Vereinbarung über eine Auftragsverarbeitung

gemäß Art. 28 DSGVO – Majourny FlexCo

abgeschlossen zwischen

Der Verantwortliche („Auftraggeber“)	Der Auftragsverarbeiter („Auftragnehmer“)
[Name des Hotels][Anschrift][Firmenbuchnummer]	Majourny FlexCoWeinheberstr. 164320 Perg

Verantwortlicher und Auftragsverarbeiter im Folgenden gemeinsam „Parteien“ genannt.

Präambel

Der Verantwortliche hat den Auftragsverarbeiter mit der Erbringung der in der zugrunde liegenden Vereinbarung bzw. dem individuellen Angebot/der Auftragsbestätigung beschriebenen Leistungen beauftragt. Teil der Leistungserbringung ist die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen. Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Erfüllung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung über eine Auftragsverarbeitung (im Folgenden „AVV“ genannt). Diese AVV ist als Ergänzung zu den Allgemeinen Geschäftsbedingungen von Majourny sowie dem individuellen Angebot bzw. der Auftragsbestätigung zu verstehen und deren Erfüllung wird nicht gesondert vergütet, sofern dies nicht ausdrücklich vereinbart ist.

1. Gegenstand und Dauer der Verarbeitung

1.1. Gegenstand dieses AVV ist die Durchführung folgender Aufgaben durch Majourny im Auftrag des Hotels:

- Bereitstellung und Betrieb einer KI-gestützten Gästekommunikationsplattform (AI Concierge) zur automatisierten Beantwortung von Gästeanfragen über WhatsApp, SMS, Web und weitere Kanäle
- Verarbeitung von Gästeprofil- und Kontaktdaten im Rahmen des digitalen Check-in-Prozesses
- Durchführung proaktiver Gästekommunikation (Pre-Arrival, In-Stay, Post-Stay) im Auftrag des Hotels
- Verarbeitung von Buchungs- und Aufenthaltsdaten zum Zweck des intelligenten Upselling und der personalisierten Angebotsausspielung (Upsell Engine)
- Entgegennahme und Weiterleitung von Gästefeedback sowie Unterstützung des Bewertungsmanagements
- Interne Aufgaben- und Kommunikationskoordination zwischen Hotelabteilungen (TeamHub) unter Verarbeitung relevanter Mitarbeiter- und Auftragsdaten
- Speicherung und Verwaltung von Gästepräferenzen und -profilen zur Personalisierung künftiger Aufenthalte

1.2. Einzelheiten zu Kategorien betroffener Personen, Kategorien personenbezogener Daten, Art und Zweck der Verarbeitung sowie zur Dauer der Verarbeitung sind in Anhang I dieser AVV abschließend beschrieben.

1.3. Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem (1) Monat zum Monatsende schriftlich gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Diese AVV endet automatisch mit Beendigung des Hauptvertrages.

2. Pflichten des Auftragnehmers (Majourny)

2.1. Weisungsgebundenheit

a) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern dies nicht wegen eines wichtigen öffentlichen Interesses untersagt ist. Der Auftraggeber kann während der gesamten Vertragsdauer weitere Weisungen erteilen; diese sind stets zu dokumentieren.

b) Erhält der Auftragnehmer einen behördlichen Auftrag zur Herausgabe von Daten des Auftraggebers, informiert er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich und verweist die Behörde an diesen. Eine Verarbeitung für eigene Zwecke des Auftragnehmers bedarf eines gesonderten schriftlichen Auftrags.

c) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die Verordnung (EU) 2016/679 oder sonstige geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

2.2. Zweckbindung und Vertraulichkeit

Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich für die in Anhang I genannten Zwecke, sofern keine weiteren Weisungen des Auftraggebers vorliegen. Der Auftragnehmer stellt sicher, dass alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung bleibt auch nach Beendigung der Tätigkeit bzw. des Ausscheidens beim Auftragnehmer aufrecht.

2.3. Sicherheit der Verarbeitung

a) Der Auftragnehmer ergreift mindestens die in Anhang II beschriebenen technischen und organisatorischen Maßnahmen (TOMs), um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO zu gewährleisten. Dies umfasst den Schutz vor Zerstörung, Verlust, Veränderung sowie unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten („Verletzung des Schutzes personenbezogener Daten“).

b) Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung der Leistungserbringung unbedingt erforderlich ist („need-to-know-Prinzip“).

2.4. Sensible Daten

Soweit die Verarbeitung ausnahmsweise besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Gesundheitsdaten, etwa im Rahmen von Ernährungsbesonderheiten/Allergien) oder Daten über strafrechtliche Verurteilungen betrifft, wendet der Auftragnehmer angemessene zusätzliche Schutzmaßnahmen an und verarbeitet diese Daten nur im für die Leistungserbringung erforderlichen Mindestumfang.

2.5. Unterstützung der Betroffenenrechte

Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen, damit der Auftraggeber seinen Pflichten nach Kapitel III DSGVO (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch, automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen nachkommen kann, und stellt ihm die dafür erforderlichen Informationen zur Verfügung. Erhält der Auftragnehmer einen Antrag einer betroffenen Person, informiert er den Auftraggeber unverzüglich hierüber und beantwortet den Antrag nicht selbst, es sei denn, er wurde hierzu ausdrücklich ermächtigt.

2.6. Unterstützung bei Art. 32–36 DSGVO

Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung von dessen Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datensicherheitsmaßnahmen, der Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, der Benachrichtigung betroffener Personen, der Datenschutz-Folgenabschätzung sowie der vorherigen Konsultation der Aufsichtsbehörde. Näheres zu Umfang und Anwendungsbereich dieser Unterstützung ergibt sich aus Anhang II.

2.7. Meldung von Datenschutzverletzungen

a) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragnehmer diese dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden. Die Meldung enthält mindestens: (i) eine Beschreibung der Art der Verletzung einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze; (ii) Kontaktdaten einer Anlaufstelle für weitere Informationen; (iii) die voraussichtlichen Folgen sowie die ergriffenen oder vorgeschlagenen Abhilfe- und Abmilderungsmaßnahmen.

b) Können nicht alle Informationen gleichzeitig bereitgestellt werden, enthält die ursprüngliche Meldung die zu diesem Zeitpunkt verfügbaren Informationen; weitere Informationen werden ohne unangemessene Verzögerung nachgereicht.

c) Der Auftragnehmer unterstützt den Auftraggeber bei der fristgerechten Erfüllung von dessen Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) und betroffenen Personen (Art. 34 DSGVO).

2.8. Verarbeitungsverzeichnis

Der Auftragnehmer führt für die vorliegende Auftragsverarbeitung ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

2.9. Nachweis- und Prüfrechte

a) Die Parteien müssen die Einhaltung der in dieser AVV festgelegten Pflichten nachweisen können. Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der unmittelbar aus Art. 28 DSGVO hervorgehenden Pflichten erforderlich sind.

b) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle eingeräumt, auch durch von ihm beauftragte, zur Verschwiegenheit verpflichtete Dritte. Prüfungen können auch Inspektionen der Räumlichkeiten bzw. Einrichtungen des Auftragnehmers umfassen und werden mit angemessener Vorankündigung (mindestens 10 Werktage), unter Wahrung der Betriebsgeheimnisse und ohne unangemessene Störung des Betriebs, durchgeführt. Bei der Entscheidung über eine Prüfung kann der Auftraggeber einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.

c) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) auf Anfrage die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse etwaiger Prüfungen, zur Verfügung.

3. Ort der Datenverarbeitung und internationale Datenübermittlung

3.1. Datenverarbeitungstätigkeiten werden grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums durchgeführt.

3.2. Jede Übermittlung personenbezogener Daten durch den Auftragnehmer an ein Drittland oder eine internationale Organisation – insbesondere im Zusammenhang mit dem Einsatz von Unterauftragsverarbeitern gemäß Anhang III – erfolgt ausschließlich auf Grundlage einer geeigneten Garantie im Sinne von Kapitel V der Verordnung (EU) 2016/679, insbesondere eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45 DSGVO) oder von Standardvertragsklauseln gemäß Art. 46 Abs. 2 DSGVO. Der Auftraggeber erklärt sich mit dem Einsatz der in Anhang III gelisteten Unterauftragsverarbeiter auf dieser Grundlage einverstanden.

4. Unterauftragsverarbeiter

4.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern für folgende Tätigkeiten: Cloud-Hosting und Infrastruktur, Datenbank-Dienste, KI-gestützte Sprach- und Textverarbeitung, Zustellung von Nachrichten über WhatsApp, E-Mail und SMS sowie sonstige technische Hilfsdienste, die zur Erbringung der vertraglich vereinbarten Leistungen erforderlich sind.

4.2. Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Unterauftragsverarbeiter sind in Anhang III aufgeführt und gelten mit Unterzeichnung dieser AVV als genehmigt.

4.3. Der Auftragnehmer unterrichtet den Auftraggeber mindestens 14 Tage im Voraus schriftlich über beabsichtigte Änderungen dieser Liste (Hinzufügung oder Ersetzung von Unterauftragsverarbeitern) und räumt dem Auftraggeber ausreichend Zeit ein, um vor der Beauftragung Einwände zu erheben. Erhebt der Auftraggeber innerhalb dieser Frist keinen Einwand, gilt die Änderung als genehmigt.

4.4. Beauftragt der Auftragnehmer einen Unterauftragsverarbeiter, erfolgt dies im Wege eines Vertrags, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt, die für den Auftragnehmer gemäß dieser AVV gelten. Der Auftragnehmer stellt dem Auftraggeber auf Verlangen eine –

erforderlichenfalls hinsichtlich Geschäftsgeheimnissen geschwärzte – Kopie dieser Vereinbarung zur Verfügung.

4.5. Der Auftragnehmer haftet gegenüber dem Auftraggeber in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten nachkommt, und benachrichtigt den Auftraggeber, sofern der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

5. Verstöße gegen die AVV und Beendigung

a) Kommt der Auftragnehmer seinen Pflichten aus dieser AVV nicht nach, kann der Auftraggeber – unbeschadet der Bestimmungen der DSGVO – anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis die Einhaltung wiederhergestellt oder der Vertrag beendet ist.

b) Der Auftraggeber ist berechtigt, die AVV, soweit sie die Verarbeitung personenbezogener Daten betrifft, zu kündigen, wenn (i) die Einhaltung nach Aussetzung gemäß lit. a nicht innerhalb einer angemessenen Frist, jedenfalls innerhalb eines Monats, wiederhergestellt wurde, (ii) der Auftragnehmer in erheblichem Umfang oder fortdauernd gegen diese AVV oder die DSGVO verstößt, oder (iii) der Auftragnehmer einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde nicht nachkommt.

c) Der Auftragnehmer ist berechtigt, die AVV zu kündigen, wenn der Auftraggeber auf der Erfüllung rechtswidriger Weisungen besteht, nachdem er gemäß Klausel 2.1 lit. c über den Verstoß informiert wurde.

6. Löschung und Rückgabe der Daten

Nach Beendigung dieser AVV löscht der Auftragnehmer nach Wahl des Auftraggebers alle in dessen Auftrag verarbeiteten personenbezogenen Daten und bescheinigt dies dem Auftraggeber, oder er gibt sämtliche personenbezogenen Daten an den Auftraggeber zurück und löscht bestehende Kopien – sofern nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten eine Pflicht zur weiteren Speicherung besteht. Verarbeitet der Auftragnehmer die Daten in einem speziellen technischen Format, gibt er die Daten in diesem Format oder, auf Wunsch des Auftraggebers, in einem gängigen anderen Format heraus. Bis zur Löschung oder Rückgabe gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser AVV.

Für den Auftraggeber:	**Für den Auftragnehmer:**
.....[Ort, Datum, Name samt Funktion]	.....[Ort, Datum, Name samt Funktion]

Anhang I – Beschreibung der Verarbeitung

Kategorien betroffener Personen

- Hotelgäste (Erwachsene und minderjährige Begleitpersonen)
- Potenzielle Gäste (im Rahmen von Pre-Arrival-Kommunikation und Buchungsanfragen)
- Mitarbeiterinnen und Mitarbeiter des Auftraggebers (im Rahmen der TeamHub-Funktion)

Kategorien personenbezogener Daten

- Identifikationsdaten: Name, Geburtsdatum, Staatsangehörigkeit, Reisedokumentdaten (Passnummer, Ausweisdaten gemäß Meldepflicht)
- Kontaktdaten: E-Mail-Adresse, Telefonnummer (insbesondere WhatsApp-Nummer), Postanschrift
- Buchungs- und Aufenthaltsdaten: Anreise-/Abreisedatum, Zimmernummer, Zimmerkategorie, Buchungskanal, Aufenthaltsdauer, gebuchte Zusatzleistungen
- Zahlungsdaten: Kreditkartendaten zur Vorautorisierung (tokenisiert, keine Vollspeicherung von Kartennummern), Rechnungsdaten
- Kommunikationsinhalte: Nachrichten zwischen Gästen und dem AI Concierge, Serviceanfragen, Beschwerden
- Präferenz- und Verhaltensdaten: Zimmerpräferenzen, Ernährungsbesonderheiten, Allergien, genutzte Serviceleistungen, Bestellhistorie
- Bewertungsdaten: Feedback-Antworten, Zufriedenheitsbewertungen
- Technische Daten: IP-Adresse, Browsertyp, Aktivitätsprotokolle
- Mitarbeiterdaten des Auftraggebers: Name, E-Mail-Adresse, Abteilung, Aufgabenzuweisungen im Rahmen des TeamHub

Art der Verarbeitung

Der Auftragnehmer verarbeitet Gäste-, Buchungs- und Aufenthaltsdaten mittels KI-gestützter Software zur automatisierten Gästekommunikation, zum digitalen Check-in, zur internen Aufgabenkoordination (TeamHub) sowie zur personalisierten Angebotsausspielung (Upsell Engine). Mithilfe intelligenter Algorithmen werden Kommunikation, Serviceangebote und interne Abläufe individualisiert und automatisiert.

Zweck(e) der Verarbeitung

- Automatisierung und Personalisierung der Gästekommunikation und des Gästeerlebnisses
- Digitaler Check-in und Verwaltung von Gästeprofilen
- Koordination interner Hotelabläufe (Housekeeping, Instandhaltung, Front Office) über TeamHub
- Umsatzsteigerung durch personalisiertes, automatisiertes Upselling
- Unterstützung des Bewertungs- und Feedbackmanagements

Dauer der Verarbeitung

Die Dauer der Verarbeitung richtet sich nach der zwischen den Parteien geschlossenen Vereinbarung zur Erbringung der Dienstleistung (vgl. Klausel 1.3 dieser AVV) sowie den gesetzlichen Aufbewahrungspflichten (z. B. Meldepflichten, Abgabenrechtliche Aufbewahrungsfristen).

Anhang II – Technisch-organisatorische Maßnahmen (TOM)

Entsprechend den bestehenden technisch-organisatorischen Maßnahmen des Auftragnehmers anzupassen und regelmäßig zu aktualisieren.

A. Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☒ Schlüssel	☐ Magnet-/Chipkarten
☐ Alarmanlagen	☐ Videoanlage

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☒ Kennwörter (inkl. regelmäßiger Änderung)	☒ Verschlüsselung von Datenträgern
☒ Automatische Sperrmechanismen	☒ Zwei-Faktor-Authentifizierung
☒ Separater Nutzeraccount je Mitarbeiter	☒ Trennung von Produktiv- und Testsystem

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☒ Standard-Berechtigungsprofile auf „need-to-know-Basis“	☒ Standardprozess für Berechtigungsvergabe
☒ Protokollierung von Zugriffen	☒ Sichere Aufbewahrung von Speichermedien
☒ Periodische Überprüfung vergebener Berechtigungen	☒ Verteilung der Administratorenrechte auf mehrere Personen

Pseudonymisierung: Sofern für die jeweilige Verarbeitung möglich, werden primäre Identifikationsmerkmale entfernt und gesondert aufbewahrt.

☒ Ja	☐ Nein

B. Datenintegrität

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung durch:

☒ Verschlüsselung von Datenträgern	☒ Verschlüsselung von Dateien
☒ Verschlüsselung der elektronischen Übertragung (TLS)	☒ Virtual Private Networks (VPN)

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden durch:

☒ Protokollierung	☒ Dokumentenmanagement

C. Verfügbarkeit und Belastbarkeit

☒ Backup-Strategie (online/offline, on-/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV)
☒ Virenschutz	☒ Firewall
☒ Meldewege und Notfallpläne	☒ Security Checks auf Infrastruktur-/Applikationsebene

Rasche Wiederherstellbarkeit:

☒ Ja	☐ Nein

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

☒ Datenschutz-Management inkl. Mitarbeiterschulungen	☒ Führen eines Verarbeitungsverzeichnisses
☒ Benennung eines Datenschutzbeauftragten/-koordinators	☒ Verpflichtung der Mitarbeiter zur Vertraulichkeit
☒ Incident-Response-Management	☒ Liste aller Dienstleister/Tools (Vendor Management)
☒ Regelmäßige Datenschutzaudits	☒ Datenschutzfreundliche Voreinstellungen (Privacy by Default)

Auftragskontrolle: Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers durch:

☒ Eindeutige Vertragsgestaltung	☒ Formalisiertes Auftragsmanagement
☒ Strenge Auswahl von Unterauftragsverarbeitern	☒ Nachkontrollen

Anhang III – Liste der Unterauftragsverarbeiter

Liste der zum Zeitpunkt der Unterzeichnung dieser AVV genehmigten Unterauftragsverarbeiter. Änderungen erfolgen gemäß Klausel 4.3.

Unternehmen	Anschrift	Leistung	Drittlandstransfer
Vercel Inc.	440 N. Barranca Ave #4133, Covina, CA 91723, USA	Hosting-Dienstleister	Angemessenheitsbeschluss (**EU-US Data Privacy Framework**) **Art. 45 DSGVO** *(bzw. Art. 46 Abs. 2 lit. c DSGVO)*
Supabase, Inc.	548 Market St, San Francisco, CA 94104, USA	Datenbank-Dienstleister	Standardvertragsklauseln (**SCC**) & EU-US Data Privacy Framework **Art. 45 DSGVO** *(bzw. Art. 46 Abs. 2 lit. c DSGVO)*
PostHog, Inc.	2261 Market Street, Suite 4008, San Francisco, CA 94114, USA	Produkt Analytics	Angemessenheitsbeschluss (**EU-US Data Privacy Framework**) bzw. SCC **Art. 45 DSGVO** *(bzw. Art. 46 Abs. 2 lit. c DSGVO)*
Google Gemini (Google LLC)	Gordon House, Barrow Street, Dublin 4, Irland	KI-gestützte Sprachverarbeitung	Angemessenheitsbeschluss (**EU-US Data Privacy Framework**) / Alternative Transfer Solutions & **SCC Art. 45 DSGVO**

			(bzw. Art. 46 Abs. 2 lit. c DSGVO)