Vereinbarung über die Verarbeitung personenbezogener Daten (Auftragsverarbeitung)

Fassung 4.0 vom 09.11.2026
zwischen
Name:
Straße:
Ort:
– nachstehend Auftraggeber genannt –
und
maniac developer GmbH, Kolpingstraße 20, 77855 Achern
– nachstehend Auftragnehmer genannt –
– nachstehend einzeln oder gemeinsam auch Parteien genannt –

Präambel

Diese Vereinbarung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht, insbesondere der Datenschutz-Grundverordnung (VO (EU) 2016/679, nachfolgend „DS-GVO“) sowie dem Bundesdatenschutzgesetz („BDSG“) in ihrer jeweils gültigen Fassung ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet. Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Dazu gehören insbesondere:

- Fernwartung, Diagnose, Support, Installation von Software und Upgrades, einschließlich eines Remotezugriffs auf das IT-System des Auftraggebers und des Umgangs mit einer Echtdaten enthaltenden Dump- oder Backup-Datei,
- der Betrieb der maniac-Zentrale für die beim Auftraggeber installierte Software (Lizenzprüfung, Betriebsdaten, Fehlerberichte, lesender Supportzugriff),
- die Weiterleitung von Anfragen der KI-gestützten Funktionen (KI-Assistentin Mina und virtuelle Mitarbeiter) an KI-Modelle und die Rückgabe der Ergebnisse an die Software des Auftraggebers,
- die optionale Bereitstellung des Zugriffs von außen auf die Weboberfläche der Software,
- Hosting von Software, ASP, SaaS oder cloudbasierte Angebote der Softwareüberlassung.

Die Software läuft auf dem IT-System des Auftraggebers. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf, mit dem Laufzeitende des letzten verbleibenden Hauptvertrages.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
(2) Verarbeitung: Verarbeitung umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten Format zu bestätigen.
Als dokumentierte Weisung gelten auch die Einstellungen des Auftraggebers in der Software, insbesondere „Mina nutzen“, „Supportzugriff erlauben“, „Betriebsdaten an maniac melden“ und „Fehler automatisch an maniac melden“. Änderungen dieser Einstellungen werden mit Benutzer und Zeitpunkt protokolliert.

§ 2 Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware, und bietet im Rahmen seiner Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Er betreibt die maniac-Zentrale, mit der sich die Software für Lizenz, Support und KI-gestützte Funktionen verbindet. Ferner bietet er Softwarelösungen auch im Rahmen von Hosting, ASP, SaaS oder cloudbasierten Angeboten an. Im Rahmen dieser Tätigkeiten kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des Hauptvertrages konkretisiert.
(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten, bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortliche Stelle ist, gegeben ist.

§ 2a Gegenstand, Art und Zweck der Verarbeitung

(1) Zweck der Verarbeitung
Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers zu folgenden Zwecken:

- Technische Unterstützung, Support und Fehlerdiagnose, einschließlich des Umgangs mit Echtdaten enthaltenden Dump- und Backup-Dateien und der Bearbeitung von Supportanfragen.
- Durchführung von Fernwartungen und Remotezugriffen auf das IT-System des Auftraggebers.
- Installation von Software und Upgrades.
- Betrieb der maniac-Zentrale: Lizenzprüfung, Empfang von Betriebsdaten und Fehlerberichten, lesender Supportzugriff.
- Weiterleitung von Anfragen der KI-gestützten Funktionen (KI-Assistentin Mina und virtuelle Mitarbeiter) an KI-Modelle und Rückgabe der Ergebnisse an die Software des Auftraggebers.
- Optional, nur wenn vom Auftraggeber eingeschaltet: Bereitstellung des Zugriffs von außen auf die Weboberfläche der Software und Adressprüfung im Versandmodul.
- Bereitstellung von Softwarelösungen im Rahmen von Hosting, ASP, SaaS oder cloudbasierten Angeboten.

Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt; § 10 Abs. 2 bleibt unberührt.
(2) Art der verarbeiteten Daten (Datenarten)
Gegenstand der Verarbeitung können – je nach Nutzung der Systeme durch den Auftraggeber – folgende Datenarten sein:

- Bestands- und Stammdaten (z. B. Namen, Anschriften, Kundennummern, Umsatzsteuer-Identifikationsnummern)
- Kontaktdaten (z. B. Telefonnummern, E-Mail-Adressen)
- Vertrags-, Bestell- und Abrechnungsdaten (z. B. Bestellpositionen, Belege, Bestellungen als PDF-Datei oder Foto)
- Nutzungs- und Protokolldaten (z. B. IP-Adressen, Logfiles und Logauszüge, Zugriffszeiten, Benutzernamen der Software)
- Inhaltsdaten (z. B. vom Auftraggeber in die Software eingegebene Texte oder Dokumente, Inhalte von Supportanfragen, Anfragen an die KI-gestützten Funktionen)

(3) Kategorien betroffener Personen
Die von der Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter und Beschäftigte des Auftraggebers, auch als Benutzer der Software
- Kunden, Interessenten und Vertragspartner des Auftraggebers, insbesondere Endkunden und Ansprechpartner von Geschäftskunden
- Lieferanten und sonstige Dritte, deren Daten der Auftraggeber in den Systemen verarbeitet

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten ergeben. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung

mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.
(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des anwendbaren Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das bedeutet insbesondere die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Dies beinhaltet insbesondere:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Kontext der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Anlage 2 diesem Vertrag beigefügt. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.
(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
(4) Der Auftragnehmer ist gesetzlich nicht zur Benennung eines Datenschutzbeauftragten verpflichtet, da er in der Regel weniger als 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 BDSG). Ansprechpartner für Datenschutz ist: Marco Schauer, Kolpingstraße 20, 77855 Achern, E-Mail: marco@maniacdev.de, Telefon: +49 7841 8389020.
(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber angemessen bei der Einhaltung der in den Artikeln 33 bis 36 DS-GVO genannten Pflichten (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Dazu gehört insbesondere:

- Der Auftragnehmer teilt dem Auftraggeber Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 36 Stunden nach Bekanntwerden mit. Das gilt vor allem im Hinblick auf Melde- und Benachrichtigungspflichten

des Auftraggebers nach Art. 33 und 34 DS-GVO.

- Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber führt der Auftragnehmer nur nach vorheriger Weisung durch.
- Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und bei vorherigen Konsultationen der Aufsichtsbehörde (Art. 36 DS-GVO).

Die gesetzlichen Unterstützungspflichten des Auftragnehmers gemäß diesem Absatz 5 sowie gemäß Art. 28 Abs. 3 DS-GVO sind grundsätzlich mit der vertraglich vereinbarten Vergütung abgegolten. Ausgenommen hiervon ist jeglicher Aufwand, der durch ein dem Auftraggeber zuzurechnendes Verhalten, durch einen Vorfall oder eine Datenpanne in der Sphäre des Auftraggebers oder durch spezifische, über den technischen und organisatorischen Standard des Auftragnehmers hinausgehende Anforderungen des Auftraggebers entsteht. Ein solcher außergewöhnlicher Mehraufwand wird nach vorheriger Abstimmung zwischen den Parteien gesondert vergütet.

(6) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Der Auftragnehmer unterstützt den Auftraggeber darüber hinaus dabei, dass die betroffene Person auf Verlangen Auskunft über die zu ihr gespeicherten personenbezogenen Daten gemäß Art. 15 DS-GVO erhält.

(8) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und auf Verlangen in geeigneter Weise nachzuweisen.

(9) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebiets darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Dabei gilt:

- Für KI-Modelle legt der Auftragnehmer bei seinen Unterauftragsverarbeitern Regionen in der EU fest.
- Für Unterauftragsverarbeiter mit Sitz im Vereinigten Königreich stützt sich die Übermittlung auf den Angemessenheitsbeschluss der EU-Kommission (Art. 45 DS-GVO).
- Soweit Unterauftragsverarbeiter in den USA eingesetzt werden, erfolgt die Absicherung primär auf Grundlage einer gültigen Zertifizierung unter dem EU-US Data Privacy Framework (DPF) oder hilfsweise über die Standardvertragsklauseln der EU-Kommission einschließlich eines Transfer Impact Assessments (TIA).

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer verantwortlich (Verantwortlicher). Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber. Er entscheidet insbesondere selbst, ob er die KI-gestützten Funktionen, den Supportzugriff, den Zugriff von außen und die Adressprüfung einschaltet.
(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftraggeber trägt hierdurch anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.
(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen freistellen, sofern die unrechtmäßige Datenverarbeitung auf Handlungen des Auftraggebers, seiner Mitarbeiter oder durch den Auftraggeber beauftragter Dritter zurückzuführen ist. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten), werden die entstehenden Kosten und der Aufwand im gegenseitigen Einvernehmen erstattet.
(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.

§ 5 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.
(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihnen bei.
(3) Kontrollen sollen höchstens einmal jährlich erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.
(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und

organisatorischen Maßnahmen anstatt durch eine Vor-Ort-Kontrolle durch die Vorlage eines geeigneten Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revisor, interner oder externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder einer geeigneten Datenschutz-Zertifizierung durch eine zugelassene Stelle erbracht werden („Zertifizierungsurkunde“). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu überzeugen.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, zur Erfüllung seiner vertraglich vereinbarten Leistungen weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen (Art. 28 Abs. 2 DS-GVO). Mit den in Anlage 1 benannten Unterauftragsverarbeitern ist der Auftraggeber einverstanden. Im Fall der Einschaltung von im Sinne der §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmen als Unterauftragsverarbeiter erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung. Die jeweils aktuelle Fassung der Anlage 1 veröffentlicht der Auftragnehmer auf seiner Website unter https://www.webshopschnittstelle.de/impressum-agb/unterauftragsverarbeiter/.
(2) Über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informiert der Auftragnehmer den Auftraggeber mindestens vier Wochen vorher per E-Mail an die beim Auftragnehmer hinterlegte Adresse und auf der in Absatz 1 genannten Seite. Der Auftraggeber kann der Änderung innerhalb dieser Frist widersprechen. Der Widerspruch ist nur aus wichtigem, dem Auftragnehmer nachzuweisendem datenschutzrechtlichem Grund zulässig. Widerspricht der Auftraggeber nicht innerhalb der Frist, gilt die Änderung als genehmigt. Bei einem berechtigten Widerspruch kann der Auftraggeber die betroffene Funktion in der Software abschalten; weitere Ansprüche, insbesondere ein Recht zur Kündigung des Hauptvertrages, ergeben sich daraus nicht. Ist die Hinzuziehung zur Abwehr einer akuten Gefahr für die Sicherheit der Daten erforderlich oder ändert ein Unterauftragsverarbeiter seinerseits kurzfristig seine Unterauftragsverarbeiter, kann die Information ausnahmsweise unverzüglich nachträglich erfolgen.
(3) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(4) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Datenschutzpflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragsverarbeiters zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

Setzt ein Unterauftragsverarbeiter seinerseits kurzfristig weitere Unterauftragsverarbeiter ein, informiert der Auftragnehmer den Auftraggeber unverzüglich, nachdem er davon Kenntnis erlangt hat.

§ 7 Informationspflichten

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne von Art. 4 Nr. 7 DS-GVO liegen.

§ 8 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des letztbestehenden Hauptvertrages.
(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen, herauszugeben oder zu sperren. Bei einer Löschung sperrt und löscht der Auftragnehmer insbesondere die Installation des Auftraggebers in der maniac-Zentrale, entfernt einen eingerichteten Zugriff von außen und löscht Supportfälle nach Ablauf der in Anlage 2 genannten Fristen. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Rechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z. B. gesetzliche Aufbewahrungspflicht).
(3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Dadurch entstehende zusätzliche Kosten für die Herausgabe oder Löschung der Daten trägt der Auftraggeber.

§ 9 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.
(2) Diese Vereinbarung kann schriftlich oder in einem elektronischen Format geschlossen werden (Art. 28 Abs. 9 DS-GVO), insbesondere durch die Bestätigung eines berechtigten Administrators des Auftraggebers in der Software. Dabei werden Benutzer, Zeitpunkt und Fassung dieser Vereinbarung protokolliert. Änderungen und Ergänzungen bedürfen derselben Form und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Änderungen der Anlage 1 und der Anlage 2 erfolgen nach § 6 Abs. 2 bzw. § 3 Abs. 2.
(3) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Falls der Auftraggeber Kaufmann im Sinne des Handelsgesetzbuches ist oder seinen Sitz im Ausland hat, wird als ausschließlicher

Gerichtsstand der Hauptsitz der maniac developer GmbH vereinbart.
(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

§ 10 KI-gestützte Funktionen und Data Act

(1) Beim Einsatz von Systemen mit Künstlicher Intelligenz (KI) im Rahmen der Leistungserbringung erfüllt der Auftragnehmer die ihn treffenden Pflichten aus der KI-Verordnung (VO (EU) 2024/1689).
(2) Der Auftragnehmer garantiert, dass personenbezogene Daten des Auftraggebers nicht ohne dessen ausdrückliche, schriftliche Einwilligung für das Training von KI-Modellen des Auftragnehmers oder von beteiligten Drittanbietern verwendet werden.
(3) Die Maßnahmen zum Schutz personenbezogener Daten bei den KI-gestützten Funktionen, insbesondere zu Pseudonymisierung und Speicherung, sind in Anlage 2 beschrieben. Sie können nach § 3 Abs. 2 an den technischen Fortschritt angepasst werden.
(4) Die Ergebnisse der KI-gestützten Funktionen sind Vorschläge. Ihre Prüfung und Übernahme liegt in der Verantwortung des Auftraggebers; das gilt auch, soweit der Auftraggeber einzelne Funktionen auf automatische Ausführung stellt. Eine Gewähr für die inhaltliche Richtigkeit der Ergebnisse übernimmt der Auftragnehmer nicht. Eine automatisierte Entscheidung im Einzelfall gegenüber betroffenen Personen im Sinne von Art. 22 DS-GVO ist nicht Gegenstand der Leistung.
(5) Der Auftraggeber kann die KI-gestützten Funktionen jederzeit in der Software abschalten.
(6) Die Bereitstellung und der Export von Daten bei Vertragsbeendigung oder Anbieterwechsel erfolgen im Einklang mit den Interoperabilitäts- und Portabilitätsvorgaben des EU Data Act (VO (EU) 2023/2854).

Ort, Datum: _____ Ort, Datum: _____

_____ _____
Auftraggeber Auftragnehmer

Anlage 1: Unterauftragsverarbeiter

Fassung 4.0 vom 09.11.2026

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen die folgenden Unterauftragsverarbeiter einsetzt. Änderungen kündigt der Auftragnehmer nach § 6 Abs. 2 an. Die jeweils aktuelle Fassung steht unter https://www.webshopschnittstelle.de/impressum-agb/unterauftragsverarbeiter/.

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Grundlage Drittland
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server für die maniac-Zentrale, das Supportsystem und den Relay-Server der Fernwartung (RustDesk)	Rechenzentren in Deutschland	entfällt
Requesty Ltd, 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, Vereinigtes Königreich (Company No. 15165717)	Weiterleitung der Anfragen der KI-gestützten Funktionen an KI-Modelle	EU-Gateway in Frankfurt am Main, Deutschland	Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich (Art. 45 DS-GVO)
Unterauftragsverarbeiter von Requesty: Amazon Web Services EMEA SARL, Luxemburg	Infrastruktur von Requesty	Frankfurt am Main (eu-central-1)	entfällt
Unterauftragsverarbeiter von Requesty: Amazon Web Services (Bedrock) und Microsoft (Azure AI)	KI-Modelle	EU-Regionen (eu-central-1 Frankfurt, germanywestcentral, francecentral)	entfällt (EU)
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	E-Mail (Google Workspace), u. a. für Supportanfragen	EU und weltweit	EU-US Data Privacy Framework (Art. 45 DS-GVO)
Zoho Corporation B.V., Beneluxlaan 4B, 3527 HT Utrecht, Niederlande	Ticketsystem für Supportanfragen (Zoho Desk, EU-Rechenzentrum, bis zur Umstellung auf das eigene System)	EU	entfällt
Nur wenn „Zugriff von außen“ eingeschaltet ist: Cloudflare, Inc., 101	Tunnel zur Weboberfläche der Software; die	weltweit	EU-US Data Privacy Framework (Zertifizierung aktiv,

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Grundlage Drittland
Townsend St, San Francisco, CA 94107, USA	Verschlüsselung endet bei Cloudflare		geprüft am 10.11.2026), ergänzend Standardvertragsklauseln
Nur wenn die Adressprüfung eingeschaltet ist: KEPTAGO LTD (Geoapify), N. Nikolaidi & T. Kolokotroni, Onisiforou Center, 2nd Floor, 8011 Paphos, Zypern	Prüfung von Lieferanschriften (ohne Namen)	Rechenzentren in Deutschland und Finnland (Hetzner); Auslieferung über BunnyCDN (BUNNYWAY d.o.o., Slowenien)	entfällt
hostNET Medien GmbH, Osterdeich 107, 28205 Bremen, Deutschland	Mailserver für die Benachrichtigungen der maniac-Zentrale	Deutschland	entfällt

Die vollständige Liste der Unterauftragsverarbeiter von Requesty steht unter https://www.requesty.ai/privacy/subprocessors. Der Auftragnehmer nutzt daraus ausschließlich die oben genannten Anbieter und Regionen.

Nicht als Unterauftragsverarbeiter gelten Dienste, an die keine personenbezogenen Daten des Auftraggebers gehen. Dazu gehört DataForSEO OÜ, Tallinn, Estland, für die Konkurrenzanalyse (nur Artikelname, EAN und Suchbegriffe).

Anlage 2 zum AVV: Technische und organisatorische Maßnahmen (TOM) i. S. d. Art. 32 DSGVO

maniac developer GmbH, Kolpingstraße 20, 77855 Achern
Stand: 09.11.2026, gehört zur Vereinbarung über die Auftragsverarbeitung, Fassung 4.0
Organisationen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die maniac developer GmbH erfüllt diesen Anspruch durch die folgenden Maßnahmen.
Arbeitsorte. Die Mitarbeiter arbeiten im Homeoffice. Personenbezogene Daten der Auftraggeber werden auf deren eigenen IT-Systemen (Fernwartung) und auf Servern des Auftragnehmers bei der Hetzner Online GmbH in Rechenzentren in Deutschland verarbeitet. Auf den Arbeitsgeräten der Mitarbeiter werden Kundendaten nur vorübergehend und nur soweit für den Support nötig gespeichert.

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

1.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren.

- Server: Rechenzentren der Hetzner Online GmbH mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal; Hetzner ist nach ISO/IEC 27001 zertifiziert. Mitarbeiter des Auftragnehmers haben keinen physischen Zutritt.
- Homeoffice: Arbeitsgeräte stehen in abschließbaren Privaträumen und werden bei Abwesenheit gesperrt; Dritte erhalten keinen Zugang zu den Geräten.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Anmeldung mit persönlichem Benutzernamen und Passwort.
- Zwei-Faktor-Anmeldung für alle Zugänge, über die Kundendaten erreichbar sind (u. a. E-Mail, Server, KI-Konto, Verwaltung der Server).
- Virenschutz und Firewall auf allen Arbeitsgeräten, automatische Aktualisierung.
- Fernwartung über einen eigenen Relay-Server bei Hetzner; der Zugriff auf ein Kundensystem erfordert die Freigabe durch den Auftraggeber.
- Jede Installation meldet sich mit einem eigenen Schlüsselpaar bei der maniac-Zentrale an; eine Sperre wirkt sofort.
- Organisatorisch: automatische und manuelle Bildschirmsperre bei Verlassen des Arbeitsplatzes.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Berechtigte nur auf die Daten ihrer Berechtigung zugreifen können.

- Berechtigungen nach Aufgabe; Zugänge ausgeschiedener Mitarbeiter werden sofort gesperrt.
- Supportzugriff über die maniac-Zentrale nur lesend und nur, wenn der Auftraggeber ihn in der

Software erlaubt hat; personenbezogene Werte gehen dabei nur als Platzhalter hinaus. Jeder Zugriff wird beim Auftraggeber protokolliert.
- Sichere Löschung von Datenträgern, Vernichtung von Papier per Aktenvernichter.

1.4 Trennungskontrolle

- Trennung von Produktiv- und Testumgebung; Entwicklung und Tests nur mit Testdaten.
- Daten der Auftraggeber werden je Installation getrennt geführt (Mandantentrennung).
- Steuerung über Berechtigungen.

1.5 Pseudonymisierung

- Vor dem Senden an KI-Modelle und in Fehlerberichten ersetzt die Software Namen, Anschriften, E-Mail-Adressen und Telefonnummern durch Platzhalter. Im Klartext geht nur, was für das Ergebnis nötig ist.

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

2.1 Weitergabekontrolle

- Übertragung nur verschlüsselt (HTTPS bzw. TLS, SFTP).
- KI-Anfragen laufen ausschließlich über die maniac-Zentrale und das EU-Gateway von Requesty zu KI-Modellen in EU-Rechenzentren; alle anderen Modellanbieter sind im Konto gesperrt.
- Die maniac-Zentrale speichert den Inhalt von KI-Anfragen nicht, nur Angaben je Aufruf (Dauer, Umfang, Kosten).
- Bei Requesty ist die Speicherung von Inhalten abgeschaltet (Zero Data Retention, seit 05.11.2026).

2.2 Eingabekontrolle

- Protokollierung von Eingabe, Änderung und Löschung von Daten in der Software.
- Protokollierung der Datenschutz-Einstellungen des Auftraggebers (Mina nutzen, Supportzugriff, Betriebsdaten, Fehlermeldungen) mit Benutzer und Zeitpunkt.
- Protokollierung der Supportzugriffe beim Auftraggeber.

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

- Nächtliche Sicherung der Server.
- Laufende Datensicherung der Arbeitsdaten (Cloud und externe Sicherungsmedien).
- Notschalter, mit dem die KI-gestützten Funktionen global oder je Installation sofort abgeschaltet werden können.
- Die Software läuft beim Auftraggeber; fällt die maniac-Zentrale aus, laufen die Grundfunktionen der Schnittstelle weiter.

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

Art. 25 DSGVO)

4.1 Datenschutz-Management

- Alle Mitarbeiter sind im Arbeitsvertrag zur Vertraulichkeit verpflichtet.
- Die Mitarbeiter sind im Umgang mit Kundendaten und KI-gestützten Funktionen erfahren.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich und bei wesentlichen Änderungen; zuletzt am 09.11.2026.

4.2 Umgang mit Datenschutzverletzungen

- Ein Verdacht auf eine Datenschutzverletzung geht sofort an die Geschäftsführung.
- Die Geschäftsführung bewertet den Fall und informiert den Auftraggeber spätestens innerhalb von 36 Stunden nach Bekanntwerden (§ 3 Abs. 5 AVV).
- Betroffene Zugänge werden gesperrt, bei KI-Funktionen über den Notschalter.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Die KI-Assistentin Mina ist ab Werk ausgeschaltet; der Auftraggeber schaltet sie selbst ein.
- Optionale Funktionen mit weiteren Empfängern (Zugriff von außen, Adressprüfung) sind ab Werk aus.

4.4 Auftragskontrolle (Unterauftragsverarbeiter)

- Auswahl der Unterauftragsverarbeiter nach Datenschutz und Datensicherheit; mit jedem besteht ein Vertrag nach Art. 28 DSGVO (Anlage 1).
- Die Verträge, Listen und Nachweise der Unterauftragsverarbeiter werden beim Auftragnehmer abgelegt.

5. Aufbewahrung und Löschung

Daten	Höchstdauer
Inhalte von KI-Anfragen in der maniac-Zentrale	werden nicht gespeichert
Angaben je KI-Aufruf (Dauer, Umfang, Kosten)	400 Tage
Fehlerberichte und Supportzugriffe	13 Monate
Betriebsdaten der Installation	25 Monate
Supportfälle und Kopien von Kundendaten für den Support	12 Monate nach Abschluss des Supportfalls

Ausgefüllt für die Organisation durch:
Marco Schauer, Geschäftsführer, Telefon +49 7841 8389020, marco@maniacdev.de

Vom Auftraggeber auszufüllen:
Geprüft am _____ durch _____
Ergebnis:
☐ Es besteht noch Klärungsbedarf zu _____
☐ Die TOM sind für den angestrebten Schutzzweck ausreichend.
☐ Die Vereinbarung zur Auftragsverarbeitung kann geschlossen werden.