Vertrag über die Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO) · Fassung vom 01.11.2026

Verantwortlicher	Auftragsverarbeiter
der Kunde von PilotStay gemäß den Angaben bei der Registrierung	Antonino Neglia, PilotStay Langwiese 19, 63477 Maintal legal@pilotstay.de

§ 1 Gegenstand, Dauer, Art und Zweck

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Nutzung von PilotStay nach den Allgemeinen Geschäftsbedingungen (AGB). Gegenstand, Art und Zweck der Verarbeitung, Datenarten und Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags einschließlich einer Testphase. Die Pflichten nach § 8 gelten darüber hinaus fort.

§ 2 Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist nach dem Recht der Union oder Deutschlands zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen diese Pflicht vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

(2) Weisungen sind dieser Vertrag, die AGB und die vom Verantwortlichen im Dashboard getroffenen Einstellungen (insbesondere Betriebsmodus und Antwortregeln). Weitere Weisungen erteilt der Verantwortliche in Textform.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich.

§ 3 Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß **Anlage 2**. Er darf sie an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für den Einsatz der in **Anlage 3** genannten Unterauftragsverarbeiter.

(2) Über beabsichtigte Hinzuziehungen oder Ersetzungen informiert der Auftragsverarbeiter den Verantwortlichen mindestens vier Wochen vorher in Textform. Der Verantwortliche kann aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Kommt keine Einigung zustande, kann der Verantwortliche den Vertrag zum Zeitpunkt der Änderung kündigen.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Er haftet gegenüber dem Verantwortlichen für deren Einhaltung.

§ 6 Übermittlung in Drittländer

Eine Übermittlung in Länder außerhalb des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-US Data Privacy Framework) oder von EU-Standardvertragsklauseln. Die jeweilige Garantie ist in Anlage 3 genannt.

§ 7 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Art. 12 bis 23 DSGVO. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.

(2) Er unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(3) Eine Verletzung des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie ihm vorliegen.

§ 8 Löschung und Rückgabe

Nach Ende des Vertrags gibt der Auftragsverarbeiter dem Verantwortlichen nach dessen Wahl die Daten zurück (Export) oder löscht sie, spätestens 30 Tage nach Vertragsende, sofern keine Pflicht zur Speicherung nach dem Recht der Union oder Deutschlands besteht. Daten in Sicherungskopien werden im regulären Backup-Zyklus gelöscht, spätestens 7 Tage nach Löschung im Live-System.

§ 9 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieser Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer nach Vorankündigung von mindestens vier Wochen. Nachweise können vorrangig durch aktuelle Dokumentation, Zertifikate oder Prüfberichte der Unterauftragsverarbeiter erbracht werden.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag den AGB in Fragen des Datenschutzes vor.

(2) Es gilt das Recht der Bundesrepublik Deutschland.

(3) Dieser Vertrag wird elektronisch abgeschlossen (Art. 28 Abs. 9 DSGVO), indem der Verantwortliche ihm bei der Registrierung zustimmt.

Anlage 1 – Gegenstand der Verarbeitung

Art und Zweck	Abruf von Buchungs- und Gästedaten aus dem Channel Manager des Verantwortlichen; Analyse eingehender Gästenachrichten mithilfe von KI; Erstellung, Prüfung (Guardian) und Versand von Antworten nach den Einstellungen des Verantwortlichen; Benachrichtigung des Verantwortlichen bei dringenden Gästeanliegen per E-Mail, SMS oder Anruf; Speicherung und Protokollierung zur Nachvollziehbarkeit.
Datenarten	Name; E-Mail; Telefonnummer; Personenzahl; Buchungsdaten (Zeitraum, Unterkunft, Preise, Zahlungsstand); Notizen zur Buchung; Inhalte von Nachrichten im Volltext; Sprache; technische Kennungen aus dem Channel Manager. Ausweis-, Pass- und Zahlungskartendaten werden nicht verarbeitet.
Betroffene Personen	Gäste und Buchungsanfragende des Verantwortlichen; ggf. Mitarbeiter und Co-Hosts des Verantwortlichen.
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Teilen Gäste in Nachrichten von sich aus solche Daten mit (z. B. zur Gesundheit), werden sie nur im Rahmen der Beantwortung verarbeitet.

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

Verschlüsselung	Übertragung ausschließlich per TLS; verschlüsselte Speicherung beim Datenbankanbieter (Encryption at rest).
Zugriffskontrolle	Zugriff nur nach Anmeldung; Passwörter gehasht gespeichert; Trennung der Kundendaten durch Row Level Security auf allen Datenbanktabellen.
Administrativer Zugang	Zugang zu Datenbank-, Hosting- und KI-Konsolen nur durch den Inhaber, abgesichert mit Zwei-Faktor-Authentifizierung.
Schutz von Zugangsschlüsseln	API-Schlüssel des Channel Managers (z. B. Smoobu) werden ausschließlich serverseitig gespeichert und sind nur für Server-Funktionen zugänglich; in der Oberfläche werden höchstens die letzten vier Zeichen angezeigt.
Verfügbarkeit	Tägliche Datensicherung durch den Datenbankanbieter, Aufbewahrung der Sicherungen 7 Tage.
Datenminimierung	An den KI-Anbieter werden Gastnamen und Telefonnummern nur als Platzhalter und E-Mail-Adressen ersetzt übermittelt; übermittelt werden der Nachrichtentext sowie für die Antwort nötige Angaben zu Unterkunft und Reisezeitraum.
KI-Verarbeitung	Anthropic darf die übermittelten Inhalte vertraglich nicht zum Training von KI-Modellen verwenden.
Protokollierung	Ausgehende Nachrichten und Entscheidungen des Guardian-Prüfschritts werden protokolliert.
Löschung	Löschung nach Vertragsende gemäß § 8.
Organisation	Verpflichtung auf Vertraulichkeit; festgelegter Ablauf für Datenschutzvorfälle (Erkennen, Bewerten, Melden).

Anlage 3 – Unterauftragsverarbeiter

Anbieter	Leistung	Ort der Verarbeitung	Garantie bei Drittland
Supabase Pte. Ltd., Singapur	Datenbank und Anmeldung	EU (Frankfurt am Main)	EU-Standardvertragsklauseln (Module 2/3) im Supabase-DPA

Anbieter	Leistung	Ort der Verarbeitung	Garantie bei Drittland
Anthropic Ireland, Limited (Dublin)	KI-Modell Claude zur Analyse von Gästenachrichten und Erstellung von Antworten	USA	EU-Standardvertragsklauseln (Module 2/3) im Data Processing Addendum
Vercel Inc., USA	Hosting der Anwendung	USA	EU-Standardvertragsklauseln im Vercel-DPA
Resend (Plus Five Five, Inc.), USA	Versand von E-Mail-Benachrichtigungen; Notfall-Mails enthalten Gastname, Buchungsnummer und einen Nachrichtenauszug	USA	EU-US Data Privacy Framework; EU-Standardvertragsklauseln
Twilio Inc., USA	SMS und Anrufe bei Notfall-Benachrichtigungen (Gastname, Buchungsnummer, Nachrichtenauszug)	USA	EU-US Data Privacy Framework; BCR; EU-Standardvertragsklauseln
Eleven Labs Inc., New York, USA	Sprachausgabe für Notfall-Anrufe	USA	EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln im ElevenLabs-DPA

Der Channel Manager des Verantwortlichen (z. B. Smoobu) ist kein Unterauftragsverarbeiter von PilotStay. Ihn beauftragt der Verantwortliche selbst.