Vereinbarung zur Auftragsverarbeitung im Sinne von Artikel 28 Absatz 3 DSGVO

zwischen

(nachfolgend Auftraggeber)

und

Alchimedus Management GmbH
Schlegelstr. 7
90491 Nürnberg (nachfolgend Auftragnehmer)

Präambel

Die Alchimedus Management GmbH stellt dem Auftraggeber die Softwarelösungen **Linear B, Linear B 365, AQM3, Alchimedus Collab, Alchimedus Cobrain und die Toolbox Onlinefragebögen** zur Verfügung, mit der verschiedene Managementsysteme eingeführt, beraten und organisiert sowie Befragungen durchgeführt werden können. Die Alchimedus Management GmbH unterstützt den Auftraggeber außerdem durch Software-Support, der in der Regel telefonisch oder per E-Mail erfolgt.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Datenschutz Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff ,,Datenverarbeitung" oder ,,Verarbeitung" (von Daten) benutzt wird, wird die Definition der ,,Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3)

2. Gegenstand des Auftrags

(1) Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß des schriftlich vereinbarten Auftrags - nachfolgend ‚Hauptvertrag' genannt - soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt.

(2) Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

3. Dauer des Auftrags

(1) Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit der im Hauptvertrag vereinbarten Frist gekündigt werden. Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt.

4. Art und Zweck des Auftrags

(1) Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

(2) Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung aus dem Hauptvertrag erforderlichen Zwecke.

(3) Im Rahmen der Kundenprojektspeicherung auf unseren Servern, des Softwares- und Beratungssupports bzw. der Auswertung von Projekten werden personenbezogene Daten genutzt.

5. Art der personenbezogenen Daten und Kategorien von Betroffenen

(1) Die Arten und Kategorien der verarbeiteten Daten ergeben sich aus den vom Auftraggeber in der Software (Offline- und / oder Online-Version) hinterlegten Daten. Dies können bspw. Kontaktdaten von Kunden oder Lieferanten oder personenbezogene Daten von Mitarbeitern sein.

6. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und / oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(2) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden vom Auftragnehmer datenschutzgerecht vernichtet, sobald diese zur Vertragserfüllung nicht mehr benötigt werden.

(3) Der Auftragnehmer gewährleistet bei gesetzlicher Voraussetzung die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.

(4) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(5) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(6) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Gleiches gilt für das Fernmeldegeheimnis nach § 88 TKG und - in Kenntnis der Strafbarkeit - für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StG B. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht im gesetzlichen Rahmen auch nach Beendigung des Auftrages fort.

7. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz- Folgeabschatzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) 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

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Kontrollbefugnisse

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht sowie trägt zu Überprüfungen bei, die durch den vom Auftraggeber beauftragten Prüfer durchgeführt werden. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und dessen Prüfer zu verlangen. Der Auftragnehmer stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftraggeber zu, sofern der Auftraggeber dem Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftragnehmers oder Personen, die für Wettbewerber des Auftragnehmers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.

(2) Das Inspektionsrecht des Auftraggebers hat das Ziel, die Einhaltung der einem Auftragsverarbeiter obliegenden Pflichten gemäß der DSGVO und dieses Vertrages zu überprüfen. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel an der Einhaltung hat oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung für den Auftraggeber dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen lassen. Diese können zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden.

(3) Sollte eine Datenschutz Aufsichtsbehörde oder eine sonstige Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gelten die vorstehenden Regeln entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch ist.

10. Weitere Auftragsverhältnisse (Subunternehmer)

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 2 beigefügt. Für die in Anlage 2 aufgezahlten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Die Alchimedus Management GmbH verpflichtet sich im Gegenzug mit allen Subunternehmern Vertrage abzuschließen, die eine rechtskonforme Verarbeitung personenbezogener Daten gewährleisten.

11. Datengeheimnis / Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

12. Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung durchgeführt, dann gelten folgende Vereinbarungen:

(1) Der Auftragnehmer fuhrt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers durch. Die Fernwartung erfolgt, soweit möglich, ohne gleichzeitige Speicherung von Daten.

(2) Der Auftragnehmer löscht personenbezogene Daten, die er während der Fernwartung erhalten oder gewonnen hat, unverzüglich.

(3) Notwendige Datenübertragungen sind in verschlüsselter Form durchzuführen. Ausnahmen müssen mit dem Auftraggeber abgestimmt werden.

(4) Der Auftraggeber ist berechtigt die Fernwartungsarbeiten von einem Kotrollbildschirm zu verfolgen. Beide Parteien sind berechtigt die Fernwartungsaktivitäten zu protokollieren und die Protokolle eine angemessene Zeit aufzubewahren.

(5) Wird die Fernwartung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Serviceleistung im gleichen Maße zu gewährleisten, wie dies bei der Durchführung aus der Servicezentrale der Fall ist.

13. Austausch von Datenträgern

(1) Werden dem Auftragnehmer zum Zwecke der Prüfung von QM-Projekten Datenträger mit personenbezogenen Daten oder sonstigen vertraulichen Unterlagen ausgehändigt, so werden diese Datenträger dem Auftraggeber zurückgegeben bzw. physikalisch vernichtet, sobald diese nicht mehr zur Erfüllung des Vertrages notwendig sind.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Personen gewährleistet. Der Auftragnehmer ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

(2) Die aktuellen technischen und organisatorischen Ma nahmen sind im Anlage 1 aufgeführt.

(3) Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Ma nahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

(4) Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen zum Stand der Technik und Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird

15. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, auf Anweisung und nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart.

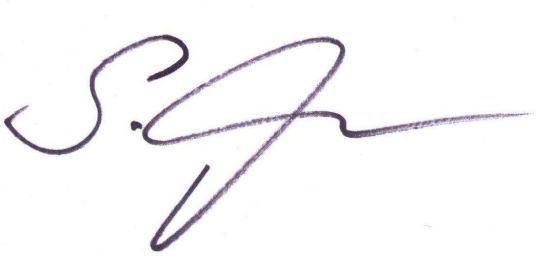
Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

16. Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Auftraggeber:	Auftragnehmer:

Ort, Datum, Unterschrift, Stempel	 Ort, Datum, Unterschrift
	Nürnberg, 07.11.2022

Ansprechpartner des Auftragnehmers:

Sascha Kugler
Schlegelstr. 7
90491 Nürnberg
E-Mail: sekretariat@alchimedus.com
Telefon: +49 (0) 911/956663-0
Telefax: +49 (0) 911/95 66 63-69

Auftraggeber:

Anlage 1

Technische und organisatorische Maßnahmen des Auftragnehmers gemäß Art. 32 DSGVO

1. Zutrittskontrolle
Der Zugang zum Serverraum ist nur berechtigten Personen gestattet. Der Serverschrank ist nochmal separat verschließbar.

2. Zugangskontrolle
Der Zugang zu den Serversystemen für administrative Zwecke erfolgt über Benutzername/Kennwort.

3. Zugriffskontrolle
Es existieren unterschiedliche Berechtigungen gemäß den unterschiedlichen Aufgaben der Mitarbeiter.

4. Trennungskontrolle
Entwicklungs-, Test- und Live-Systeme sind getrennt eingerichtet.

5. Weitergabekontrolle
Die Weitergabe von Daten an Dienstleister zur Auftragserfüllung erfolgt in verschlüsselter Form über verifizierte Kommunikationswege.

6. Eingabekontrolle
Dokumentation der Eingabeberechtigten

7. Verfügbarkeitskontrolle
- Es werden tägliche Backups der Daten in den verschiedenen Bereichen durchgeführt.
- Server sind mit redundanten Festplattensystemen ausgestattet.
- Unsere Server sind über eine unterbrechungsfreie Stromversorgung angebunden
- Das Wiederherstellen von Backups wird regelmäßig getestet.

8. Auftragskontrolle
Die Kompetenzen zwischen Auftraggeber und Auftragnehmer werden bei Datenverarbeitungsverträgen mittels folgender Maßnahmen abgegrenzt:
- Eindeutige Vertragsgestaltung, - Formalisierte Auftragserteilung, - Kontrolle der Vertragsausführung

9. Verwendungszweckkontrolle
Wir achten auf Sparsamkeit bei der Datenerhebung

10. Organisationskontrolle
- Schulung und Verpflichtung unserer Mitarbeiter, - Interne Aufgabenverteilung, - Funktionstrennung und -zuordnung, - Vertreterregelungen, - Interne Audits

Anlage 2

Subunternehmer

Firma	Teilleistung
KeywebAG Neuwerkstraße 45/46 D-99084 Erfurt	Serverhousing / techn. Serveradministration / Backup
impulsPark Ulf Schröder Birkenweg 5 17121 Görmin	Techn. Serveradministration / techn. Programmierungen

New SunWare Erik Memmert Ravenspurgerstraße 20 86150 Augsburg	Softwareentwickler in Augsburg, Bayern
Kube Studio GmbH Am Weinmarkt 10 Nürnberg	Softwareentwickler in Nürnberg, Bayern
DigitalOcean, LLC., 101 Avenue of the Americas, 10th Floor, New York, NY 10013, United States of America mit Serverstandort Deutschland, Frankfurt am Main.	Serverfirma