Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · Stand: Juli 2026

Zwischen

Firma / Name (Verantwortlicher)

Anschrift

— nachfolgend „Verantwortlicher“ —

und

Spacious Living Operations GmbH, Pfotenhauerstraße 50a, 01307 Dresden
vertreten durch den Geschäftsführer Richard-Kurt Galle
— nachfolgend „Auftragsverarbeiter“ —

Präambel

Der Verantwortliche nutzt die Software „StayTax“ zur Berechnung und Meldung der Beherbergungs-/Übernachtungssteuer. Dabei speichert er personenbezogene Daten seiner Gäste in der Anwendung. Diese Daten verarbeitet der Auftragsverarbeiter ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Diese Vereinbarung ist Bestandteil des Nutzungsvertrags (AGB, abrufbar unter staytax.de/agb).

§ 1 Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung der StayTax-Anwendung. Die Dauer entspricht der Laufzeit des Nutzungsvertrags. Sie endet mit dessen Beendigung; § 10 (Löschung und Rückgabe) bleibt unberührt.

§ 2 Art und Zweck der Verarbeitung

Erhebung, Speicherung, Berechnung, Auswertung und Übermittlung von Buchungs- und Gastdaten zum Zweck der Ermittlung, Erklärung und Dokumentation der Beherbergungs-/Übernachtungssteuer, einschließlich der Erstellung amtlicher Meldeformulare, des Versands an die zuständige Behörde im Auftrag des Verantwortlichen sowie der prüfungssicheren Archivierung.

§ 3 Betroffene Personen und Datenarten

Kategorien betroffener Personen:

- Gäste bzw. übernachtungspflichtige Personen des Verantwortlichen,
- Mitarbeiter/Beauftragte des Verantwortlichen (Konto- und Teamdaten).

Datenarten:

- Gastdaten: Name, Aufenthaltszeitraum, Personenzahl (Erwachsene/Kinder), Buchungskanal,
- Entgeltdaten: Übernachtungsentgelt, Preisbestandteile, berechnete Steuer,
- Befreiungsdaten inkl. Nachweise. Hinweis: Befreiungsnachweise können besondere Kategorien personenbezogener Daten enthalten (z. B. Schwerbehinderung, medizinische Notwendigkeit — Art. 9 DSGVO). Der Verantwortliche stellt sicher, dass für deren Verarbeitung eine geeignete Rechtsgrundlage besteht,

– Konto-/Nutzungsdaten des Verantwortlichen (E-Mail, Firmendaten, Protokolldaten).

§ 4 Weisungsrecht

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO). Weisungen werden grundsätzlich durch die Nutzung der Funktionen der Anwendung erteilt (z. B. Anlage von Buchungen, Freigabe und Versand einer Meldung). Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich.

§ 5 Vertraulichkeit

Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

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

Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen. Sie werden dem Stand der Technik entsprechend fortgeschrieben; ein Sicherheitsniveau unterhalb des vereinbarten ist unzulässig.

§ 7 Unterauftragsverarbeiter

Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern (Art. 28 Abs. 2 DSGVO); die aktuell eingesetzten sind in Anlage 2 aufgeführt. Über beabsichtigte Änderungen (Hinzufügen/Ersetzen) informiert der Auftragsverarbeiter vorab in Textform; der Verantwortliche kann aus wichtigem, datenschutzrechtlichem Grund binnen 14 Tagen widersprechen. Mit jedem Unterauftragsverarbeiter bestehen Verträge mit Pflichten entsprechend dieser Vereinbarung.

§ 8 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Mitteln bei der Erfüllung der Betroffenenrechte (Art. 12–23 DSGVO; u. a. durch Export-, Korrektur- und Löschfunktionen der Anwendung) sowie bei den Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung), soweit ihm dies möglich ist.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Auftragsdaten betrifft, unverzüglich nach Bekanntwerden und unterstützt ihn bei seinen Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO).

§ 10 Löschung und Rückgabe

Nach Beendigung des Nutzungsvertrags stehen dem Verantwortlichen die Exportfunktionen der Anwendung zur Verfügung (u. a. vollständiger Datenexport, Meldungs-Archiv). Der Auftragsverarbeiter löscht die Auftragsdaten nach Vertragsende, spätestens jedoch nach Ablauf einer Übergangsfrist von 90 Tagen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Konto-Löschfunktion bewirkt die vollständige Löschung auf Veranlassung des Verantwortlichen.

§ 11 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieser Vereinbarung zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO). Kontrollen erfolgen vorrangig durch Auskünfte, vorhandene Testate und Zertifikate der Unterauftragsverarbeiter; Vor-Ort-Kontrollen nach angemessener Ankündigung zu üblichen Geschäftszeiten.

§ 12 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO sowie den Regelungen des Nutzungsvertrags (AGB).

§ 13 Schlussbestimmungen

Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Bei Widersprüchen zu den AGB gehen die Regelungen dieser Vereinbarung hinsichtlich des Datenschutzes vor.

Unterschriften

Ort, Datum	Ort, Datum
Unterschrift Verantwortlicher	Unterschrift Auftragsverarbeiter

Anlage 1 — Technische und organisatorische Maßnahmen

(Art. 32 DSGVO)

- Transportverschlüsselung (TLS) für sämtliche Verbindungen,
- Verschlüsselung der Daten im Ruhezustand beim Datenbank-Dienstleister,
- zusätzliche anwendungsseitige Verschlüsselung hinterlegter Zugangsdaten (z. B. PMS-API-Schlüssel),
- Datenhaltung in der EU (Region Frankfurt am Main),
- mandantenbezogene Zugriffskontrolle auf Datenbankebene (Row Level Security) und Rollenmodell (Eigentümer / Bearbeiter / Lesend),
- Protokollierung sicherheits- und meldungsrelevanter Aktionen (Audit-Log),
- regelmäßige Datensicherungen durch den Datenbank-Dienstleister,
- Trennung von Produktions- und Entwicklungsumgebungen.

Anlage 2 — Unterauftragsverarbeiter

(Stand: Juli 2026)

- Supabase, Inc. — Datenbank, Authentifizierung, Datei-Speicher; Datenhaltung: EU (Frankfurt am Main),
- Vercel Inc. (USA) — Hosting und Auslieferung der Anwendung; Übermittlung auf Grundlage des EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln,
- Resend, Inc. (USA) — E-Mail-Versand (z. B. System- und Meldungs-E-Mails); Übermittlung auf Grundlage der EU-Standardvertragsklauseln.