Verstoß gegen diesen AVV oder das Datenschutzrecht beruhen. Für den Kunden gilt das insbesondere, wenn er, seine Nutzer oder seine Agenten personenbezogene Daten ohne Rechtsgrundlage einbringen, verarbeiten lassen oder öffentlich machen.

§ 15 Schlussbestimmungen

1. Rangfolge in Fragen des Datenschutzes: individuell vereinbarte Datenschutzregelungen (einschließlich eines vom Kunden gestellten und von Telesherpa angenommenen AVV), dann dieser AVV, dann die AGB.
2. **Änderungen.** Telesherpa darf diesen AVV einseitig nur ändern, soweit eine geänderte Rechtslage oder behördliche Vorgabe dies erfordert oder das Schutzniveau für den Kunden nicht sinkt; Telesherpa teilt solche Änderungen mindestens 30 Tage vorher in Textform mit. Andere Änderungen bedürfen der Zustimmung des Kunden in Textform. Widerspricht der Kunde einer einseitigen Änderung, kann er den Vertrag zum Wirksamwerden kündigen; § 6 Abs. 4 Satz 3 gilt entsprechend. Änderungen der Anlagen 1 und 2 richten sich nach § 5 Abs. 2 und § 6.
3. **Versionen.** Telesherpa hält jede Version dieses AVV mit Datum unter <https://www.telesherpa.com/avv> abrufbar.
4. Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen unberührt. An ihre Stelle tritt die gesetzliche Regelung, insbesondere Art. 28 DSGVO.
5. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand nach AGB Ziffer 13.
6. Werden die Daten des Kunden bei Telesherpa durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert Telesherpa den Kunden unverzüglich und weist die Dritten darauf hin, dass die Verfügungsbefugnis über die Daten beim Kunden liegt.

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

Version 1.0, Stand 21.10.2026.

1. Vertraulichkeit

Maßnahme	Beschreibung
Zutritt Rechenzentrum	Rechenzentrum der OVH GmbH am Standort Limburg (Anlage 2 Teil B Nr. 1); physische Sicherung nach den Maßnahmen und Zertifizierungen der OVH GmbH (laut deren AVV u. a. ISO 27001, ISO 27017, ISO 27018, ISO 27701)
Zugang Nutzer	Konten mit Passwort, Option Passkey; Aktivierung per E-Mail-Code bzw. Einladungscode; Bearer-Token 10 h, Refresh-Token 30 Tage mit Rotation und Replay-Schutz;

	MCP-Session verfällt nach 12 h Inaktivität; Web-Session 30 min
Zugang Schnittstellen	OAuth 2.1 mit Authorization Code und PKCE (S256), Dynamic Client Registration; ohne Token nur 6 öffentliche Tools (Registrierung, Login, Status, Preisliste)
Passwortspeicherung	Gesalzener Hash mit einem aktuellen Verfahren (Argon2id oder bcrypt)
Zugang Administration	Einzigster Administrator von Servern, Datenbank, Speicher, Backups und Produktivprotokollen ist ein Mitglied der Geschäftsführung; Zugang per SSH-Schlüssel mit zweitem Faktor, protokolliert. Für den Notfall wird ein versiegelter Notfallzugang im Telesherpa-Büro verwahrt; jede Öffnung wird dokumentiert, die Zugangsdaten werden danach erneuert. Keine Zugänge für KI-Agenten (§ 8 Abs. 4 lit. a)
Zugriffskontrolle	Rechte ausschließlich über Scope-Mitgliedschaften (can_read, can_write, can_manage_scope), serverseitig geprüft; Lesen und Schreiben getrennt; Agentenkonten ohne Einladung isoliert. Einschränkung: kein Recht je Objekt, Schreibrecht gilt für alle Objekte eines Scopes
Admin-Werkzeuge	Scope-übergreifende Werkzeuge (Suche über Scopes, Aktionsprotokolle, Nutzer- und Importverwaltung, Reports mit eigenem SQL) nur für benannte menschliche Administratoren; Report-SQL nur mit Scope-Bedingung; jeder scope-übergreifende Zugriff wird protokolliert
Trennung	Mandantentrennung über Scopes; Entwicklungs- und Testumgebung getrennt von der Produktion, nur mit synthetischen Daten
Verschlüsselung gespeicherter Daten	Datenhaltung auf einem hochverfügbaren NAS (HA-NAS) bei OVH, von Telesherpa selbst mit LUKS verschlüsselt; OVH hat keinen Schlüssel. Nach einem Neustart wird der Speicher von Hand durch den Administrator entsperrt
Interne KI-Agenten	Code-Review-Agent (Sebastian) und Konzept-Review-Agent (Falco): keine Konten, kein Systemzugang. Entwicklungsagent (Herbert): nur Code, Konfiguration und synthetische Testdaten, kein Zugriff auf Kundendaten, keine personenbezogenen Daten an seinen Modellanbieter, Produktiv-Deployments nur nach Freigabe durch die Geschäftsführung.

2. Integrität

Maßnahme	Beschreibung
Transport	Verschlüsselte Übertragung mit TLS 1.2 oder höher; kein vorgeschaltetes CDN; Domains bei deutschem Registrar
Geocodierung	Übermittlung nur der Adresszeichenfolge bzw. Koordinaten an Google (ersatzweise Nominatim), verschlüsselt (TLS); keine Namen oder sonstigen Objektdaten; Google als eigenständig Verantwortlicher in den USA auf Grundlage des Data Privacy Framework (§ 7 Abs. 5)
Push-Verschlüsselung	Web Push nach W3C Push API / RFC 8030 mit VAPID

	(RFC 8292). Titel, Text und Ziel-URL jeder Benachrichtigung werden nach RFC 8291 (aes128gcm) Ende-zu-Ende verschlüsselt; nur der Browser des Empfängers kann sie entschlüsseln. Der Push-Dienst sieht nur Chiffretext, Endpunkt und Zeitpunkt. Die Plattform (ontouser/push.php) akzeptiert nur Endpunkte der vier Push-Dienste nach Anlage 2 Teil C
Eingabekontrolle	Änderungs- und Aktionsprotokoll je Konto einschließlich Agenten, Aufbewahrung 12 Monate (§ 8 Abs. 5)
Automatisierte Abläufe	Regeln mit begrenzter Tiefe (max_depth 3), Dedupe-Fenster 60 s, Zeitlimit für Funktionen 100 bis 30.000 ms, Rollen-Whitelist; Anlegen nur mit can_manage_scope; keine Webhook-Effekte nach außen
Tool-Kennzeichnung	MCP-Tools mit Annotations (readOnlyHint, destructiveHint, idempotentHint, openWorldHint)
Plattformweite Zähler	Zählwerte, die Werkzeuge plattformweit ausgeben (z. B. Anzahl Objekte je Typ), werden auf die Scopes des Aufrufers beschränkt

3. Verfügbarkeit und Belastbarkeit

Maßnahme	Beschreibung
Datensicherung	Verschlüsselte Backups bei OVH am Standort Limburg, keine Spiegelung an andere Standorte; täglich, Aufbewahrung 35 Tage, Wiederherstellungstest mindestens einmal pro Quartal
Redundanz	Hochverfügbarer Speicher (HA-NAS) innerhalb des Standorts Limburg; Strom-, Klima- und Netzredundanz nach den Maßnahmen der OVH GmbH. Derzeit kein zweiter Standort: Ein schwerer Schaden am Standort kann Produktivdaten und Sicherungen zugleich treffen
Überwachung	Health-Endpunkt (/health) mit automatischer Alarmierung
Missbrauch und Überlast	Abweisung bei fehlendem Guthaben (HTTP 402); Begrenzung der Anfragerate
Wiederherstellung	Ziel: Wiederherstellung binnen 24 h, Datenverlust höchstens 24 h (gilt nicht bei Verlust des gesamten Standorts, siehe Redundanz)
Verfügbarkeit	Keine geschuldete Verfügbarkeit (AGB Ziffer 8)

4. Regelmäßige Überprüfung

Maßnahme	Beschreibung
Datenschutz-Management	Verantwortlich: Geschäftsführung; jährliche Überprüfung dieser Anlage, erstmals bis 31.10.2027
Änderungen am Code	Prüfung durch Code- und Konzept-Review-Agenten ohne Produktivdaten; Einspielen in die Produktion nur nach Freigabe durch die Geschäftsführung
Schwachstellen	Sicherheitsupdates für Server und Abhängigkeiten binnen 14 Tagen, kritische binnen 72 h
Incident-Response	Meldekette: Erkennung → Geschäftsführung → Meldung an den Kunden binnen 24 h (§ 10); Prozesse auf den Cyber Resilience Act ausgerichtet, Meldungen nach dem CRA über die Single Reporting Platform (SRP)

Verpflichtung	Schriftliche Verpflichtung aller Personen auf Vertraulichkeit vor Zugang zu Kundendaten
Voreinstellungen	Neue Konten ohne fremde Rechte; PUBLIC nur durch einen Administrator von Telesherpa
Auftragskontrolle	Unterauftragsverarbeiter nur nach § 6, mit AVV und geprüften Garantien

Anlage 2: Verarbeitungsorte und Unterauftragsverarbeiter

Version 1.0, Stand 21.10.2026. Änderungen nach § 6 Abs. 3, Liste mit Historie unter <https://www.telesherpa.com/avv>. Leistungen mit **Drittlandbezug** sind fett gekennzeichnet.

Teil A: Verarbeitungsorte von Telesherpa

Ort	Art	Was dort verarbeitet wird	Wann
Rechenzentrum der OVH GmbH, Standort Limburg, Deutschland (Teil B Nr. 1)	Rechenzentrum	Plattform, Datenbank, Dateien, Datensicherungen; keine Spiegelung an andere Standorte	dauerhaft

Teil B: Unterauftragsverarbeiter

#	Unterauftragsverarbeiter	Leistung	Ort	Drittlandbezug / Garantie
1	OVH GmbH, Oskar-Jäger-Straße 173/K6, 50825 Köln, Amtsgericht Köln HRB 122481	Server, Datenbank, HA-NAS-Speicher, Datensicherungen	Rechenzentrum Limburg, Deutschland (nur dieser Standort)	Möglicher Fernzugriff für Sicherheit und Wartung durch die gruppeninternen Unterauftragsverarbeiter OVH Hebergement INC (Kanada) und OVH Limited (Vereinigtes Königreich); Angemessenheitsbeschluss (Art. 45 DSGVO) für beide Länder. Grundlage: AVV der OVH GmbH, Version 17.10.2025, Ziffer 6.2; Unterauftragsverarbeiterliste der OVH GmbH, Stand 16.10.2025. Weitere gruppeninterne Unterauftragsverarbeiter der OVH in EU/EWR laut dieser Liste
2	Apple: iCloud Mail mit eigener Domain. Apple Distribution	Versand von Aktivierungscodes, Benachrichtigungen und E-Mails mit	EU und USA	Drittlandbezug USA: EU-U.S. Data Privacy Framework (Apple Inc.)

	International Ltd., Hollyhill Industrial Estate, Hollyhill, Cork, Irland; Verarbeitung auch durch Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA	PDF-Anhang		zertifiziert) bzw. Standardvertragskla useln
3	KI-Modellanbieter für interne Agenten	—	—	nicht anwendbar: Interne Agenten haben keinen Zugriff auf Daten des Kunden (§ 8 Abs. 4)

Telesherpa setzt keine weiteren externen Dienste ein (keine externen Ticket-, Monitoring- oder Logging-Werkzeuge). Die Plattform selbst ruft kein KI-Modell auf.

Teil C: Zustelldienste der Browser, nur verschlüsselte Inhalte

Push-Benachrichtigungen an Web-Anwendung und PWA werden per Web Push (W3C Push API / RFC 8030, VAPID nach RFC 8292) zugestellt. Telesherpa betreibt keine eigene Push-Infrastruktur und nutzt weder APNs-Zertifikate noch das FCM-SDK. Welcher der folgenden Dienste die Benachrichtigung transportiert, bestimmt der Browser des Nutzers, nicht Telesherpa. Titel, Text und Ziel-URL sind nach RFC 8291 (aes128gcm) Ende-zu-Ende verschlüsselt; der Push-Dienst erhält **keine Inhalte im Klartext**, sondern nur Chiffretext und die zur Zustellung nötigen Metadaten (Endpunkt-Adresse des Geräts, Zeitpunkt, IP-Adresse). Die Push-Dienste transportieren die verschlüsselten Nachrichten und haben keinen Zugriff auf deren Inhalt.

Push-Dienst (Endpunkt)	Browser	Anbieter	Drittlandbezug / Garantie
push.apple.com	Safari, iOS	Apple Inc., USA	USA: EU-U.S. Data Privacy Framework
fcm.googleapis.com	Chrome, Edge (Chromium), Android	Google LLC, USA	USA: EU-U.S. Data Privacy Framework
Mozilla Push Service	Firefox	Mozilla Corporation, USA	USA: nicht unter dem Data Privacy Framework zertifiziert; Mozilla stützt Übermittlungen nach eigener Angabe auf Standardvertragsklauseln . Inhalte erreichen Mozilla nur verschlüsselt (Anlage 1)
Windows Push Notification Services	Edge (Windows)	Microsoft Corporation, USA	USA: EU-U.S. Data Privacy Framework

Andere Endpunkte weist die Plattform zurück.

Teil D: Dienste als eigenständige Verantwortliche

Die folgenden Dienste sind **keine Unterauftragsverarbeiter**. Sie handeln nach ihren eigenen Bedingungen als eigenständig Verantwortliche. Die Geocodierung über Google ist fester Bestandteil der Leistung; Telesherpa übermittelt Adressdaten auf Weisung des Kunden, die in der Nutzung der

Plattform und der Eingabe von Adressen liegt (§ 7 Abs. 5). Der Kunde informiert seine betroffenen Personen darüber.

Dienst	Anbieter	Zweck und Daten	Ort	Grundlage / Garantie
Google Maps Geocoding API (Standard)	Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland (Vertragspartner); Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Verarbeitung)	Geocodierung (onto_object_geocode): Adresszeichenfolgen von Objekten bzw. Koordinaten; technische Daten der Anfrage (Server-IP, Zeitpunkt, API-Schlüssel von Telesherpa)	USA	Google Maps Platform Terms of Service mit Google Controller-Controller Data Protection Terms (Version 11 vom 7.5.2026); Übermittlung in die USA auf Grundlage des EU-U.S. Data Privacy Framework (Google LLC zertifiziert)
Nominatim (Fallback, nur wenn kein Google-Schlüssel hinterlegt ist oder Google kein Ergebnis liefert)	OpenStreetMap Foundation, St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, Vereinigtes Königreich	Adresszeichenfolgen von Objekten	Vereinigtes Königreich, Irland, Niederlande (laut OSMF)	Nutzungs- und Datenschutzbedingungen der OSMF; Angemessenheitsbeschluss für das Vereinigte Königreich (Art. 45 DSGVO)

Keine Unterauftragsverarbeiter von Telesherpa

- **KI-Modelle und Agenten des Kunden** (z. B. Anbieter großer Sprachmodelle, Agenten-Frameworks, eigene Modelle des Kunden): Sie werden vom Kunden gewählt, verbunden und betrieben. Ihre Anbieter sind je nach Ausgestaltung Auftragsverarbeiter des Kunden oder eigenständig verantwortlich. Telesherpa übermittelt Daten an sie nur auf Weisung des Kunden; AVV und Drittlandprüfung liegen beim Kunden (§ 8 Abs. 2).
- **Modelle interner Agenten ohne Zugriff auf Kundendaten** und die Dienste, über die diese Modelle bereitgestellt werden: nicht Teil der Leistung; diese Agenten haben nach § 8 Abs. 4 lit. a und c technisch keinen Zugang zu personenbezogenen Daten des Kunden.
- **Zahlungsdienstleister (SumUp)** für den Kauf von Credits: eigene Verantwortung von Telesherpa bzw. des Zahlungsdienstleisters; siehe Datenschutzerklärung.
- **Webanalyse auf www.telesherpa.com (Ahrefs)**: nur Website, nicht Plattform; Abschaltung am 11.11.2026.
- **Domainregistrar** (Deutschland): kein Zugriff auf Kundendaten.

Anlage 3: Kontaktstellen und Ansprechpartner

Rolle	Kunde	Telesherpa
Weisungen und Erklärungen (§ 3 Abs. 5)	Jedes vom Kunden berechnigte Konto, auch ein Agentenkonto	—
Kontaktstelle (§ 3 Abs. 5 lit. d)	Kontaktmöglichkeit des Betreibers nach AGB Ziffer 4 und Plattform-Postfach	—

Optional: natürliche Person als Ansprechpartner	Name, Funktion, E-Mail-Adresse, falls der Kunde dies wünscht	—
Empfang von Weisungen und Service-Anfragen	—	service@telesherpa.com
Meldungen zu Datenschutzverletzungen (§ 10)	an die Kontaktstelle	Meldungen des Kunden an adg@telesherpa.com
Ansprechpartner Datenschutz	nach Angabe des Kunden	Geschäftsführung, adg@telesherpa.com