

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO
Stand: Juli 2026 | Tinybooking

Parteien Auftraggeber (Organizer): Die natürliche oder juristische Person, welche sich als Unternehmer auf der Plattform Tinybooking registriert und die Plattform für die Verwaltung eigener Buchungen nutzt. Auftragnehmer (Tinybooking): Tinybooking, vertreten durch Timmy Wagner, Meesmannstr. 27, 58456 Witten · E-Mail: info@tinybooking.de

Präambel

Die vorliegende Anlage (nachfolgend als „AVV“ bezeichnet) dient der Präzisierung der datenschutzrechtlichen Pflichten, welche aus dem zwischen Auftraggeber und Auftragnehmer geschlossenen Nutzungsvertrag (im Folgenden „Hauptvertrag“) resultieren. Dieser AVV erstreckt sich auf sämtliche Verarbeitungstätigkeiten von personenbezogenen Daten (nachfolgend „Daten“), die der Auftragnehmer oder von ihm autorisierte Subunternehmer im Rahmen der Erfüllung des Hauptvertrages durchführen.

Hiermit wird den Anforderungen des Art. 28 Abs. 3 der Datenschutz-Grundverordnung (DSGVO) entsprochen. Diese Norm verpflichtet Verantwortliche, die Datenverarbeitung durch Dritte vertraglich oder durch ein anderes Rechtsinstrument abzusichern. Dementsprechend werden im Folgenden die Zuständigkeiten beider Parteien, Dauer, Gegenstand, Art und Zweck der Datenverarbeitung sowie die Kategorien der verarbeiteten Daten und die beiderseitigen Rechte und Pflichten rechtsverbindlich festgelegt.

Sofern in diesem Dokument Schriftform verlangt wird, genügt zur Wahrung dieser Anforderung die Textform gemäß § 126b BGB (z. B. E-Mail).

Dieser Auftragsverarbeitungsvertrag entfaltet seine rechtliche Wirkung ausschließlich in Kombination mit einem gültigen, aktiven Nutzungsvertrag mit Tinybooking zur Bereitstellung der Tinybooking-Software.

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragnehmer ist Entwickler und Betreiber der SaaS-Lösung Tinybooking.

Diese Vereinbarung regelt die beiderseitigen Rechte und Pflichten von Auftragnehmer und Auftraggeber (Kunde) im Zuge der im Hauptvertrag vereinbarten Leistungen, insofern dabei eine Verarbeitung personenbezogener Daten im Sinne von Art. 28 DSGVO durch den Auftragnehmer stattfindet. Eingeschlossen sind sämtliche Aktivitäten, die der Auftragnehmer bei dieser Verarbeitung übernimmt. Diese Regelung behält ihre Gültigkeit auch dann, wenn im Hauptvertrag nicht explizit auf diesen AVV verwiesen wird.

Die zeitliche Dauer der Datenverarbeitung ist strikt an die Laufzeit des zugrundeliegenden Hauptvertrages gekoppelt.

§ 2 Art und Zweck der Verarbeitung

Kategorie	Beschreibung
Art der Daten	Vorname, Nachname, E-Mail-Adresse, Telefonnummer (optional), Buchungsdaten (Datum, Uhrzeit, gewählte Dienstleistung), Statusdaten (z.B. PayPal-Transaktions-ID), Einwilligungsdaten (Legal Consent Logs), IP-Adressen (Logfiles).
Betroffene Personen	Gäste und Endkunden der vom Auftraggeber angebotenen Veranstaltungen und Termine.

Zweck der Verarbeitung	Bereitstellung einer Online-Buchungsseite, Verwaltung von Terminen im Dashboard, Versand von systemseitigen Bestätigungs-E-Mails an Gäste, Dokumentation von rechtlichen Einwilligungen.
Ort der Verarbeitung	Deutschland / Europäische Union (Server beim Hoster des Auftragnehmers)

§ 3 Weisungsrecht und Verantwortung des Auftraggebers

Der Auftraggeber trägt im Rahmen dieses Vertrages die alleinige Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften, insbesondere für die Zulässigkeit der Datenverarbeitung sowie die Wahrung der Betroffenenrechte (Verantwortlicher gem. Art. 4 Nr. 7 DSGVO).

Der vertraglich vereinbarte Leistungsumfang bildet die anfängliche, dokumentierte Weisung. Darüber hinausgehende Weisungen, etwa zur Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten, bedürfen stets der Textform (z. B. E-Mail). In dringenden Ausnahmefällen ist eine mündliche Weisung zulässig, sofern diese vom Auftraggeber unverzüglich in Textform nachgereicht und bestätigt wird.

Der Auftraggeber ist berechtigt, explizit weisungsbefugte Personen zu benennen. Auf Seiten des Auftragnehmers nehmen die Support-Mitarbeiter Weisungen entgegen. Bei einem längerfristigen Ausfall oder Wechsel der primären Ansprechpartner ist die jeweils andere Partei unverzüglich in Textform über entsprechende Nachfolger oder Vertreter zu informieren.

Sofern der Auftragnehmer der Auffassung ist, dass eine erteilte Weisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. Der Auftragnehmer ist in einem solchen Fall berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis der Auftraggeber diese anpasst oder deren rechtliche Zulässigkeit hinreichend belegt. Offensichtlich rechtswidrige Weisungen wird der Auftragnehmer konsequent ablehnen.

Der Auftraggeber verpflichtet sich zudem, alle ihm im Rahmen dieses Vertrages bekannt werdenden Geschäftsgeheimnisse und Details zu den Datensicherheitsmaßnahmen des Auftragnehmers streng vertraulich zu behandeln. Diese Verschwiegenheitspflicht gilt über das Ende des Hauptvertrages hinaus.

§ 4 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, insbesondere:

- Verschlüsselte Übertragung aller Daten via TLS/HTTPS
- Verschlüsselung sensibler Datenbankfelder auf Applikationsebene (AES-256-CBC)
- Passwort-Hashing (bcrypt) für alle Nutzerkonten
- Zentrales Audit-Logging von Einwilligungen (Consent Logs)
- Zugriffsbeschränkung auf Daten nach dem Prinzip der geringsten Rechte
- CSRF-Schutz für alle Formulare
- Regelmäßige Datenbank-Backups
- Session-Sicherheit (HttpOnly, Secure, SameSite)

Die vollständigen und rechtlich bindenden Maßnahmen sind in Anlage 1 (Technisch-organisatorische Maßnahmen - TOM) festgelegt, welche untrennbarer Bestandteil dieses Vertrages ist.

§ 5 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, personenbezogene Daten ausschließlich im vertraglich vereinbarten Umfang oder auf ausdrückliche Weisung des Auftraggebers zu verarbeiten, es sei denn, zwingende gesetzliche Vorgaben erfordern eine abweichende Verarbeitung. In einem solchen Fall informiert der Auftragnehmer den Auftraggeber vorab, sofern dem keine gesetzlichen Verbote entgegenstehen. Eine Nutzung der überlassenen Daten für eigene Zwecke des Auftragnehmers ist strikt ausgeschlossen.

Der Auftragnehmer gewährleistet, dass sämtliche Personen, die Zugriff auf die im Auftrag verarbeiteten Daten haben, schriftlich zur strengen Vertraulichkeit verpflichtet wurden, sofern sie nicht bereits einer gesetzlichen Geheimhaltungspflicht unterliegen. Zudem stellt der Auftragnehmer sicher, dass diese Personen regelmäßig im Umgang mit datenschutzrechtlichen Vorgaben geschult, sensibilisiert und bei der Einhaltung dieser Anforderungen kontinuierlich überwacht werden.

Die Datenverarbeitung findet ausnahmslos auf Servern innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) statt. Eine Verlagerung in Drittstaaten bedarf der vorherigen, ausdrücklichen Zustimmung des Auftraggebers und darf nur unter strikter Einhaltung der Vorgaben aus Kapitel V der DSGVO erfolgen.

Der Auftragnehmer leistet dem Auftraggeber im zumutbaren Umfang Unterstützung bei der Erfüllung der gesetzlichen Pflichten gemäß Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung), insbesondere bei behördlichen Kontrollen oder der Bearbeitung von Betroffenenanfragen.

Gemäß Art. 33 Abs. 2 DSGVO ist der Auftragnehmer verpflichtet, dem Auftraggeber jedwede festgestellte Verletzung des Schutzes personenbezogener Daten, die unter diesen Vertrag fallen, unverzüglich zu melden. Sollte der Auftraggeber von einer betroffenen Person auf Schadensersatz nach Art. 82 DSGVO in Anspruch genommen werden, wird der Auftragnehmer nach besten Kräften bei der Abwehr dieser Ansprüche unterstützen.

§ 6 Einsatz von Unterauftragnehmern

Ein Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer Dritte (verbundene oder externe Unternehmen) mit Dienstleistungen betraut, die unmittelbar der Erbringung der Hauptleistung dienen.

Der Auftraggeber stimmt dem grundsätzlichen Einsatz solcher Subunternehmer durch den Auftragnehmer zu. Eine aktuelle Übersicht der eingesetzten Unterauftragnehmer (inklusive deren Sitz und Leistung) ist den Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers zu entnehmen. Diese Liste wird bei Änderungen entsprechend aktualisiert.

Der Auftragnehmer wird den Auftraggeber spätestens 14 Tage vor der geplanten Hinzuziehung oder dem Austausch eines Subunternehmers in Textform informieren. Der Auftraggeber ist berechtigt, aus einem wichtigen datenschutzrechtlichen Grund innerhalb dieser Frist zu widersprechen. Macht der Auftraggeber von diesem Widerspruchsrecht Gebrauch, steht dem Auftragnehmer das Recht zu, diesen AVV sowie den zugrundeliegenden Hauptvertrag fristlos zu kündigen.

Beauftragt der Auftragnehmer Subunternehmer, ist er verpflichtet, diesen dieselben datenschutzrechtlichen Pflichten vertraglich aufzuerlegen, die in diesem AVV festgelegt sind (gemäß Art. 28 Abs. 2 bis 4 DSGVO). Der Auftragnehmer trägt gegenüber dem Auftraggeber die volle Verantwortung für die Einhaltung des Datenschutzes durch die von ihm eingesetzten Unterauftragnehmer.

§ 7 Betroffenenrechte

Sollte sich eine betroffene Person mit Begehren auf Auskunft, Löschung oder Berichtigung unmittelbar an den Auftragnehmer wenden, leitet dieser die betroffene Person an den Auftraggeber weiter, sofern eine eindeutige Zuordnung der Person zum jeweiligen Auftraggeber rechtlich und faktisch machbar ist.

Der Auftragnehmer leistet dem Auftraggeber im Rahmen seiner technischen und organisatorischen Möglichkeiten Beistand bei der Wahrung der Betroffenenrechte gemäß Kapitel 3 der DSGVO (darunter Rechte auf Auskunft, Berichtigung, Löschung, Widerspruch und Datenübertragbarkeit).

Die Verantwortung für die fristgerechte, inhaltlich korrekte und vollständige Beantwortung derartiger Anfragen liegt jedoch ausschließlich beim Auftraggeber. Eine Haftung des Auftragnehmers für Fristversäumnisse oder unzureichende Auskünfte im Rahmen dieser Betroffenenanfragen wird ausdrücklich ausgeschlossen.

§ 8 Löschung und Rückgabe von Daten

Mit Beendigung des Auftragsverhältnisses – oder jederzeit auf explizite Anforderung des Auftraggebers – verpflichtet sich der Auftragnehmer, sämtliche im Rahmen dieses Vertrages verarbeiteten Daten nach Wahl des Auftraggebers entweder datenschutzkonform zu vernichten oder vollständig an diesen zurückzugeben.

Eine Löschung umfasst ausnahmslos auch alle angefertigten Kopien und Backups und muss so ausgeführt werden, dass eine Wiederherstellung der Informationen nach dem aktuellen Stand der Technik faktisch ausgeschlossen ist. Der Auftragnehmer trägt zudem die Sorge dafür, dass diese Lösch- oder Rückgabepflichten ebenso konsequent bei allen eingebundenen Unterauftragnehmern vollzogen werden.

Hiervon unberührt bleiben Dokumentationen und Protokolle, die dem Nachweis einer ordnungsgemäßen und rechtskonformen Datenverarbeitung dienen; diese werden vom Auftragnehmer entsprechend der gesetzlichen Aufbewahrungsfristen auch über das Vertragsende hinaus gesichert.

§ 9 Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Vorgaben sowie der vertraglichen Abmachungen durch den Auftragnehmer in angemessenem Rahmen zu überprüfen – entweder eigenständig oder durch einen beauftragten Dritten. Dies umfasst insbesondere das Recht auf Auskunftseinholung sowie die Vor-Ort-Einsichtnahme in die Datenverarbeitungsprozesse.

Der Auftragnehmer gewährt den Kontrollierenden den hierfür erforderlichen Zutritt und Einblick, erteilt notwendige Auskünfte und demonstriert relevante Abläufe. Solche Inspektionen sind dem Auftragnehmer mit einer angemessenen Vorlaufzeit anzukündigen, dürfen den regulären Geschäftsbetrieb nicht unverhältnismäßig stören und finden zu den üblichen Geschäftszeiten statt. Vorab ist eine entsprechende Verschwiegenheitsvereinbarung zu unterzeichnen.

Vor-Ort-Kontrollen sind grundsätzlich auf maximal einmal pro Kalenderjahr (alle 12 Monate) beschränkt. Legt der Auftragnehmer aussagekräftige Nachweise über die korrekte Umsetzung der Datenschutzmaßnahmen vor, sollte sich eine Prüfung primär auf Stichproben beschränken. Der Auftragnehmer behält sich vor, für den personellen und zeitlichen Aufwand, der bei der Unterstützung einer Inspektion entsteht, eine angemessene Vergütung in Rechnung zu stellen.

§ 10 Außerordentliche Kündigung

Sollte der Auftragnehmer nachweislich und gravierend gegen geltende Datenschutzgesetze oder die in dieser Vereinbarung festgelegten Pflichten verstoßen, steht dem Auftraggeber das Recht zu, den zugrundeliegenden Hauptvertrag in Textform fristlos außerordentlich zu kündigen.

§ 11 Haftung und Schadensersatz

Hinsichtlich möglicher Schadensersatzansprüche betroffener Personen richtet sich die Haftung von Auftraggeber und Auftragnehmer vollumfänglich nach den gesetzlichen Bestimmungen des Art. 82 DSGVO.

§ 12 Schlussbestimmungen

Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragnehmers (Witten). Änderungen dieses Vertrages bedürfen der Textform.