VERTRAG ÜBER DIE AUFTRAGSVERARBEITUNG PERSONENBEZOGENER DATEN

für die Nutzung von ZemiPro · Version 1.1 · Stand 05.09.2026

zwischen

Guido Schedlbauer
EDV-Beratung - Softwareentwicklung
Finkenstr. 41
94315 Straubing
Deutschland

vertreten durch
Guido Schedlbauer

im Folgenden: Auftragnehmer

und

dem jeweiligen Vertragspartner des Hauptvertrags über die Nutzung von ZemiPro

im Folgenden: Auftraggeber

Der elektronische Abschluss dieses Vertrages wird dem jeweiligen ZemiPro-Konto zugeordnet und unter Angabe der Vertragsversion und des Abschlusszeitpunkts in ZemiPro dokumentiert.

1. EINLEITUNG, GELTUNGSBEREICH, DEFINITIONEN

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“)

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Erklärungen, Weisungen und Mitteilungen im Rahmen dieses Vertrages können in Textform oder in elektronischer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist. Dieser Vertrag kann elektronisch abgeschlossen und der Abschluss innerhalb von ZemiPro dokumentiert werden.

2. GEGENSTAND UND DAUER DER VERARBEITUNG

2.1. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung bzw. Erfassung, Speicherung, Organisation, Auswertung, Bereitstellung,

Übermittlung und Löschung personenbezogener Daten, die der Auftraggeber im Rahmen der Nutzung der webbasierten Anwendung ZemiPro verarbeitet oder durch seine Nutzer verarbeiten lässt.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag über die Nutzung der Software-as-a-Service-Anwendung ZemiPro einschließlich der hierfür geltenden Allgemeinen Geschäftsbedingungen (im Folgenden „Hauptvertrag").

2.2. Die Verarbeitung beginnt mit Bereitstellung bzw. produktiver Nutzung von ZemiPro für den Auftraggeber und erfolgt für die Dauer des Hauptvertrags. Soweit nach Beendigung des Hauptvertrags noch personenbezogene Daten im Auftrag verarbeitet werden, gelten die Regelungen dieses Vertrages bis zum tatsächlichen Ende der Verarbeitung fort.

3. Art und Zweck der Datenverarbeitung

3.1. Der Auftragnehmer stellt dem Auftraggeber die webbasierte Software-as-a-Service-Anwendung ZemiPro zur Zeiterfassung sowie zur Verwaltung von Kunden, Projekten, Projektzuordnungen, Nutzern und zugehörigen Auswertungen bereit. Im Rahmen des Betriebs, der Wartung, der Datensicherung sowie der technischen oder fachlichen Unterstützung kann der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers erhalten.

3.2. Die Verarbeitung durch den Auftragnehmer umfasst insbesondere das Erheben und Erfassen, Speichern, Ordnen, Zuordnen, Auslesen, Auswerten, Bereitstellen, Übermitteln, Sichern und Löschen der vom Auftraggeber innerhalb von ZemiPro verarbeiteten Daten sowie technisch erforderliche Protokollierungs- und Sicherungsvorgänge. Der Auftraggeber nutzt ZemiPro im Rahmen seiner gewerblichen oder selbständigen beruflichen Tätigkeit zur Organisation und Dokumentation von Arbeits- und Projektzeiten sowie damit verbundenen Kunden- und Projektdaten.

3.3. Die Verarbeitung dient der Bereitstellung und Nutzung von ZemiPro, insbesondere der Erfassung und Auswertung von Arbeits- und Projektzeiten, der Verwaltung von Nutzern, Kunden und Projekten, der Erstellung von Zeitnachweisen und Ausgabedokumenten, der Datensicherung sowie der technischen Bereitstellung, Wartung, Fehleranalyse und Unterstützung bei der Nutzung der Anwendung.

3.4. Es werden folgende Kategorien personenbezogener Daten verarbeitet:

- Stamm- und Identifikationsdaten (insbesondere Name, Anzeigename, Benutzerkennung, Unternehmenszuordnung)
- Kontakt- und Kommunikationsdaten (insbesondere E-Mail-Adresse, Telefonnummer und gegebenenfalls Anschrift)
- Beschäftigungs-, Organisations- und Zuordnungsdaten (z. B. Mitarbeiter-/Nutzerzuordnung, Projektverantwortung, Kunden- und Projektzuordnungen)
- Arbeits- und Projektzeitdaten (insbesondere Zeitbuchungen, Pausen, Zeiträume, Tätigkeits- und Projektbezug sowie daraus erzeugte Zeitnachweise und Auswertungen)
- Technische Nutzungs- und Protokolldaten (insbesondere IP-Adresse, Login-Zeitpunkte und technisch erforderliche System- und Protokolldaten).

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO sind nicht Gegenstand der vereinbarten Nutzung und dürfen dort nicht bestimmungsgemäß verarbeitet werden.

3.5. Von der Verarbeitung betroffen sind:

- Beschäftigte, freie Mitarbeiter und sonstige Nutzer des Auftraggebers
- Kunden, Auftraggeber, Ansprechpartner und sonstige Geschäftskontakte des Auftraggebers, soweit deren Daten in ZemiPro gespeichert werden
- Projektbeteiligte und weitere natürliche Personen, deren Daten der Auftraggeber im Rahmen der vertragsgemäßen Nutzung von ZemiPro verarbeitet

4. PFLICHTEN DES AUFTRAGNEHMERS

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

4.10. Die Kernverarbeitung und Speicherung der ZemiPro-Anwendungsdaten erfolgt grundsätzlich innerhalb der EU bzw. des EWR. Soweit in Anlage 2 benannte Unterauftragnehmer Daten in einem Drittland verarbeiten oder ein Drittlandzugriff nicht ausgeschlossen werden kann, erfolgt dies nur unter Beachtung der Voraussetzungen der Art. 44 ff. DSGVO und der jeweils erforderlichen geeigneten Garantien. Mit Abschluss dieses Vertrages stimmt der Auftraggeber dem Einsatz der in Anlage 2 benannten Unterauftragnehmer zu.

5. Technische und organisatorische Maßnahmen

5.1. Der Auftragnehmer setzt die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen ein. Diese Maßnahmen bilden das vereinbarte Mindestschutzniveau für die Verarbeitung personenbezogener Daten.

5.2. Die technischen und organisatorischen Maßnahmen können der technischen und organisatorischen Weiterentwicklung sowie der Risikolage entsprechend angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen werden angemessen zeitnah umgesetzt. Wesentliche Änderungen werden dokumentiert.

5.3. Der Auftragnehmer informiert den Auftraggeber, wenn ihm bekannt wird, dass die eingesetzten Schutzmaßnahmen den gesetzlichen Anforderungen oder dem vereinbarten Schutzniveau nicht mehr entsprechen.

5.4. Kundendaten werden logisch voneinander getrennt verarbeitet. Die Trennung erfolgt insbesondere durch mandantenbezogene Zuordnung innerhalb der Anwendung und der Datenbank.

5.5. Kopien oder Duplikate personenbezogener Daten werden nur erstellt, soweit dies für den Betrieb, die Datensicherung, Wiederherstellung, Fehleranalyse oder sonstige technisch erforderliche Zwecke notwendig ist.

5.6. Eine Verarbeitung außerhalb der Geschäftsräume des Auftragnehmers ist zulässig, sofern durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau gewährleistet wird.

5.7. Der Auftraggeber ist berechtigt, die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen sowie der Pflichten aus diesem Vertrag in angemessenem Umfang zu überprüfen. Der Nachweis kann insbesondere durch geeignete Dokumentationen, Auskünfte, Zertifikate, Prüfberichte oder vergleichbare Nachweise des Auftragnehmers oder seiner Unterauftragnehmer erfolgen.

6. Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung

6.1. Im Rahmen des Auftrags verarbeitete personenbezogene Daten werden vom Auftragnehmer nur entsprechend der vertraglichen Vereinbarung oder auf dokumentierte Weisung des Auftraggebers berichtigt, gelöscht oder in ihrer Verarbeitung eingeschränkt.

6.2. Soweit der Auftraggeber entsprechende Weisungen erteilt, setzt der Auftragnehmer diese im Rahmen der technisch und rechtlich bestehenden Möglichkeiten um. Dies gilt auch nach Beendigung des Hauptvertrags, soweit noch personenbezogene Daten im Auftrag verarbeitet werden.

7. Unterauftragsverhältnisse

7.1. Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist zulässig. Der Auftragnehmer erteilt dem Auftraggeber auf Verlangen Auskunft über die im Rahmen der Auftragsverarbeitung eingesetzten Unterauftragnehmer.

7.2. Die Verantwortlichkeiten des Auftragnehmers und des jeweiligen Unterauftragnehmers sind eindeutig voneinander abzugrenzen.

7.3. Weitere Unterbeauftragungen durch einen Unterauftragnehmer sind zulässig, sofern die Anforderungen des Art. 28 DSGVO eingehalten werden.

7.4. Der Auftragnehmer wählt Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.5. Soweit Unterauftragnehmer personenbezogene Daten außerhalb der EU bzw. des EWR verarbeiten oder ein Drittlandzugriff nicht ausgeschlossen werden kann, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und geeignete Garantien bestehen.

7.6. Der Auftragnehmer stellt sicher, dass den eingesetzten Unterauftragnehmern die für die jeweilige Verarbeitung erforderlichen Datenschutzpflichten gemäß Art. 28 DSGVO auferlegt werden. Die Einhaltung der datenschutzrechtlichen Anforderungen wird regelmäßig in angemessenem Umfang überprüft und dokumentiert. Die Dokumentation wird dem Auftraggeber auf Verlangen in angemessenem Umfang zur Verfügung gestellt.

7.7. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.8. Die zum Zeitpunkt des Abschlusses dieses Vertrages eingesetzten Unterauftragnehmer sind in Anlage 2 mit Namen, Sitz und Art der erbrachten Leistung aufgeführt.

7.9. Unterauftragsverhältnisse im Sinne dieses Vertrages sind nur solche Leistungen, die einen unmittelbaren Zusammenhang mit der Erbringung der ZemiPro-Leistung aufweisen. Nebenleistungen ohne unmittelbaren Bezug zur Auftragsverarbeitung sind hiervon nicht erfasst. Die Pflicht des Auftragnehmers, auch insoweit ein angemessenes Datenschutz- und Sicherheitsniveau sicherzustellen, bleibt unberührt.

7.10. Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragnehmern werden dem Auftraggeber in geeigneter elektronischer Form mitgeteilt; der Auftraggeber erhält Gelegenheit, der Änderung aus sachlich begründeten datenschutzrechtlichen Gründen zu widersprechen. Kann der Auftragnehmer dem Widerspruch nicht abhelfen, ist er berechtigt, die hiervon betroffene Leistung oder den Hauptvertrag unter Einhaltung einer angemessenen Frist zu kündigen.

8. Rechte und Pflichten des Auftraggebers

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in dokumentierter Form. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung oder der Erbringung der vereinbarten Leistungen feststellt.

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen und vertraglichen Pflichten des Auftragnehmers in angemessenem Umfang zu überprüfen. Der Auftragnehmer kann hierfür insbesondere geeignete Auskünfte, Dokumentationen, Zertifikate, Prüfberichte oder sonstige geeignete Nachweise bereitstellen.

8.5. Soweit diese Nachweise im Einzelfall nicht ausreichen und eine weitergehende Prüfung erforderlich ist, kann der Auftraggeber eine Kontrolle durch sich selbst oder einen zur Vertraulichkeit verpflichteten fachkundigen Dritten verlangen. Die Prüfung ist mit angemessener Vorankündigung, während der üblichen Geschäftszeiten und unter möglichst geringer Beeinträchtigung des Geschäftsbetriebs durchzuführen. Ein Zugriff auf Daten anderer Kunden, auf Geschäftsgeheimnisse oder auf sicherheitskritische Systeme und Informationen ist ausgeschlossen, soweit dies für die Prüfung nicht zwingend erforderlich ist. Gleichwertige Nachweise können an die Stelle einer unmittelbaren Einsichtnahme treten. Kontrollen finden grundsätzlich nicht häufiger als einmal innerhalb von zwölf Monaten statt, soweit nicht ein besonderer datenschutzrechtlicher Anlass eine weitere Kontrolle erforderlich macht.

8.6. Kosten einer Kontrolle trägt der Auftraggeber, soweit die Kontrolle nicht aufgrund eines Verstoßes des Auftragnehmers erforderlich wird.

9. MITTEILUNGSPFLICHTEN

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten, die die Auftragsverarbeitung betreffen, unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung erfolgt nach Möglichkeit innerhalb von 24 Stunden nach Bekanntwerden des Vorfalls.
Die Mitteilung enthält, soweit zum Zeitpunkt der Meldung bekannt und verfügbar, insbesondere:

- eine Beschreibung der Art der Datenschutzverletzung,
- soweit möglich die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze,
- die Kontaktdaten einer Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen,
- eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung bzw. Begrenzung der Auswirkungen.

9.2. Weitere Informationen werden dem Auftraggeber nachgereicht, sobald sie verfügbar sind.

9.3. Der Auftragnehmer informiert den Auftraggeber ebenfalls unverzüglich über Verstöße gegen datenschutzrechtliche Bestimmungen sowie über Kontrollen oder Maßnahmen von Aufsichtsbehörden, soweit diese im Zusammenhang mit der Auftragsverarbeitung stehen.

9.4. Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei der Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO.

10. WEISUNGEN

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Die zur Erteilung und Entgegennahme von Weisungen befugten Personen bzw. Funktionen ergeben sich aus Anlage 3.

10.3. Änderungen der weisungsberechtigten Personen auf Seiten des Auftraggebers sind durch Aktualisierung der hinterlegten Administratoren oder durch ausdrückliche Mitteilung an den Auftragnehmer zu dokumentieren.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder zu einer Haftung des Auftragnehmers führen kann. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10.5. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.

11. BEENDIGUNG DES AUFTRAGS

11.1. Während der Vertragslaufzeit stellt der Auftragnehmer dem Auftraggeber die im Rahmen der vertragsgemäßen Nutzung vorgesehenen Möglichkeiten zur Sicherung und zum Export seiner Daten zur Verfügung. Der Auftraggeber ist dafür verantwortlich, benötigte Daten rechtzeitig vor Vertragsende zu sichern oder zu exportieren.

11.2. Nach Wirksamwerden der Vertragsbeendigung werden die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers gelöscht oder ihm in einem geeigneten, technisch verfügbaren Format zur Verfügung gestellt. Nach erfolgter Bereitstellung werden die beim Auftragnehmer verbleibenden personenbezogenen Daten gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten oder Regelungen zum Anbieterwechsel entgegenstehen.

11.3. Soweit personenbezogene Daten aufgrund technischer Sicherungs- und Backupverfahren nach Vertragsende noch vorübergehend vorhanden sind, werden diese im Rahmen der regulären Lösch- und Überschreibzyklen gelöscht und bis dahin nicht mehr produktiv verarbeitet, soweit nicht eine gesetzliche Verpflichtung oder eine technisch erforderliche Wiederherstellung im Rahmen der Datensicherung besteht.

11.4. Der Auftragnehmer stellt sicher, dass die Löschung bzw. Rückgabe personenbezogener Daten auch bei den eingesetzten Unterauftragnehmern entsprechend den vertraglichen und gesetzlichen Vorgaben erfolgt.

11.5. Soweit der Auftraggeber im Rahmen eines Anbieterwechsels die Bereitstellung oder Übermittlung von Daten verlangt, gelten ergänzend die hierfür im Hauptvertrag bzw. in den Regelungen zum Anbieterwechsel vereinbarten Bestimmungen.

11.6. Dokumentationen und Nachweise, die gesetzlichen Aufbewahrungs- oder Nachweispflichten unterliegen, dürfen für die Dauer dieser Pflichten gespeichert werden.

12. VERGÜTUNG

12.1. Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. HAFTUNG

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

13.2. Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit personenbezogene Daten in seiner Verantwortung vom Auftragnehmer unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Unterauftragnehmer im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffer 13.3 gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14. SONDERKÜNDIGUNGSRECHT

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. SONSTIGES

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

15.2. Sollten Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, insbesondere durch Pfändung, Beschlagnahme, Insolvenzverfahren oder sonstige vergleichbare Ereignisse gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist.

15.3. Änderungen und Ergänzungen dieses Vertrages können in Textform oder elektronischer Form vereinbart und dokumentiert werden.

15.4. Die Einrede eines Zurückbehaltungsrechts hinsichtlich der im Auftrag verarbeiteten personenbezogenen Daten ist ausgeschlossen.

15.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Nachweis des elektronischen Vertragsschlusses

Der elektronische Abschluss wird in ZemiPro unter Zuordnung zum jeweiligen ZemiPro-Konto, zur Vertragsversion und zum Abschlusszeitpunkt dokumentiert.

ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Die folgenden Maßnahmen beschreiben das bei ZemiPro eingesetzte Mindestschutzniveau. Sie können entsprechend dem Stand der Technik weiterentwickelt werden, sofern das Schutzniveau nicht unterschritten wird.

ZUTRITTSKONTROLLE

Die produktiven ZemiPro-Systeme werden auf Serverinfrastruktur der STRATO GmbH betrieben. Der physische Zutritt zu den Rechenzentrumsbereichen wird durch STRATO kontrolliert. Büro- und Arbeitsbereiche des Auftragnehmers werden gegen unbefugten Zutritt geschützt; Besucher erhalten keinen unbeaufsichtigten Zugang zu produktiven Systemen.

ZUGANGSKONTROLLE

Zugänge zu den administrativen Systemen sowie zu ZemiPro werden durch individuelle Benutzerkonten und Authentifizierungsverfahren geschützt. Administrative Berechtigungen werden nur autorisierten Personen erteilt. Für Benutzerkonten kann optional eine Zwei-Faktor-Authentifizierung (2FA) aktiviert werden. Übertragungen erfolgen verschlüsselt über TLS/HTTPS. Für Benutzer kann zusätzlich die Anmeldung über Google bzw. Microsoft mittels OpenID Connect genutzt werden.

ZUGRIFFSKONTROLLE

Berechtigungen innerhalb von ZemiPro werden rollen- und funktionsbezogen vergeben. Administrative Zugriffe auf produktive Daten werden auf das für Betrieb, Wartung, Support und Fehleranalyse erforderliche Maß beschränkt. Zugänge und Berechtigungen werden bei Wegfall der Erforderlichkeit entzogen.

TRENNUNGSGEBOT UND MANDANTENTRENNUNG

Daten unterschiedlicher ZemiPro-Kunden werden innerhalb der Anwendung und der zugrunde liegenden Datenhaltung logisch mandantenbezogen getrennt. Test-, Entwicklungs- und Produktivumgebungen werden auf derselben Serverinfrastruktur in getrennten Instanzen und getrennten Datenbanken betrieben. Produktive Kundendaten werden grundsätzlich nicht in Entwicklungs- oder Testumgebungen übernommen. Soweit dies im Einzelfall technisch oder fachlich erforderlich ist, erfolgt die Verarbeitung nur im erforderlichen Umfang und unter Anwendung der vereinbarten Schutzmaßnahmen.

ÜBERTRAGUNGS- UND WEITERGABEKONTROLLE

Die Übertragung zwischen Browser und ZemiPro erfolgt verschlüsselt über HTTPS/TLS. Datenübermittlungen an Unterauftragnehmer erfolgen nur im Rahmen der vertraglich vorgesehenen Leistungen und unter Verwendung angemessener gesicherter Übertragungswege.

VERFÜGBARKEITSKONTROLLE UND DATENSICHERUNG

Die ZemiPro-Daten werden regelmäßig, grundsätzlich täglich, gesichert. Sicherungen werden getrennt vom produktiven System auf einem externen Speichersystem vorgehalten und dienen der Wiederherstellung des Anwendungsbetriebs bei technischen Störungen. Der Auftraggeber wird ergänzend darauf hingewiesen, wichtige Daten regelmäßig über die vorhandenen Exportfunktionen zu sichern.

INTEGRITÄT, SYSTEMSCHUTZ UND AKTUALISIERUNG

Die Server- und Anwendungsumgebung wird durch technische Schutzmaßnahmen wie Firewall- und Netzwerkschutz, Zugriffsbeschränkungen sowie regelmäßige Sicherheits- und Systemaktualisierungen geschützt. Sicherheitsrelevante Änderungen und erkannte Schwachstellen werden nach ihrer Dringlichkeit bewertet und bearbeitet.

PROTOKOLLIERUNG UND NACHVOLLZIEHBARKEIT

Technisch erforderliche System-, Zugriffs- und Fehlerprotokolle werden zur Sicherstellung des Betriebs, zur Fehleranalyse und zur Erkennung von Missbrauch verarbeitet. Der Zugriff auf solche Protokolle ist auf berechtigte Personen beschränkt.

LÖSCH- UND AUFBEWAHRUNGSKONTROLLE

Nutzdaten werden nach Vertragsende entsprechend dem Hauptvertrag, den gesetzlichen Vorgaben und den Regelungen zum Anbieterwechsel gelöscht. Gesetzlich aufbewahrungspflichtige Daten können hiervon ausgenommen sein. Temporäre Sicherungskopien werden im Rahmen der vorgesehenen Sicherungszyklen gelöscht bzw. überschrieben.

AUFTRAGSKONTROLLE UND UNTERAUFTRAGNEHMER

Unterauftragnehmer werden unter Berücksichtigung ihrer Eignung und der datenschutzrechtlichen Anforderungen ausgewählt. Mit Unterauftragnehmern werden, soweit erforderlich, die notwendigen Vereinbarungen nach Art. 28 DSGVO geschlossen. Verfügbare Sicherheits- und Datenschutzinformationen der Unterauftragnehmer werden dokumentiert und bei Bedarf überprüft.

INCIDENT- UND WIEDERHERSTELLUNGSMANAGEMENT

Sicherheits- und Datenschutzvorfälle werden bewertet, dokumentiert und nach den gesetzlichen und vertraglichen Vorgaben bearbeitet. Bei Verletzungen des Schutzes personenbezogener Daten wird der Auftraggeber gemäß Ziffer 9 informiert. Für technische Störungen bestehen Verfahren zur Wiederherstellung des Anwendungsbetriebs unter Verwendung vorhandener Sicherungen.

ANLAGE 2 – GEGENWÄRTIGE UNTERAUFTRAGNEHMER

Der Auftragnehmer bedient sich zur Erbringung der Auftragsverarbeitung zum Zeitpunkt des Vertragsschlusses der folgenden Unterauftragnehmer. Weitere Unterauftragnehmer können nach Maßgabe der Ziffer 7 eingesetzt werden.

Unterauftragnehmer	**Anschrift / Sitz**	**Leistung für ZemiPro**	**Drittland / Garantien**
STRATO GmbH	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Bereitstellung und Betrieb der Server-/VPS-Infrastruktur; Hosting technischer ZemiPro-Komponenten; HiDrive-Cloudspeicher für Datensicherungen; Bereitstellung der E-Mail-Infrastruktur	Kernleistung EU/EWR; etwaige Drittlandverarbeitung nach STRATO-AVV und Art. 44 ff. DSGVO
Cloudflare, Inc.	101 Townsend St., San Francisco, CA 94107, USA	Cloudflare Turnstile zur Absicherung von Registrierungs- und gegebenenfalls weiteren Authentifizierungsprozessen gegen Bots, Spam und automatisierten Missbrauch.	Cloudflare Customer DPA; Übermittlungen nur unter den Voraussetzungen der Art. 44 ff. DSGVO und den jeweils einschlägigen Garantien

Weitere eingesetzte Dienste, die nicht als Unterauftragnehmer dieses AV-Vertrags eingeordnet werden

Google Sign-In wird ausschließlich als optionaler Identitätsdienst genutzt. Anbieter für Nutzer im Europäischen Wirtschaftsraum ist grundsätzlich die Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland. Google Sign-In ist nicht als Unterauftragnehmer dieses AV-Vertrags eingeordnet.

Microsoft Single Sign-On wird ebenfalls ausschließlich als optionaler Identitätsdienst genutzt. Anbieter im Europäischen Wirtschaftsraum ist die Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland. Microsoft Single Sign-On ist nicht als Unterauftragnehmer dieses AV-Vertrags eingeordnet.

Lexware Office wird vom Auftragnehmer ausschließlich für eigene kaufmännische Zwecke, insbesondere zur Erstellung und Verwaltung von Rechnungen gegenüber ZemiPro-Kunden, eingesetzt. Anbieter ist die Haufe Service Center GmbH, Munzinger Straße 9, 79111 Freiburg, Deutschland. Dabei werden nur die hierfür erforderlichen Kunden-, Kontakt- und Abrechnungsdaten verarbeitet. Lexware Office ist nicht in die eigentliche, für den Auftraggeber erbrachte ZemiPro-Auftragsverarbeitung eingebunden; insbesondere werden dort keine ZemiPro-Nutz-, Projekt- oder Zeiterfassungsdaten verarbeitet. Für die Nutzung von Lexware Office besteht eine gesonderte Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO.

ANLAGE 3 – WEISUNGSBERECHTIGTE PERSONEN

WEISUNGSERTEILUNG DURCH DEN AUFTRAGGEBER

Weisungsberechtigt sind die im jeweiligen ZemiPro-Konto als Administratoren hinterlegten Personen sowie weitere Personen, die dem Auftragnehmer vom Auftraggeber ausdrücklich als weisungsberechtigt benannt wurden.

WEISUNGSENTGEGENNAHME DURCH DEN AUFTRAGNEHMER

Weisungen können gegenüber dem Auftragnehmer über die hierfür vorgesehenen Kontaktwege erteilt werden, insbesondere per E-Mail an info@zemipro.de sowie über gegebenenfalls im ZemiPro-Supportbereich angegebene weitere Kontaktadressen.