

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Art. 28 DSGVO — Auftragsverarbeitungsvertrag (AVV)

ENTWURF, Stand 03.09.2026. Er ist nach bestem Wissen und Gewissen aus dem Quelltext und der laufenden Anlage geschrieben, aber **nicht anwaltlich geprüft**. Vor der ersten Verwendung gegenüber einem Kunden muss ein Rechtsanwalt darüber gesehen haben. Was hier über die Software behauptet wird, ist am 03.09.2026 gemessen worden; die Belegstellen stehen in docs/recht/AVV-BELEG.md. Ändert sich die Software, ändert sich dieser Vertrag mit — sonst wird er zur Falschauskunft gegenüber den Gästen des Kunden.

Zwischen

dem Verantwortlichen — im Folgenden „Kunde“ —

Name, Anschrift und Vertretungsberechtigter des Kunden

und

dem Auftragsverarbeiter — im Folgenden „Space Booking“ —

Pascal Reischl
Josef Mayer-Gasse 5/8/10
2340 Mödling
Österreich
inbox@pascalreischl.com

wird der folgende Vertrag geschlossen. Er ergänzt die zwischen den Parteien geschlossene Nutzungsvereinbarung über den Dienst Space Booking (spacebooking.pascalreischl.com) — im Folgenden „Hauptvertrag“ — und geht ihm bei Widersprüchen in Fragen des Datenschutzes vor.

§ 1 Gegenstand und Dauer

- (1) Space Booking stellt dem Kunden eine Terminbuchungsseite zur Verfügung. Die Gäste des Kunden buchen darüber Termine; die dabei anfallenden personenbezogenen Daten verarbeitet Space Booking ausschließlich im Auftrag und nach Weisung des Kunden.
- (2) **Verantwortlicher für die Daten der Gäste ist der Kunde.** Er entscheidet über Zwecke und Mittel: er legt die Terminarten an, bestimmt die Zeiten, wählt die Pflichtfelder und entscheidet, ob und welchen eigenen Kalender er verbindet.
- (3) Dieser Vertrag beginnt mit dem Hauptvertrag und endet mit ihm. Er kann nicht gesondert gekündigt werden, solange der Hauptvertrag läuft.
- (4) Nicht Gegenstand dieses Vertrags sind die Daten des **Kunden selbst** (Kontodaten, Anmeldedaten, Abrechnungsdaten). Für sie ist Space Booking selbst Verantwortlicher; die Einzelheiten stehen in der Datenschutzerklärung unter /datenschutz.

§ 2 Art, Zweck, Datenarten, betroffene Personen

- (1) **Art der Verarbeitung:** Erheben, Speichern, Ordnen, Auslesen, Verwenden, Übermitteln an den vom Kunden verbundenen Kalender und an den Gast per E-Mail, Einschränken und Löschen.
- (2) **Zweck:** Zustandekommen, Verwaltung, Änderung und Absage von Terminen zwischen dem Kunden und dessen Gästen sowie der Versand der zugehörigen Nachrichten.
- (3) **Kreis der Betroffenen:** die Gäste des Kunden — also Personen, die auf der Buchungsseite des Kunden einen Termin buchen, verschieben oder absagen.
- (4) **Arten der Daten:** siehe **Anlage 3**. Sie ist abschließend: was dort nicht steht, verarbeitet Space Booking über diesen Vertrag nicht.
- (5) **Besondere Kategorien** nach Art. 9 DSGVO sind nicht Gegenstand dieses Vertrags. Der Kunde stellt sicher,

dass er keine Pflichtfelder einrichtet und keine Terminarten benennt, die solche Daten erheben oder aus dem Namen der Terminart offenlegen. Space Booking kann das technisch nicht verhindern: das Freitextfeld „Nachricht an uns“ und die Namen der Terminarten sind vom Kunden frei belegbar.

§ 3 Weisungsrecht

- (1) Space Booking verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden, einschließlich der Übermittlung in ein Drittland. Dieser Vertrag und die Einstellungen, die der Kunde in seinem Konto vornimmt, sind die Standardweisung.
- (2) Weitere Weisungen erteilt der Kunde in Textform an inbox@pascalreischl.com. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
- (3) Hält Space Booking eine Weisung für rechtswidrig, teilt er dies dem Kunden unverzüglich mit und darf die Ausführung bis zur Bestätigung aussetzen.
- (4) Ist Space Booking nach Unionsrecht oder mitgliedstaatlichem Recht zu einer Verarbeitung verpflichtet, teilt er dem Kunden diese Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 4 Pflichten von Space Booking

Space Booking

- a) verarbeitet die Daten nur wie in § 2 und § 3 beschrieben;
- b) trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (**Anlage 1**) und hält sie während der Vertragsdauer aufrecht; er darf sie fortentwickeln, solange das Schutzniveau nicht unterschritten wird;
- c) verpflichtet Personen, die Zugang zu den Daten haben, zur Vertraulichkeit (§ 5);
- d) setzt weitere Auftragsverarbeiter nur nach Maßgabe von § 7 ein;
- e) unterstützt den Kunden nach § 6 und § 8;
- f) benennt als Ansprechpartner für den Datenschutz: Pascal Reischl, inbox@pascalreischl.com. Ein Datenschutzbeauftragter ist nach Art. 37 DSGVO nicht zu benennen; die Voraussetzungen liegen nicht vor;
- g) berichtigt, löscht oder schränkt die Verarbeitung ein, wenn der Kunde es anweist;
- h) führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 5 Vertraulichkeit

- (1) Space Booking wird derzeit ohne Beschäftigte betrieben. Zugang zu den Daten hat allein Pascal Reischl als Betreiber, der von Gesetzes wegen und durch diesen Vertrag zur Vertraulichkeit verpflichtet ist.
- (2) Werden künftig Personen beschäftigt oder beauftragt, verpflichtet Space Booking sie **vor** dem ersten Zugang schriftlich auf die Vertraulichkeit; die Verpflichtung wirkt über das Ende ihrer Tätigkeit hinaus.

§ 6 Unterstützung des Kunden

- (1) Space Booking unterstützt den Kunden bei der Einhaltung der Art. 32 bis 36 DSGVO, soweit dem Kunden die dafür nötigen Angaben nicht selbst vorliegen.
- (2) **Meldung einer Verletzung.** Wird Space Booking eine Verletzung des Schutzes personenbezogener Daten des Kunden bekannt, meldet er sie dem Kunden **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntnis, in Textform. Die Meldung beschreibt, soweit bekannt: Art der Verletzung, betroffene Datenarten, ungefähre Zahl der Betroffenen, wahrscheinliche Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Die Frist nach Art. 33 Abs. 1 DSGVO gegenüber der Aufsichtsbehörde läuft für den **Kunden**; er meldet.
- (3) Space Booking meldet nicht selbst an eine Aufsichtsbehörde, es sei denn, der Kunde weist ihn dazu an.

§ 7 Weitere Auftragsverarbeiter

- (1) Der Kunde stimmt dem Einsatz der in **Anlage 2** genannten weiteren Auftragsverarbeiter zu (allgemeine schriftliche Genehmigung nach Art. 28 Abs. 4 DSGVO).
- (2) Space Booking unterrichtet den Kunden über jede beabsichtigte Änderung **mindestens 30 Tage im Voraus**

in Textform. Der Kunde kann innerhalb dieser Frist aus einem datenschutzrechtlichen Grund widersprechen. Widerspricht er, darf er den Hauptvertrag zum Wirksamwerden der Änderung außerordentlich kündigen.

(3) Space Booking erlegt jedem weiteren Auftragsverarbeiter dieselben Datenschutzpflichten auf, die ihn nach diesem Vertrag treffen, und haftet gegenüber dem Kunden für dessen Verhalten wie für eigenes.

(4) **Keine Auftragsverarbeiter im Sinne dieses Paragraphen** sind Dienste, die der **Kunde selbst** mit seinem Konto verbindet — insbesondere sein eigener Kalender bei Google, Microsoft oder einem CalDAV-Anbieter. Verbindet der Kunde einen solchen Kalender, übermittelt Space Booking auf seine Weisung TerminiDaten dorthin. Für dieses Verhältnis ist der Kunde gegenüber seinem Anbieter selbst verantwortlich und schließt die nötigen Vereinbarungen selbst.

§ 8 Rechte der betroffenen Personen

(1) Die Rechte der Gäste macht der **Kunde** ihnen gegenüber wahr. Space Booking beantwortet Anfragen von Gästen nicht selbst, sondern leitet sie unverzüglich an den Kunden weiter.

(2) Space Booking unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Der Kunde kann die Daten eines Gastes über seine Oberfläche einsehen, berichtigen und löschen; darüber hinausgehende Unterstützung leistet Space Booking auf Anfrage in Textform.

(3) Über eine automatische Löschrfrist (Anlage 3) hinaus löscht Space Booking auf Weisung des Kunden ohne unangemessene Verzögerung.

§ 9 Nachweise und Kontrollen

(1) Space Booking stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen.

(2) Der Nachweis wird in der Regel durch die jeweils aktuelle Fassung von **Anlage 1** und durch die Bestätigungen der Unterauftragsverarbeiter geführt.

(3) Eine Kontrolle vor Ort ist nach Anmeldung mit einer Frist von 14 Tagen während üblicher Geschäftszeiten und höchstens einmal je Kalenderjahr zulässig, sofern nicht ein besonderer Anlass vorliegt. Sie darf den Betrieb nicht unverhältnismäßig stören und die Vertraulichkeit der Daten anderer Kunden nicht gefährden. Der Kunde trägt die Kosten seiner Kontrolle.

§ 10 Löschung und Rückgabe

(1) Nach Ende des Hauptvertrags löscht Space Booking alle im Auftrag verarbeiteten Daten **innerhalb von 30 Tagen**, es sei denn, das Unionsrecht oder mitgliedstaatliche Recht verpflichtet zur Aufbewahrung.

(2) Vor der Löschung kann der Kunde die Herausgabe in einem gängigen Format verlangen. Das Verlangen ist innerhalb von 30 Tagen nach Vertragsende in Textform zu stellen.

(3) **Sicherungskopien** sind in die Löschung eingeschlossen. Sie werden nicht gesondert gelöscht, sondern laufen mit dem Generationenwechsel aus; der Bestand umfasst sieben tägliche Stände, sodass die Daten spätestens **sieben Tage** nach der Löschung aus dem laufenden Betrieb auch dort verschwunden sind. Bis dahin werden sie ausschließlich zur Wiederherstellung verwendet.

(4) Die Löschung wird dem Kunden auf Verlangen in Textform bestätigt.

§ 11 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Regelungen des Hauptvertrags.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses.

(2) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt, was ihrem Zweck am nächsten kommt.

(3) Es gilt österreichisches Recht unter Ausschluss des Kollisionsrechts. Die zwingenden Vorschriften der DSGVO und des Datenschutzrechts am Sitz des Kunden bleiben unberührt.

Ort, Datum · Der Kunde

Ort, Datum · Space Booking

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

Stand 03.09.2026. Alle Angaben sind an der laufenden Anlage gemessen.

1. Vertraulichkeit

Zutritt. Die Verarbeitung findet auf einem Server der Hetzner Online GmbH im Rechenzentrum **Falkenstein, Deutschland** statt. Für den physischen Zutritt gelten die zertifizierten Maßnahmen von Hetzner (ISO/IEC 27001).

Zugang. Der Zugang zum Server erfolgt ausschließlich über SSH mit einem Ed25519-Schlüssel; die Anmeldung mit Passwort ist abgeschaltet. Die Datenbank hört nur auf der Rückschleife (localhost) und ist von außen nicht erreichbar.

Zugriff. Der Dienst läuft als eigener, nicht privilegierter Benutzer. Geheimnisse (Verschlüsselungs- und Sitzungsschlüssel, OAuth-Geheimnisse, Mailpasswort) liegen als `systemd`-Credentials verschlüsselt auf der Platte und stehen nur dem laufenden Prozess zur Verfügung; sie stehen **nicht** in der Prozessumgebung.

Mandantentrennung. Jede Abfrage ist auf das Konto des Kunden bezogen; die Zuordnung wird nicht aus der Anfrage übernommen, sondern serverseitig aus der Sitzung bestimmt.

Verschlüsselung.

- **Übertragung:** ausschließlich TLS. HTTP wird auf HTTPS umgeleitet, HSTS ist mit einem Jahr gesetzt.
- **Gespeicherte Zugangsdaten Dritter:** die OAuth-Token der vom Kunden verbundenen Kalender liegen mit **AES-256-GCM** in einer Umschlagverschlüsselung; der Schlüssel steht nie in einer SQL-Anweisung und damit in keinem Abfrageprotokoll.
- **Gastdaten:** liegen in gewöhnlichen Spalten der PostgreSQL-Datenbank, **nicht zusätzlich spaltenweise verschlüsselt**. Die Platte des Servers ist **nicht** verschlüsselt (ext4 ohne LUKS). Der Schutz beruht hier auf Zutritts-, Zugangs- und Zugriffskontrolle, nicht auf Kryptographie. (*Offener Punkt, siehe Abschnitt 5.*)

2. Integrität

Eingabekontrolle. Änderungen an Buchungen sind mit Zeitstempeln versehen. Der Versand von Nachrichten läuft über eine Ausgangstabelle, die jeden Versuch festhält.

Weitergabekontrolle. Nach außen gehen Daten nur an: den vom Kunden verbundenen Kalender, den Mailversand (Anlage 2) und den Gast selbst. Es gibt keine Analysedienste, keine Werbenetzwerke und kein Contentnetzwerk. Die Buchungsseite lädt keine fremden Ressourcen nach; die Content-Security-Policy steht auf `default-src 'none'`.

Trennungskontrolle. Die öffentliche Gast-API schreibt keine Cookies und liest keine Sitzung.

3. Verfügbarkeit und Belastbarkeit

Sicherung. Täglich um 03:20 UTC ein vollständiger `pg_dump` im Custom-Format, mit `zstd` komprimiert. Es werden **sieben** tägliche Stände vorgehalten.

Offener Punkt, ehrlich benannt: die Sicherungen liegen derzeit **auf derselben Platte wie die Datenbank**. Ein Plattenausfall verlöre beide. Ein externes Ziel ist eingeplant und noch nicht eingerichtet. Solange das so ist, schützt die Sicherung gegen Bedienfehler und fehlerhafte Migrationen, nicht gegen einen Hardwareausfall.

Wiederherstellung. Der Stand lässt sich mit `pg_restore` einspielen; das Verfahren ist in `scripts/backup-holen.sh` beschrieben.

Betriebsbereitschaft. Der Dienst wird von `systemd` überwacht und nach einem Absturz neu gestartet. Eine Auslieferung, die den Gesundheitsendpunkt nicht grün beantwortet, wird automatisch zurückgerollt.

Abwehr. `nginx` begrenzt die Zahl der Anfragen je Adresse.

4. Verfahren zur Überprüfung

Prüfung. Der Quelltext trägt eine automatisierte Testsuite, die vor jeder Auslieferung läuft. Die Löschfristen und die Rechtstexte sind durch Tests an ihre Quelle gebunden; ändert sich eine Frist im Schema, ohne dass der Text folgt, schlägt die Prüfung fehl.

Protokolle. Zugriffsprotokolle des Webserver werden nach **14 Tagen** gelöscht. Auf den Pfaden der Gäste protokolliert der Webserver keine Zugriffe. Wird eine Anfrage wegen Überlast abgewiesen, hält das Fehlerprotokoll die IP-Adresse fest; auch dieses wird nach 14 Tagen gelöscht.

Datenschutz durch Voreinstellung. Pflichtfeld ist allein die E-Mail-Adresse. Name, Telefonnummer und Nachricht sind freiwillig. Aus fremden Kalendern werden ausschließlich Anfang und Ende belegter Zeiten gespeichert — keine Titel, keine Orte, keine Beschreibungen, keine Teilnehmer.

5. Offene Punkte

Diese Anlage nennt sie, statt sie wegzulassen:

1. Sicherungen liegen auf derselben Platte wie die Datenbank (Abschnitt 3).
2. Keine Verschlüsselung der Gastdaten im Ruhezustand (Abschnitt 1).
3. Kein dokumentierter, geprobter Wiederanlauf mit gemessener Wiederherstellzeit.

Anlage 2 — Weitere Auftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Datenarten
Hetzner Online GmbH , Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server und Rechenzentrum	Falkenstein, Deutschland	alle in Anlage 3 genannten
Google Ireland Ltd. , Gordon House, Barrow Street, Dublin 4, Irland	Versand der Bestätigungs-, Änderungs- und Absagemails über Google Workspace (smtp.gmail.com)	EU mit möglicher Übermittlung in die USA	E-Mail-Adresse des Gastes, Name, Termindaten und der Inhalt der jeweiligen Nachricht

Zu Google: Die Übermittlung in die USA stützt sich auf den EU-US Data Privacy Framework, an dem Google LLC teilnimmt, sowie ergänzend auf die Standardvertragsklauseln der Kommission.

Kein Unterauftragsverarbeiter ist der vom Kunden selbst verbundene Kalender (Google, Microsoft, CalDAV/Apple) — siehe § 7 Abs. 4.

Anlage 3 — Datenarten, Herkunft und Löschfristen

Vom Gast selbst angegeben

Daten	Pflicht?	Löschung
E-Mail-Adresse	ja — das einzige Pflichtfeld	730 Tage nach dem letzten Termin
Name	nein	730 Tage nach dem letzten Termin
Telefonnummer	nein	730 Tage nach dem letzten Termin
Nachricht an den Kunden (max. 500 Zeichen)	nein	730 Tage nach dem letzten Termin
Grund der Absage (max. 1000 Zeichen)	nein	730 Tage nach dem letzten Termin

Vom Browser des Gastes gemeldet

Daten	Zweck	Löschung
Zeitzone	richtige Uhrzeit in der Bestätigung	mit dem Gastdatensatz
Sprache	Sprache der Bestätigung	mit dem Gastdatensatz

Vom Dienst erzeugt

Daten	Zweck	Löschung
Buchungsnummer, Zeitraum, gewählte Terminart, Status	die Buchung selbst	bleibt ohne Personenbezug bestehen
Prüfwert des Zugangslinks aus der Bestätigungsmail	Ansehen, Verschieben, Absagen ohne Konto	24 Stunden nach dem Termin
Kennwert (HMAC) der E-Mail-Adresse	Wiedererkennung desselben Gastes ohne Klartextsuche	mit dem Gastdatensatz

Aus dem verbundenen Kalender des Kunden

Daten	Löschung
Anfang und Ende belegter Zeiten, Ganztagskennzeichen	mit dem Abgleich überschrieben, beim Trennen des Kalenders gelöscht

Nicht gespeichert werden Titel, Ort, Beschreibung und Teilnehmer fremder Kalendereinträge. Der Titel wird beim Abgleich im Arbeitsspeicher gegen eine Stichwortliste geprüft (etwa „Urlaub“) und danach verworfen.

Was die Löschung nach 730 Tagen bedeutet

Name, E-Mail-Adresse, Telefonnummer, Nachricht und Absagegrund werden geleert, der Gastdatensatz wird als anonymisiert gekennzeichnet. Die Buchung selbst bleibt ohne Personenbezug bestehen, damit die Zahlen des Kunden stimmen.

Die Frist ist die Voreinstellung des Kontos (`accounts.guest_retention_days`). Der Kunde kann sie kürzen; sie gilt dann für alle seine Gäste.