

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO Anlage 2 zu den Allgemeinen Geschäftsbedingungen für die Nutzung der Software „teamora“

Stand: 23.08.2026 · Version 1.0

Zwischen

dem Nutzer der Software „teamora“, identifiziert durch die im Nutzerkonto hinterlegten Angaben — nachfolgend **„Verantwortlicher“** —

und

Ronny Mühlbach

Am Heim 8

09116 Chemnitz, Deutschland — nachfolgend „Auftragsverarbeiter“ —

— gemeinsam die **„Parteien“** —

Inhaltsübersicht

§ 1	Gegenstand, Dauer und Rollenverteilung
§ 2	Art, Zweck und Umfang der Verarbeitung
§ 3	Weisungsrecht des Verantwortlichen
§ 4	Pflichten des Auftragsverarbeiters
§ 5	Pflichten des Verantwortlichen
§ 6	Betroffenenrechte
§ 7	Unterauftragsverarbeiter
§ 8	Übermittlung in Drittländer
§ 9	Verletzung des Schutzes personenbezogener Daten
§ 10	Löschung und Rückgabe nach Vertragsende
§ 11	Nachweise und Kontrollen
§ 12	Haftung
§ 13	Schlussbestimmungen
Anlage 1	— Technische und organisatorische Maßnahmen
Anlage 2	— Unterauftragsverarbeiter

Präambel

Der Auftragsverarbeiter stellt dem Verantwortlichen die Software „teamora“ zur Nutzung bereit. Der Verantwortliche verarbeitet mit dieser Software personenbezogene Daten Dritter, insbesondere seiner geschäftlichen Kontakte und Interessenten.

Der Verantwortliche bestimmt allein über Zwecke und Mittel dieser Verarbeitung. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich in seinem Auftrag und nach seinen Weisungen.

Dieser Vertrag konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO. Er kommt mit der Zustimmung des Verantwortlichen im Rahmen der Registrierung zustande und gilt für die Dauer des Hauptvertrages.

§ 1 Gegenstand, Dauer und Rollenverteilung

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs der Software „teamora“ gemäß dem Hauptvertrag.

(2) Die Dauer dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Er endet automatisch mit dessen Beendigung, mit Ausnahme der Regelungen des § 10, die fortgelten.

(3) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung allein verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage nach Art. 6 DSGVO, für die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO gegenüber den betroffenen Personen und für die Wahrung von Betroffenenrechten.

(4) Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen selbst — insbesondere dessen Stammdaten, Zahlungs- und Nutzungsdaten — als eigener Verantwortlicher. Diese Verarbeitung ist nicht Gegenstand dieses Vertrages; sie richtet sich nach der Datenschutzerklärung des Auftragsverarbeiters.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art der Verarbeitung: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Verknüpfen, Einschränken, Löschen und Vernichten.

(2) Zweck der Verarbeitung: Bereitstellung der Softwarefunktionen zur Organisation der Vertriebstätigkeit des Verantwortlichen, insbesondere Kontaktverwaltung, Nachverfolgung von Vertriebsvorgängen, Darstellung von Vertriebsstrukturen, KI-gestützte Unterstützung sowie der Versand von Nachrichten im Auftrag des Verantwortlichen.

(3) Kategorien betroffener Personen:

- Geschäftliche Kontakte und Interessenten des Verantwortlichen
- Mitglieder der Vertriebsstruktur des Verantwortlichen
- Empfänger von Nachrichten, die der Verantwortliche über die Software versendet
- Sonstige natürliche Personen, deren Daten der Verantwortliche eigenverantwortlich in die Software eingibt

(4) Kategorien personenbezogener Daten:

- Stammdaten: Name, Anrede, Geburtsdatum
- Kontaktdaten: E-Mail-Adresse, Telefonnummer, Anschrift, Profile in sozialen Netzwerken
- Vertriebsbezogene Daten: Status im Vertriebsprozess, Zuordnung zu Vertriebsstrukturen, Rangbezeichnungen, Zugehörigkeit zu Vertriebsunternehmen
- Kommunikationsdaten: Gesprächsnotizen, Verlauf von Kontaktaufnahmen, Inhalte versendeter Nachrichten
- Freitextangaben, deren Inhalt allein der Verantwortliche bestimmt
- Eingaben in die KI-Funktion, soweit der Verantwortliche dort personenbezogene Daten eingibt

(5) Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO sind nicht Gegenstand dieses Vertrages. Der Verantwortliche verpflichtet sich, solche Daten nicht in die Software einzugeben. Gibt er sie entgegen dieser Verpflichtung dennoch ein, geschieht dies auf sein alleiniges Risiko; der Auftragsverarbeiter trifft insoweit keine über diesen Vertrag hinausgehenden Schutzpflichten.

(6) Ort der Verarbeitung: Die Verarbeitung erfolgt in Rechenzentren innerhalb der Europäischen Union sowie, im Umfang der in Anlage 2 bezeichneten Unterauftragsverarbeiter, in Drittländern. Für Übermittlungen in Drittländer gilt § 8.

§ 3 Weisungsrecht des Verantwortlichen

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

(2) Die Nutzung der Softwarefunktionen durch den Verantwortlichen gilt als Weisung im Sinne des Absatzes 1. Der Hauptvertrag, diese Vereinbarung und die Leistungsbeschreibung stellen die initiale Weisung dar.

(3) Darüber hinausgehende Einzelweisungen erteilt der Verantwortliche in Textform an [support@myteamora.de]. Sie sind vom Auftragsverarbeiter zu dokumentieren.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

(5) Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen und beim Auftragsverarbeiter einen erheblichen Mehraufwand verursachen, kann dieser von einer gesonderten Vergütungsvereinbarung abhängig machen. Dies gilt nicht für Weisungen, die zur Erfüllung zwingender gesetzlicher Pflichten erforderlich sind.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Rahmen dieses Vertrages und der Weisungen des Verantwortlichen. Eine Nutzung für eigene Zwecke findet nicht statt. Eine Auswertung anonymisierter und aggregierter Daten, die keinen Rückschluss auf betroffene Personen zulässt, bleibt hiervon unberührt.

(2) Der Auftragsverarbeiter stellt sicher, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

(3) Der Auftragsverarbeiter ergreift die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in **Anlage 1** beschrieben. Der Auftragsverarbeiter ist berechtigt, die Maßnahmen anzupassen, sofern das Schutzniveau nicht unterschritten wird.

(4) Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten bestellt, da die Voraussetzungen des Art. 37 DSGVO in Verbindung mit § 38 BDSG derzeit nicht vorliegen. Ansprechpartner für Datenschutzfragen ist Ronny Mühlbach, support@myteamora.de. Der Auftragsverarbeiter informiert den Verantwortlichen, sobald eine Bestellpflicht eintritt.

Hinweis: Eine Bestellpflicht entsteht nach § 38 BDSG unter anderem, wenn in der Regel mindestens 20 Personen ständig mit automatisierter Verarbeitung beschäftigt sind, oder unabhängig davon nach Art. 37 Abs. 1 lit. b DSGVO bei umfangreicher regelmäßiger und systematischer Überwachung. Prüfe das mit steigender Nutzerzahl erneut.

(5) Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dieses dem Verantwortlichen auf Anfrage zur Verfügung.

(6) Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung der Daten nur auf Weisung des Verantwortlichen ein, soweit nicht eine gesetzliche Verpflichtung besteht.

(7) Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Anforderung bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und bei vorherigen Konsultationen nach Art. 36 DSGVO, soweit dies im Rahmen der ihm zur Verfügung stehenden Informationen möglich und zumutbar ist.

§ 5 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich.

(2) Der Verantwortliche stellt insbesondere sicher, dass

- a) für jede Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO besteht,
- b) betroffene Personen nach Art. 13 und 14 DSGVO informiert wurden,
- c) für den Versand von Nachrichten die erforderlichen Einwilligungen oder gesetzlichen Erlaubnistatbestände vorliegen, insbesondere nach § 7 UWG,
- d) keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO eingegeben werden,
- e) keine personenbezogenen Daten in die KI-Funktion eingegeben werden, soweit dies für den verfolgten Zweck nicht erforderlich ist.

(3) Der Verantwortliche führt ein eigenes Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO, soweit er hierzu verpflichtet ist.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(5) Der Verantwortliche benennt einen für Datenschutzfragen zuständigen Ansprechpartner. Fehlt eine gesonderte Benennung, gilt die im Nutzerkonto hinterlegte E-Mail-Adresse.

§ 5a Verknüpfte Drittdienste

(1) Die Software ermöglicht dem Verantwortlichen, eigene Konten bei Drittanbietern zu verknüpfen, insbesondere WhatsApp, Telegram, Instagram, Facebook, Microsoft Teams, Zoom und E-Mail-Dienste (nachfolgend „verknüpfte Drittdienste“). Der Verantwortliche unterhält diese Konten eigenständig und in eigener Verantwortung; sie sind nicht Gegenstand einer Beauftragung des Auftragsverarbeiters.

(2) Der Auftragsverarbeiter verarbeitet die über verknüpfte Drittdienste zugänglichen Daten ausschließlich auf Weisung und im Rahmen der vom Verantwortlichen veranlassten Nutzung der Software. Diese Verarbeitung ist von diesem Vertrag umfasst; eines gesonderten Vertrages zwischen dem Auftragsverarbeiter und dem jeweiligen Drittanbieter bedarf es hierfür nicht.

(3) Der Verantwortliche ist allein dafür verantwortlich, dass

- a) eine Rechtsgrundlage für die Nutzung des jeweiligen Drittdienstes und die dort erfolgende Verarbeitung personenbezogener Daten besteht,
- b) die Verknüpfung und ihre Nutzung mit den Nutzungsbedingungen des jeweiligen Drittanbieters vereinbar ist,
- c) etwaige eigene vertragliche oder datenschutzrechtliche Verpflichtungen gegenüber dem Drittanbieter erfüllt werden.

(4) Der Auftragsverarbeiter trifft keine Aussage über die datenschutzrechtliche Einordnung der Beziehung zwischen dem Verantwortlichen und dem jeweiligen Drittanbieter und übernimmt keine Gewähr für dessen Datenschutz-, Sicherheits- oder Verfügbarkeitspraxis. Beschränkungen, Sperrungen oder sonstige Maßnahmen, die ein Drittanbieter gegenüber dem Konto des Verantwortlichen ergreift, hat der Auftragsverarbeiter nicht zu vertreten.

§ 6 Betroffenenrechte

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Kapitel III der DSGVO, insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit.

(2) Der Auftragsverarbeiter stellt hierfür Funktionen innerhalb der Software bereit, insbesondere zur Suche, Berichtigung, Löschung und zum Export von Datensätzen. Der Verantwortliche nutzt vorrangig diese Funktionen.

(3) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst. Er weist die betroffene Person darauf hin, dass der Verantwortliche zuständig ist.

(4) Für eine über Absatz 2 hinausgehende Unterstützung kann der Auftragsverarbeiter eine angemessene Vergütung verlangen, soweit der Aufwand nicht auf einem von ihm zu vertretender Umstand beruht.

§ 7 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung nach Art. 28 Abs. 2 Satz 1 DSGVO zur Hinzuziehung von Unterauftragsverarbeitern.

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier (4) Wochen vor der beabsichtigten Hinzuziehung eines neuen oder dem Wechsel eines bestehenden Unterauftragsverarbeiters in Textform.

(4) Der Verantwortliche kann einer beabsichtigten Änderung innerhalb der Frist nach Absatz 3 aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen. Im Fall eines Widerspruchs suchen die Parteien eine einvernehmliche Lösung. Kommt eine solche nicht zustande und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht in zumutbarer Weise erbringen, ist jede Partei berechtigt, den Hauptvertrag zum Zeitpunkt der Umstellung außerordentlich zu kündigen. Im Voraus gezahlte Entgelte werden anteilig erstattet.

(5) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten aus diesem Vertrag im Wesentlichen entsprechen. Er wählt Unterauftragsverarbeiter sorgfältig aus und prüft vor Beauftragung, ob diese hinreichende Garantien nach Art. 28 Abs. 1 DSGVO bieten.

(6) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Datenschutzpflichten durch seine Unterauftragsverarbeiter wie für eigenes Handeln.

(7) Nicht als Unterauftragsverarbeitung im Sinne dieser Vorschrift gelten Nebenleistungen Dritter, die der Auftragsverarbeiter zur Unterstützung seiner Geschäftstätigkeit in Anspruch nimmt und bei denen ein Zugriff auf personenbezogene Daten des Verantwortlichen nicht bestimmungsgemäß erfolgt, etwa Telekommunikations- oder Postdienstleistungen.

(8) Nicht als Unterauftragsverarbeiter im Sinne dieses Paragraphen gelten Drittanbieter, deren Dienste der Verantwortliche als verknüpfte Drittdienste nach § 5a mit der Software verbindet, insbesondere WhatsApp, Telegram, Instagram, Facebook, Microsoft Teams, Zoom und der vom Verantwortlichen gewählte E-Mail-Anbieter. Der Verantwortliche wählt diese Anbieter eigenständig aus und unterhält mit ihnen ein eigenes Vertragsverhältnis; der Auftragsverarbeiter beauftragt sie nicht und hat auf ihre Auswahl keinen Einfluss. Absatz 1 bis 6 finden auf diese Anbieter keine Anwendung. § 5a Abs. 4 bleibt unberührt.

§ 8 Übermittlung in Drittländer

(1) Eine Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, soweit die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

(2) Der Auftragsverarbeiter setzt zur Erbringung der KI-gestützten Funktionen einen Dienstleister mit Sitz in den Vereinigten Staaten von Amerika ein. Die Verarbeitung kann außerhalb der Europäischen Union erfolgen. Grundlage der Übermittlung sind die

Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914, Modul 3: Auftragsverarbeiter an Unterauftragsverarbeiter) in Verbindung mit ergänzenden Maßnahmen.

(3) Der Auftragsverarbeiter hat für die betreffenden Übermittlungen eine Abwägung der Rechtslage im Empfängerland vorgenommen und ergänzende Maßnahmen umgesetzt, insbesondere Transportverschlüsselung, Datenminimierung sowie vertragliche Zusicherungen zur Behandlung behördlicher Zugriffersuchen.

(4) Der Verantwortliche wird ausdrücklich darauf hingewiesen, dass er die KI-Funktionen ohne Eingabe personenbezogener Daten Dritter nutzen kann und soll. Gibt er solche Daten dennoch ein, erfolgt die damit verbundene Drittlandübermittlung auf seine Weisung im Sinne des § 3 Abs. 2.

(5) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn die Grundlage einer Drittlandübermittlung entfällt oder eine zuständige Behörde oder ein Gericht deren Unzulässigkeit feststellt.

§ 9 Verletzung des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von vierundzwanzig (24) Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten, die den Verantwortlichen betrifft.

(2) Die Mitteilung enthält, soweit bekannt:

- a) eine Beschreibung der Art der Verletzung einschließlich der Kategorien und der ungefähren Zahl betroffener Personen und Datensätze,
- b) den Namen und die Kontaktdaten des Ansprechpartners,
- c) eine Beschreibung der wahrscheinlichen Folgen,
- d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Schadensminderung.

Sind nicht alle Angaben zeitgleich verfügbar, erfolgt eine unverzügliche Nachmeldung.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Meldepflichten nach Art. 33 DSGVO gegenüber der Aufsichtsbehörde und bei der Benachrichtigung betroffener Personen nach Art. 34 DSGVO.

(4) Meldungen an Aufsichtsbehörden oder Benachrichtigungen betroffener Personen im Namen des Verantwortlichen nimmt der Auftragsverarbeiter nur auf ausdrückliche Weisung vor.

(5) Der Auftragsverarbeiter dokumentiert jede Verletzung einschließlich der ergriffenen Maßnahmen.

§ 10 Löschung und Rückgabe nach Vertragsende

- (1)** Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht.
- (2)** Der Verantwortliche kann seine Daten über die Exportfunktion der Software eigenständig sichern. Diese Funktion bleibt für dreißig (30) Tage nach Beendigung des Hauptvertrages verfügbar. Nach Ablauf dieser Frist erfolgt die Löschung aus den produktiven Systemen.
- (3)** In Datensicherungen können die Daten für weitere 90 Tage enthalten sein. Sie werden mit dem Auslaufen der jeweiligen Sicherung automatisch und ohne gesonderte Anforderung gelöscht. Ein Zugriff auf diese Sicherungen erfolgt ausschließlich zum Zweck der Wiederherstellung im Störfall.
- (4)** Der Auftragsverarbeiter weist die Löschung auf Anforderung des Verantwortlichen in Textform nach.
- (5)** Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, darf der Auftragsverarbeiter über das Vertragsende hinaus für die Dauer der jeweiligen gesetzlichen Aufbewahrungsfrist aufbewahren. Die Verarbeitung ist insoweit auf den Nachweiszweck beschränkt.

§ 11 Nachweise und Kontrollen

- (1)** Der Auftragsverarbeiter weist dem Verantwortlichen die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage nach.
- (2)** Der Nachweis erfolgt vorrangig durch geeignete Unterlagen, insbesondere durch die Dokumentation der technischen und organisatorischen Maßnahmen nach Anlage 1, durch Zertifikate anerkannter Stellen oder durch Prüfberichte unabhängiger Dritter, soweit vorhanden.
- (3)** Genügen diese Nachweise im Einzelfall nicht, ist der Verantwortliche berechtigt, nach vorheriger Anmeldung mit einer angemessenen Frist von mindestens vier (4) Wochen während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs eine Überprüfung durchzuführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen zu lassen. Der Prüfer darf kein Wettbewerber des Auftragsverarbeiters sein.
- (4)** Überprüfungen erfolgen in der Regel höchstens einmal jährlich. Bei konkreten Anhaltspunkten für einen Verstoß oder nach einer Verletzung des Schutzes

personenbezogener Daten ist eine anlassbezogene Prüfung auch außerhalb dieses Rhythmus zulässig.

(5) Für den Aufwand einer Vor-Ort-Prüfung nach Absatz 3 kann der Auftragsverarbeiter eine angemessene Vergütung verlangen, es sei denn, die Prüfung ist durch einen von ihm zu vertretender Verstoß veranlasst.

(6) Der Auftragsverarbeiter ist verpflichtet, bei Kontrollen einer Aufsichtsbehörde mitzuwirken, soweit diese die Verarbeitung im Auftrag des Verantwortlichen betreffen, und den Verantwortlichen hierüber unverzüglich zu informieren.

§ 12 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Hauptvertrages, soweit nachfolgend nichts Abweichendes bestimmt ist.

(2) Im Außenverhältnis gegenüber betroffenen Personen und Aufsichtsbehörden gelten die Art. 82 und 83 DSGVO. Diese Vorschriften sind nicht abdingbar und werden durch diesen Vertrag nicht eingeschränkt.

(3) Im Innenverhältnis tragen die Parteien Schadensersatz und Bußgelder in dem Verhältnis, in dem sie zur Entstehung des Schadens beigetragen haben. Hat eine Partei den vollen Betrag geleistet, kann sie von der anderen Partei den auf deren Verantwortungsanteil entfallenden Teil ersetzt verlangen (Art. 82 Abs. 5 DSGVO).

(4) Der Verantwortliche stellt den Auftragsverarbeiter von Ansprüchen Dritter frei, die darauf beruhen, dass der Verantwortliche gegen seine Pflichten aus § 5 verstoßen hat, insbesondere bei fehlender Rechtsgrundlage für die Verarbeitung oder bei unzulässigem Nachrichtenversand.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Der Auftragsverarbeiter kann diesen Vertrag anpassen, soweit dies aufgrund einer Änderung der Rechtslage, aufgrund von Vorgaben oder Entscheidungen von Aufsichtsbehörden oder Gerichten oder aufgrund technischer Entwicklungen erforderlich wird. Die Anpassung wird dem Verantwortlichen mindestens vier (4) Wochen vor Inkrafttreten in Textform mitgeteilt. Widerspricht der Verantwortliche, gilt § 7 Abs. 4 Satz 3 entsprechend.

(3) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieses Vertrages vor.

(4) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) Es gilt das Recht der Bundesrepublik Deutschland. Für Verantwortliche mit Sitz in Österreich oder der Schweiz gilt § 27 der AGB entsprechend.

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

1. Vertraulichkeit

1.1 Zutrittskontrolle (physischer Zugang)

Die Verarbeitung erfolgt in Rechenzentren der eingesetzten Hosting-Dienstleister. Diese verfügen über eigene Zutrittskontrollsysteme, in der Regel einschließlich Vereinzelungsanlagen, Videoüberwachung, Alarmanlagen und protokollierter Besucherverwaltung. Der Auftragsverarbeiter selbst unterhält keine eigenen Serverräume.

1.2 Zugangskontrolle (Systemzugang)

- Zugang zur Software ausschließlich über persönliche Zugangsdaten
- Speicherung von Passwörtern ausschließlich als kryptografischer Hash mit Salt - Verfahren: bcrypt
- Zwei-Faktor-Authentifizierung für administrative Zugänge [umgesetzt]
- Zwei-Faktor-Authentifizierung für Nutzerkonten [verfügbar]
- Automatische Sperrung nach mehrfacher Fehleingabe
- Automatische Beendigung inaktiver Sitzungen
- Verschlüsselte Übertragung aller Daten über TLS

1.3 Zugriffskontrolle (Berechtigungen)

- Strikte Mandantentrennung: Nutzer haben ausschließlich Zugriff auf die eigenen Daten
- Administrativer Zugriff auf Produktivdaten beschränkt auf [Anzahl] Person(en); Zugriff nur zur Störungsbehebung und zur Erfüllung von Support-Anfragen
- Verschlüsselung der Datenbank im Ruhezustand
- Kontrollierte Löschung von Datenträgern und Löschung nach Vertragsende gemäß § 10

1.4 Trennungskontrolle

- Logische Mandantentrennung auf Datenbankebene
- Getrennte Umgebungen für Entwicklung, Test und Produktion
- Keine Verwendung von Produktivdaten in Entwicklungs- und Testumgebungen

1.5 Pseudonymisierung

- Eine Pseudonymisierung erfolgt derzeit nicht, da die Daten zur Erfüllung des Vertragszwecks im Klartext benötigt werden.“ — das ist eine zulässige Angabe.

2. Integrität

2.1 Weitergabekontrolle

- Übertragung ausschließlich über verschlüsselte Verbindungen (TLS 1.2 oder höher)
- Keine Übermittlung an Dritte außerhalb der in Anlage 2 genannten Unterauftragsverarbeiter
- Datenexport für den Verantwortlichen ausschließlich über authentifizierten Zugang

2.2 Eingabekontrolle

- Protokollierung sicherheitsrelevanter Ereignisse, insbesondere Anmeldungen und Änderungen an Zugangsdaten

3. Verfügbarkeit und Belastbarkeit

- Regelmäßige automatisierte Datensicherung im Abstand von 24 Stunden.
- Aufbewahrung der Sicherungen für 90 Tage (gelöschte Daten ausgenommen)
- Verschlüsselte Speicherung der Sicherungen
- Regelmäßige Prüfung der Wiederherstellbarkeit [halbjährlich]
- Redundante Infrastruktur beim Hosting-Dienstleister
- Schutz vor Schadsoftware und unbefugten Zugriffen auf Systemebene
- Zeitnahe Einspielung sicherheitsrelevanter Aktualisierungen

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung und Aktualisierung dieser Maßnahmen [mindestens einmal jährlich]
- Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO
- Prozess zur Behandlung von Verletzungen des Schutzes personenbezogener Daten gemäß § 9
- Sorgfältige Auswahl und Prüfung von Unterauftragsverarbeitern
- Auftragskontrolle durch vertragliche Bindung aller Unterauftragsverarbeiter

5. Datenschutz durch Technikgestaltung und Voreinstellungen

- Datenminimierung: Erhebung nur der für den Vertragszweck erforderlichen Daten
- Datenschutzfreundliche Voreinstellungen bei neuen Funktionen
- Hinweis innerhalb der KI-Funktion, keine personenbezogenen Daten Dritter einzugeben [geplant zum: 01.09.2026]

Anlage 2 — Unterauftragsverarbeiter

Unternehm en	Sitz	Leistung	Verarbeitungso rt	Grundlage bei Drittland
Hostinger	Zyper n	Bereitstellung der Server- und Datenbankinfrastrukt ur	EU/Deutschlan d	—
Stripe Payments Europe, Ltd.	Irland	Zahlungsabwicklung, Abonnementverwaltu ng	EU / USA	Standardvertragsklaus eln
Anthropic PBC	USA	KI-gestützte Funktionen („Mora“)	USA	Standardvertragsklaus eln, Modul 3

Schlussbemerkung

Dieser Entwurf wurde nach bestem Wissen und unter Berücksichtigung der zum Erstellungszeitpunkt geltenden Rechtslage erstellt. Er ersetzt keine anwaltliche Beratung im Einzelfall.

Die inhaltliche Richtigkeit der Anlage 1 (technische und organisatorische Maßnahmen) und der Anlage 2 (Unterauftragsverarbeiter) kann nur der Auftragsverarbeiter selbst verantworten. Beide Anlagen sind vor Veröffentlichung vollständig gegen die tatsächliche technische Umsetzung abzugleichen und danach mindestens jährlich zu überprüfen.