

Vertrag zur Auftragsverarbeitung

nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Stand: 24.08.2026

zwischen

[Name des Kunden] [Anschrift] [vertreten durch]	busical AI GmbH Fraunhoferstraße 8/2, 88239 Wangen Vertreten durch GF Kai Stückmann
im Folgenden "Auftraggeber" (Verantwortlicher)	im Folgenden "Auftragnehmer" (Auftragsverarbeiter)

Präambel

Der Auftragnehmer stellt dem Auftraggeber eine webbasierte Anwendung zur Verfügung, mit der der Auftraggeber zeitlich begrenzte Übernachtungsangebote erstellt und veröffentlicht, Anfragen und Reisewünsche von Gästen entgegennimmt und Interessenten benachrichtigt (im Folgenden „der Dienst“). Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien. Er ergänzt den zwischen den Parteien geschlossenen Vertrag über die Nutzung des Dienstes (im Folgenden „Hauptvertrag“).

§ 1 Gegenstand und Dauer der Verarbeitung

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrags.
- (2) Gegenstand des Auftrags ist der Betrieb des Dienstes einschließlich der Speicherung, Anzeige und Übermittlung der dabei anfallenden personenbezogenen Daten. Der Umfang der Leistungen ergibt sich aus dem Hauptvertrag.
- (3) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags. Er endet automatisch mit dessen Beendigung; die Pflichten nach § 10 bleiben davon unberührt.
- (4) Der Auftraggeber kann diesen Vertrag und den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 2 Art und Zweck der Verarbeitung, Datenkategorien, betroffene Personen

- (1) Die Verarbeitung umfasst das Erheben, Erfassen, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Übermitteln, Einschränken und Löschen von Daten. Sie erfolgt mit Hilfe automatisierter Verfahren.
- (2) Zweck der Verarbeitung ist die Bereitstellung des Dienstes für den Auftraggeber: die Veröffentlichung von Angeboten auf den Seiten des Auftraggebers, die Entgegennahme und Verwaltung

von Anfragen und Reisewünschen, die Benachrichtigung von Interessenten sowie die Auswertung der Nutzung ohne Personenbezug.

(3) Gegenstand der Verarbeitung sind folgende Kategorien personenbezogener Daten:

- Stamm- und Kontaktdaten von Gästen und Interessenten (Name, E-Mail-Adresse, gegebenenfalls Telefonnummer),
- Angaben zu Reisewünschen und Anfragen (Reisezeitraum, Aufenthaltsdauer, Personenzahl, gewählte Angebote),
- Kommunikationsdaten (Inhalte von Anfragen und versandten Benachrichtigungen, Nachweise über deren Einwilligung),
- Konto- und Nutzungsdaten der Beschäftigten des Auftraggebers (Anmeldedaten, Protokolle über Änderungen),
- technische Zugriffsdaten der Besucher (IP-Adresse, Zeitpunkt des Zugriffs, Geräte- und Browserinformationen).

(4) Von der Verarbeitung betroffen sind:

- Gäste, Interessenten und Besucher der Angebotsseiten des Auftraggebers,
- Beschäftigte und Beauftragte des Auftraggebers, die den Dienst bedienen.

(5) Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO sind nicht Gegenstand der Verarbeitung und dürfen über den Dienst nicht verarbeitet werden.

§ 3 Ort der Verarbeitung

(1) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Der Betrieb der Server- und Speicherinfrastruktur erfolgt bei unserem Hosting-Partner in Europa in Rechenzentren innerhalb der Europäischen Union; die namentliche Benennung enthält Anlage 2.

(2) Jede Verlagerung der Dienstleistung oder von Teilleistungen in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Für die in Anlage 2 ausgewiesene Nebenleistung mit Drittlandbezug gelten die dort genannten Garantien.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrags und auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt; ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass sie vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des

Datenschutzes vertraut gemacht wurden. Diese Verpflichtungen bestehen auch nach Beendigung dieses Vertrags fort.

(4) Der Auftragnehmer trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen, die den Anforderungen des Art. 32 DSGVO genügen. Er überprüft ihre Wirksamkeit bei gegebenem Anlass, mindestens aber jährlich, und passt sie dem Stand der Technik an; das vereinbarte Schutzniveau darf dabei nicht unterschritten werden.

(5) Der Auftragnehmer unterstützt den Auftraggeber im nötigen Umfang und soweit möglich bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO und bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(7) Der Auftragnehmer nennt dem Auftraggeber einen Ansprechpartner für den Datenschutz (Anlage 3). Soweit er gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist, teilt er dessen Kontaktdaten mit; ein Wechsel ist unverzüglich mitzuteilen.

§ 5 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Er erteilt alle Weisungen schriftlich oder in einem dokumentierten elektronischen Format; mündliche Weisungen sind unverzüglich in dieser Form zu bestätigen.

(2) Der Umfang der im Dienst standardmäßig vorgesehenen Verarbeitungen gilt als vereinbarte Grundweisung. Einstellungen, die der Auftraggeber selbst im Dienst vornimmt, gelten als dokumentierte Weisungen.

(3) Die zur Erteilung und Entgegennahme von Weisungen befugten Personen sind in Anlage 3 benannt. Ein Wechsel ist der jeweils anderen Partei unverzüglich mitzuteilen.

§ 6 Unterauftragsverhältnisse

(1) Ein Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Nebenleistungen ohne direkten Zusammenhang mit der Hauptleistung, etwa Telekommunikations-, Wartungs- oder Reinigungsleistungen, sind keine Unterauftragsverhältnisse; die Pflicht des Auftragnehmers, auch dabei Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 2 mit Name, Anschrift und Leistungsbeschreibung aufgeführten Unternehmen als Unterauftragsverarbeiter einzusetzen.

(3) Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Ersetzung oder Neubeauftragung eines Unterauftragsverarbeiters. Der Auftraggeber kann der Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von vier Wochen nach Zugang der Information widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Wird eine einvernehmliche Lösung nicht gefunden, sind beide Parteien berechtigt, diesen Vertrag und den Hauptvertrag mit einer Frist von einem Monat zu kündigen.

(4) Der Auftragnehmer wählt Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung ihrer technischen und organisatorischen Maßnahmen sorgfältig aus und erlegt ihnen vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Der Auftraggeber muss seine Kontrollrechte auch gegenüber Unterauftragsverarbeitern ausüben können.

(5) Die Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere ein Angemessenheitsbeschluss der Europäischen Kommission oder geeignete Garantien im Sinne von Art. 46 DSGVO vorliegen.

(6) Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

§ 7 Rechte betroffener Personen

(1) Für die Wahrung der Rechte der betroffenen Personen ist der Auftraggeber verantwortlich. Macht eine betroffene Person ihre Rechte nach Art. 15 ff. DSGVO gegenüber dem Auftragnehmer geltend, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter.

(2) Der Auftragnehmer berichtigt, löscht oder sperrt im Auftrag verarbeitete Daten nur entsprechend der vertraglichen Vereinbarung oder nach dokumentierter Weisung des Auftraggebers. Soweit der Dienst dem Auftraggeber entsprechende Funktionen bereitstellt, kann der Auftraggeber diese Vorgänge selbst ausführen.

§ 8 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes der im Auftrag verarbeiteten personenbezogenen Daten unverzüglich, spätestens innerhalb von 48 Stunden ab Kenntnis, an die in Anlage 3 benannte Adresse mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung enthält mindestens die Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie zu diesem Zeitpunkt vorliegen; fehlende Angaben werden nachgereicht.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang. Meldungen an Aufsichtsbehörden oder Benachrichtigungen betroffener Personen für den Auftraggeber nimmt der Auftragnehmer nur nach vorheriger Weisung vor.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit sie Bezüge zur Auftragsverarbeitung aufweisen, sowie darüber, wenn das Eigentum des Auftraggebers oder die im Auftrag verarbeiteten Daten durch Maßnahmen Dritter, etwa Pfändung oder Beschlagnahme, oder durch ein Insolvenzverfahren gefährdet werden.

§ 9 Nachweise und Kontrollrechte

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten auf Anforderung innerhalb einer angemessenen Frist durch geeignete Auskünfte und Unterlagen nach, insbesondere durch die Beschreibung der technischen und organisatorischen Maßnahmen, einschlägige Berichte über deren Überprüfung oder vorhandene Zertifikate und genehmigte Verhaltensregeln.

(2) Der Auftraggeber oder ein von ihm beauftragter Prüfer ist berechtigt, sich in angemessener Weise von der Einhaltung der getroffenen Maßnahmen und der vertraglichen Verpflichtungen zu überzeugen, einschließlich Inspektionen. Kontrollen erfolgen nach angemessener Vorankündigung, zu üblichen Geschäftszeiten, ohne vermeidbare Störung des Betriebs und in der Regel nicht häufiger als alle zwölf Monate. Soweit der Auftragnehmer aussagekräftige Nachweise nach Absatz 1 vorlegt, beschränkt sich eine Kontrolle auf Stichproben.

(3) Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, die mit ihm in einem Wettbewerbsverhältnis stehen; in diesem Fall benennt der Auftraggeber einen anderen Prüfer.

§ 10 Beendigung des Auftrags

(1) Nach Beendigung des Hauptvertrags gibt der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers in einem gängigen, strukturierten Format heraus oder löscht sie datenschutzgerecht, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Pflicht zur Speicherung besteht. Die Wahl trifft der Auftraggeber innerhalb von zwei Wochen nach Aufforderung; äußert er sich nicht, werden die Daten nach Ablauf weiterer zwei Wochen gelöscht.

(2) Die Löschung ist dem Auftraggeber auf Verlangen schriftlich oder in einem dokumentierten elektronischen Format mit Datumsangabe zu bestätigen. Der Auftragnehmer führt die Löschung auch bei Unterauftragsverarbeitern herbei.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, bewahrt der Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus auf.

§ 11 Vergütung, Haftung, Schlussbestimmungen

(1) Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung im Rahmen dieses Vertrags erfolgt nicht.

(2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für den Schaden, der durch eine ihr zuzurechnende Verletzung dieses Vertrags oder der DSGVO entstanden ist.

(3) Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB ist hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Beide Parteien behandeln alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich, auch über die Beendigung des Vertrags hinaus.

(5) Änderungen und Ergänzungen dieses Vertrags bedürfen einer schriftlichen Vereinbarung, die auch in einem dokumentierten elektronischen Format erfolgen kann. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(6) Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(7) Dieser Vertrag unterliegt deutschem Recht.

Ort, Datum

Auftraggeber

Ort, Datum

Auftragnehmer

Anlage 1: Technische und organisatorische Maßnahmen

Der Auftragnehmer hat mindestens die folgenden Maßnahmen eingerichtet und hält sie laufend aufrecht. Sie können der technischen Weiterentwicklung entsprechend angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zugangskontrolle: Der Zugang zum Dienst erfolgt ausschließlich über personalisierte Konten. Passwörter werden nur als kryptografische Prüfwerte gespeichert. Wiederholt fehlgeschlagene Anmeldeversuche werden begrenzt.
- Zugriffskontrolle: Berechtigungen werden rollenbasiert vergeben; administrative Zugänge sind auf das erforderliche Personal beschränkt.
- Trennungskontrolle: Die Daten der einzelnen Auftraggeber werden logisch strikt getrennt verarbeitet. Die Trennung wird technisch auf der Ebene des Datenzugriffs erzwungen, sodass jeder Zugriff auf den jeweiligen Auftraggeber begrenzt ist.
- Zutrittskontrolle: Der Betrieb erfolgt in professionellen Rechenzentren innerhalb der EU mit Zutrittsbeschränkung, Überwachung und Protokollierung durch den in Anlage 2 benannten Betreiber.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Übertragungskontrolle: Jede Übertragung personenbezogener Daten zwischen Besuchern, Auftraggeber und Dienst erfolgt ausschließlich über verschlüsselte Verbindungen (TLS).
- Eingabekontrolle: Änderungen an fachlichen Daten werden mit Zeitpunkt und handelndem Konto protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Es werden regelmäßig Sicherungskopien der Datenbestände erstellt und getrennt vom Produktivsystem aufbewahrt.
- Für den Störfall besteht ein erprobtes Verfahren zur Wiederherstellung aus der Sicherung.
- Die Verfügbarkeit des Dienstes wird laufend überwacht.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Die Wirksamkeit der Maßnahmen wird bei gegebenem Anlass, mindestens jährlich, überprüft und bewertet.
- Sicherheitsvorfälle werden nach einem festgelegten Ablauf erkannt, behandelt und dokumentiert (Incident-Response).
- Neue Funktionen werden vor der Bereitstellung automatisiert geprüft; Änderungen am Dienst durchlaufen ein dokumentiertes Freigabeverfahren.

Anlage 2: Genehmigte Unterauftragsverarbeiter und technische Partner

Die vertraglich vereinbarten Leistungen werden unter Beauftragung der folgenden Unternehmen erbracht. Mit deren Einsatz erklärt sich der Auftraggeber im Rahmen von § 6 einverstanden.

Unternehmen und Anschrift	Leistung	Ort der Verarbeitung, Garantien
BunnyWay d.o.o.	Betrieb der Server- und Speicherinfrastruktur sowie	Rechenzentren innerhalb der EU.

Cesta komandanta Staneta 4A 1215 Medvode, Slowenien	Auslieferung der Inhalte des Dienstes (Hosting und Content Delivery). In Kundenunterlagen auch bezeichnet als „unser Hosting-Partner in Europa“.	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.
Cloudflare, Inc. 101 Townsend Street San Francisco, CA 94107, USA	Verwaltung der Domain und Namensauflösung (DNS). Cloudflare erhält dabei keinen Zugriff auf Inhalts- oder Bestandsdaten; die Anwendung selbst wird nicht über Cloudflare ausgeliefert.	Drittlandbezug USA. Zertifiziert unter dem EU-U.S. Data Privacy Framework; ergänzend Standardvertragsklauseln der EU-Kommission.

Hinweis: Die Namensauflösung ist eine der Hauptleistung dienende technische Nebenleistung. Sie wird hier aus Gründen der Transparenz namentlich ausgewiesen, obwohl dabei keine Inhaltsdaten des Auftraggebers verarbeitet werden.

Anlage 3: Ansprechpartner und Meldewege

Zur Erteilung von Weisungen befugt (Auftraggeber)

- [Name, Funktion, E-Mail-Adresse, Telefonnummer]

Zur Entgegennahme von Weisungen befugt (Auftragnehmer)

- [Name, Funktion, E-Mail-Adresse, Telefonnummer]

Ansprechpartner für den Datenschutz beim Auftragnehmer

- [Name, E-Mail-Adresse]

Adresse des Auftraggebers zur Meldung von Datenschutzverletzungen

- [E-Mail-Adresse, gegebenenfalls Telefonnummer]