Vertrag zur Auftragsverarbeitung Ospitra Stay, Serve und Rent

Fassung 2026-11-03b. Freigegeben am 03.11.2026. Löst die Fassung 2026-11-03 ab, bevor diese veröffentlicht wurde; geändert ist nur die Angabe zum Datenschutz im Kopf.

Zwischen dem Betrieb ("Sie", Verantwortlicher) und der billiton internet services GmbH, Tölzer Str. 1, 82031 Grünwald ("wir", Auftragsverarbeiter) nach Art. 28 DSGVO. Teil des Vertrags über Ospitra Stay, Serve und Rent nach unseren AGB.

Ansprechpartner für den Datenschutz: datenschutz@ospitra.com. Benennen wir einen Datenschutzbeauftragten, teilen wir Ihnen Namen und Kontakt in Textform mit.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten, die wir bei der Bereitstellung von Ospitra Stay, Serve und Rent für Sie vornehmen, einschließlich der Website Ihres Betriebs mit Buchungsstrecke, des Supports und der Datenübernahme aus einem Vorgängersystem.

(2) Der AVV gilt ab Vertragsschluss, auch für eine Datenübernahme vorher, bis zur vollständigen Löschung nach § 12.

§ 2 Art und Zweck der Verarbeitung

(1) Art: Erheben über Ospitra und die Buchungsstrecke, Speichern, Anzeigen, Verändern, Auswerten für Ihre Berichte, Übermitteln an Empfänger, die Sie bestimmen, Sperren und Löschen.

(2) Zweck: Ihren Betrieb zu führen, also Reservierungen, Aufenthalte, Bewirtung, Verleih, Rechnungen, Kasse, Meldeschein, Kurtaxe, Statistik, Housekeeping, Zutritt und Kommunikation mit Gästen; Ihre Website und Buchungsstrecke zu betreiben; Ihnen Support zu leisten.

(3) Empfänger, die Sie bestimmen, sind etwa Ihr Zahlungsinstitut, Ihr Kanalmanager, Ihre Gemeinde, das Statistische Landesamt, das Finanzamt und der Anbieter Ihrer Schließanlage. Wir übermitteln nur, wenn Sie die Anbindung eingerichtet oder die Übermittlung freigegeben haben. Diese Empfänger sind keine Unterauftragsverarbeiter von uns.

(4) Wir verarbeiten die Daten nicht für eigene Zwecke. Ausnahmen sind abschließend: die Zahlungsumsätze Ihres Betriebs ohne Angaben zu Gästen für die Abrechnung (AGB § 8 Abs. 3), und Lösungstexte geschlossener Supportanfragen, nachdem ein Filter Namen, Kontaktdaten, Zimmernummern, Daten und Beträge entfernt hat, um die Hilfe von Ospitra zu verbessern.

§ 3 Art der Daten

Bereich	Daten
Gäste und Mitreisende	Name, Anschrift, Kontaktdaten, Geburtsdatum, Staatsangehörigkeit, Ausweisangaben soweit das Meldegesetz sie verlangt, Aufenthalte, Reservierungen, Wünsche, Notizen, Kurtaxmerkmale
Firmenkunden	Ansprechpartner, Kontaktdaten, Rechnungsangaben, Zugehörigkeit von Gästen
Zahlungen und Rechnungen	Folios, Rechnungen, Beträge, Zahlungsart, Referenzen des Zahlungsinstituts; keine Kartennummern und keine Kartendaten
Restaurant	Tischreservierungen, Bestellungen, Kassenbelege, Buchungen auf Zimmer
Verleih	Kunden, Verleihvorgänge, Kautionen, Schäden, Zustandsfotos
Zutritt	Zutrittsmittel und -zeiträume, soweit eine Schließanlage angebunden ist
Kommunikation	Nachrichten und E-Mails an Gäste mit Versandstand

Bereich	Daten
Website	Anfragen und Buchungen über die Buchungsstrecke, technische Protokolle
Mitarbeiter	Name, Dienstadresse, Rolle, Bedienerkennung, Zugangs- und Zugriffsprotokolle, Aufgaben im Housekeeping
Fotos	Mängel, Fundsachen, Zustand von Verleihobjekten

Besondere Kategorien nach Art. 9 DSGVO erhebt Ospitra nicht gezielt. Sie können in Freitexten stehen, etwa eine Allergie als Wunsch. Erfassen Sie sie, tragen Sie dafür die Rechtsgrundlage.

§ 4 Betroffene Personen

Gäste und Mitreisende, Ansprechpartner von Firmenkunden und Reisebüros, Restaurantgäste, Kunden des Verleihs, Besucher Ihrer Website und Ihrer Buchungsstrecke, Ihre Mitarbeiter, Fundsachenverlierer.

§ 5 Weisungen

(1) Wir verarbeiten die Daten nur auf Ihre dokumentierte Weisung. Weisungen sind dieser Vertrag, die Einstellungen Ihres Betriebs in Ospitra und die Handlungen Ihrer Mitarbeiter in Ospitra. Weitere Weisungen erteilen Inhaber Ihres Betriebs in Textform.

(2) Gibt ein Inhaber in Ospitra einem Vertriebspartner oder uns den Zugriff auf Ihren Betrieb frei, ist diese Freigabe Ihre dokumentierte Weisung, im angezeigten Umfang und Zeitraum. Die Freigabe nennt den Wortlaut der Weisung in ihrer Fassung; wir speichern die Fassung zur Freigabe.

(3) Notzugang: Sie weisen uns vorab an, ohne Freigabe nur lesend auf Ihren Betrieb zuzugreifen, wenn beide Bedingungen erfüllt sind: Wir haben Sie über Inhaber und Vertriebspartner zweimal binnen einer Stunde vergeblich zu erreichen versucht, und Daten oder Betrieb Ihres Hauses sind in Gefahr. Der Notzugang dauert höchstens vier Stunden und wird nicht verlängert. Sie erhalten sofort eine automatische Meldung und binnen 24 Stunden nach dem Ende einen Bericht.

(4) Ist eine Weisung nach unserer Ansicht rechtswidrig, weisen wir Sie unverzüglich darauf hin. Sind wir gesetzlich zu einer anderen Verarbeitung verpflichtet, teilen wir Ihnen das vorher mit, soweit das Gesetz es erlaubt.

(5) Sperre zum Schutz des Systems: Besteht der Verdacht, dass ein Zugang missbraucht wird, dürfen wir ihn ohne Ihre Zustimmung sperren. Wir löschen dabei nichts und melden die Sperre sofort Ihnen und dem Betroffenen. Besteht der Verdacht eines Zugriffs auf Ihre Daten, gilt zusätzlich § 11.

§ 6 Vertraulichkeit

(1) Wir setzen nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Unsere Mitarbeiter und die Vertriebspartner sehen Daten Ihres Betriebs nur mit Freigabe nach § 5 Abs. 2 oder im Notzugang nach § 5 Abs. 3. Jeder solche Zugriff wird protokolliert, und Sie können das Protokoll in Ospitra lesen.

§ 7 Sicherheit der Verarbeitung

Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 1 beschreibt. Wir dürfen sie durch gleichwertige oder bessere Maßnahmen ersetzen. Das Schutzniveau sinkt dadurch nicht.

§ 8 Unterauftragsverarbeiter

(1) Sie genehmigen allgemein den Einsatz weiterer Auftragsverarbeiter. Die bei Vertragsschluss eingesetzten nennt Anlage 2. Die geltende Liste mit Fassungen steht jederzeit in Ospitra. Ihr zuständiger Vertriebspartner

steht namentlich darauf, soweit er mit Freigabe Support leistet.

(2) Eine beabsichtigte Änderung teilen wir den Inhabern Ihres Betriebs per E-Mail und in Ospitra mindestens 30 Tage vor ihrem Wirksamwerden mit.

(3) Ist ein sofortiger Wechsel nötig, etwa wegen eines Ausfalls, einer Insolvenz oder eines Sicherheitsvorfalls beim bisherigen Dienst, dürfen wir sofort wechseln. Wir teilen den Wechsel spätestens am selben Tag mit Begründung mit.

(4) Sie können einer Änderung binnen 30 Tagen nach der Mitteilung aus einem sachlichen Grund des Datenschutzes widersprechen. Wir prüfen binnen 14 Tagen, ob wir Ihren Betrieb ohne den Dienst führen können, und teilen Ihnen das Ergebnis mit. Ist das nicht möglich, können Sie den Vertrag zum Wirksamwerden der Änderung kündigen, beim sofortigen Wechsel binnen 30 Tagen nach der Mitteilung. Vorausbezahlte Entgelte erstatten wir anteilig. Bis dahin läuft der Betrieb weiter.

(5) Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf die Datenschutzpflichten dieses Vertrags und haften Ihnen für dessen Pflichterfüllung.

§ 9 Unterstützung bei den Rechten der Betroffenen

(1) Ospitra bietet Ihnen Funktionen, um Auskunft zu erteilen, Daten zu berichtigen, zu sperren, zu löschen und herauszugeben.

(2) Wendet sich eine betroffene Person mit einem Anliegen zu ihren Rechten an uns, leiten wir es unverzüglich an Sie weiter und beantworten es nicht selbst, außer auf Ihre Weisung.

§ 10 Unterstützung bei Sicherheit, Folgenabschätzung und Konsultation

(1) Wir unterstützen Sie mit den Informationen, die uns vorliegen, bei der Sicherheit der Verarbeitung, bei einer Datenschutz-Folgenabschätzung und bei einer vorherigen Konsultation der Aufsichtsbehörde (Art. 32 bis 36 DSGVO).

(2) Für Stay mit Meldeschein und Schließanlage stellen wir Ihnen ein Muster einer Datenschutz-Folgenabschätzung bereit. Die Folgenabschätzung selbst führen Sie als Verantwortlicher durch.

§ 11 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Wir melden Ihnen eine Verletzung des Schutzes personenbezogener Daten, die Ihren Betrieb betrifft, unverzüglich, spätestens 24 Stunden nach Kenntnis, auch wenn noch nicht alle Angaben feststehen.

(2) Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, Zeitraum, einen Ansprechpartner bei uns, die wahrscheinlichen Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Was noch nicht feststeht, liefern wir schrittweise nach. Die betroffenen Gäste, Datenarten und den Zeitraum stellen wir aus den Protokollen für Ihren Betrieb zusammen.

(3) Betrifft eine Verletzung mehrere Betriebe, erhält jeder nur die Angaben zu seinem eigenen Betrieb. Über die Meldung an die Aufsichtsbehörde und die Benachrichtigung der Betroffenen entscheiden Sie.

§ 12 Löschung und Herausgabe

(1) Während der Laufzeit löschen Sie Daten mit den Funktionen von Ospitra und nach den Fristen, die Sie in Ihrem Betrieb einstellen. Ospitra löscht außerdem selbst:

- Fotos einer Mängelmeldung 12 Monate nach Erledigung des Mangels (einstellbar von 6 bis 60 Monaten); Fotos einer Fundsache mit deren Akte;
- Zustandsfotos und Übergabeprotokoll eines Verleihs sechs Monate nach Rückgabe, bei einem erfassten Schaden sechs Monate nach dessen Erledigung;
- Zugangs- und Zugriffsprotokolle 36 Monate nach dem Eintrag, Zugriffsprotokolle zu aufbewahrungspflichtigen Daten frühestens mit deren Frist;

- technische Protokolle nach 90 Tagen; sie enthalten keine Gast- oder Zahlungsdaten.

(2) Setzen Sie in Ospitra den Schalter "Aufbewahrung angehalten", etwa wegen einer laufenden Außenprüfung oder eines Rechtsstreits, setzt Ospitra die Löschung nach Absatz 1 bis zur Aufhebung aus.

(3) Nach dem Ende des Vertrags bleibt Ihr Datenbestand 90 Tage gesperrt erhalten. In dieser Zeit können die Inhaber Ihres Betriebs den vollständigen Herausgabebestand in gängigen Formaten herunterladen. Wir erinnern die Inhaber und Ihren Vertriebspartner beim Ende sowie 30 und 7 Tage vor Ablauf daran, dass danach unwiderruflich gelöscht wird und Ihre Aufbewahrungspflichten bei Ihnen bleiben. Danach löschen wir alle Daten Ihres Betriebs, auch ohne Ihre Bestätigung.

(4) Ist für Ihren Betrieb ein Insolvenzverfahren eröffnet und uns der Insolvenzverwalter bekannt, erinnern wir auch ihn. Die Frist nach Absatz 3 beginnt dann mit unserer Mitteilung an ihn einmal neu.

(5) Wir bewahren Daten Ihres Betriebs nach diesen Fristen nicht auf. Gesetzliche Aufbewahrungspflichten, etwa nach § 147 AO, treffen Sie.

(6) Den Herausgabebestand können Sie während der Laufzeit jederzeit abrufen. Stellen wir den Dienst ein, auch in unserer Insolvenz, können Sie ihn noch mindestens 90 Tage abrufen.

§ 13 Nachweise und Kontrollen

(1) Wir stellen Ihnen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus diesem Vertrag nötig sind. Für den Anteil der Unterauftragsverarbeiter können wir auf deren Zertifikate und Prüfberichte verweisen.

(2) Sie oder ein von Ihnen beauftragter Prüfer, der zur Verschwiegenheit verpflichtet ist, können die Einhaltung kontrollieren, auch vor Ort. Eine Kontrolle vor Ort melden Sie in Textform mit einer Frist von mindestens 14 Tagen an. Sie findet während der Geschäftszeiten statt und wahrt die Vertraulichkeit der Daten anderer Betriebe.

§ 14 Ort der Verarbeitung und Drittländer

(1) Wir speichern die Daten in der Europäischen Union, in Rechenzentren in Frankfurt am Main.

(2) Eine Übermittlung in ein Drittland findet nur statt, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Für Unterauftragsverarbeiter mit Sitz außerhalb der EU nennt Anlage 2 die Grundlage.

§ 15 Haftung und Vorrang

(1) Für die Haftung gilt § 16 der AGB. Art. 82 DSGVO bleibt unberührt.

(2) Bei Widersprüchen geht dieser AVV den AGB vor, soweit es um die Verarbeitung personenbezogener Daten in Ihrem Auftrag geht.

(3) Der AVV endet mit der Löschung nach § 12. Pflichten zur Vertraulichkeit gelten darüber hinaus.

Anlage 1: Technische und organisatorische Maßnahmen

Gegliedert nach Art. 32 Abs. 1 DSGVO. Für Rechenzentren und Infrastruktur verweisen wir auf die Nachweise der Unterauftragsverarbeiter.

1. Pseudonymisierung und Verschlüsselung

- Alle Verbindungen zu Ospitra und von Ospitra zu angebundenen Diensten laufen verschlüsselt (TLS).
- Gespeicherte Daten sind beim Hoster im Ruhezustand verschlüsselt.
- Protokolle führen Kennungen statt Gastdaten. Kartendaten erreichen Ospitra nie.
- Geheimnisse stehen ohne Wert in einem Verzeichnis mit benanntem Besitzer und festgelegter Erneuerung.

2. Vertraulichkeit

- **Zutritt:** Die Rechenzentren betreiben die Unterauftragsverarbeiter; maßgeblich sind deren Nachweise.
- **Zugang:** Persönliche Zugänge. Ein zweiter Faktor (Einmalcode aus einer App oder Passkey) ist für Inhaber, technische Rollen und unsere Mitarbeiter Pflicht. Fehlversuche werden gedrosselt und protokolliert.
- **Zugriff:** Rollen je Betrieb. Jede Rolle sieht nur, was sie für ihre Aufgabe braucht; Meldescheine sehen nur Rollen, die das erlauben.
- **Trennung:** Jeder Betrieb sieht nur seine eigenen Daten. Die Datenbank erzwingt die Trennung durch Zeilenschutz je Betrieb. Die Datenbank ist von außen nicht direkt erreichbar.
- **Fremdzugriff:** Vertriebspartner und unsere Mitarbeiter greifen nur mit Freigabe eines Inhabers zu, befristet und protokolliert; Notzugang nur nach AVV § 5 Abs. 3.
- **Übungsbetrieb:** Ein Übungsbetrieb hat eine eigene Kennung und keine Außenwirkung.

3. Integrität

- Zugangs-, Zugriffs- und Änderungsprotokoll halten fest, wer wann was gelesen oder geändert hat; Protokolle werden nur angefügt, nie geändert.
- Steuerrelevante Daten wie abgeschlossene Rechnungen und Kassenbelege sind unveränderbar; Korrekturen entstehen als neue Buchung.
- Kassenvorgänge werden durch die technische Sicherheitseinrichtung signiert.

4. Verfügbarkeit und Belastbarkeit

- Betrieb in Rechenzentren in Frankfurt am Main.
- Grenzen je Zugang schützen vor Überlastung.
- Festgelegte Ereignisse, etwa Fehlerhäufungen, Anmeldespitzen oder Verstöße gegen die Trennung der Betriebe, lösen einen Alarm aus.

5. Wiederherstellbarkeit

- Tägliche Sicherung mit Wiederherstellung auf einen Zeitpunkt.
- Ein festgelegtes Wiederherstellungsziel und ein Notfallplan.
- Regelmäßige Probe der Wiederherstellung in einer getrennten Umgebung.

6. Regelmäßige Überprüfung

- Jährliche dokumentierte Überprüfung dieser Maßnahmen.
- Änderungen an der Datenbank laufen zuerst gegen eine Probeumgebung mit Prüfreihen zur Trennung der Betriebe.

7. Auftragskontrolle

- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO und nach Anlage 2.
- Vertriebspartner sind vertraglich auf diesen AVV verpflichtet; Support über Messenger nie mit Gastdaten.
- Alle Mitarbeiter sind zur Vertraulichkeit verpflichtet.

Anlage 2: Unterauftragsverarbeiter

Stand bei Vertragsschluss. Die geltende Liste steht in Ospitra.

Unterauftragsverarbeiter	Leistung	Daten	Ort der Verarbeitung	Grundlage der Übermittlung
Supabase Inc., USA	Datenbank, Anmeldung, Dateiablage	alle Daten nach § 3	Rechenzentrum in Frankfurt am Main	EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795), zusätzlich Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
Vercel Inc., USA	Betrieb der Anwendung, der Websites und der Schnittstellen	alle Daten nach § 3, bei der Übertragung	Funktionen in der Region Frankfurt am Main	EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795), zusätzlich Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
rapidmail GmbH, Freiburg im Breisgau	Versand von E-Mails an Gäste und Mitarbeiter	Name, E-Mail-Adresse, Inhalt der Nachricht, Versandstand	Deutschland	entfällt
fiskaly GmbH, Wien	Technische Sicherheitseinrichtung, Export, Mitteilung an das Finanzamt (nur Serve)	Kassenvorgänge, Bedienerkennungen, Angaben zur Kasse	Europäische Union	entfällt
Ihr Vertriebspartner (Name in Ospitra)	First-Level-Support und Einrichtung, nur mit Freigabe	im freigegebenen Umfang	Sitz des Partners	entfällt, solange der Partner in der EU sitzt

Einen Anbieter eines Sprachmodells setzen wir derzeit nicht ein. Setzen wir einen ein, kündigen wir ihn nach § 8 an; er verarbeitet dann nur gefilterte Texte in der EU, ohne Training und ohne Speicherung.