Vereinbarung

zwischen

[ ]

nachstehend „Auftraggeber“ genannt –

und

cometis AG
nachstehend „Auftragnehmer“ genannt

1. Gegenstand und Dauer des Auftrags

(a) Gegenstand
Der Auftragnehmer führt die in Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(b) Dauer
Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

2. Technisch-organisatorische Maßnahmen

(a) Die Datenverarbeitung und Datennutzung findet nur in den Geschäftsräumen und mit den Arbeitsmitteln, EDV- & Kommunikations-einrichtungen des Auftraggebers statt. Der Auftragnehmer stellt in seinem Verantwortungsbereich sicher, das die internen Vorschriften zur EDV-Sicherheit und Datensicherheit am Arbeitsplatz, zur Übermittlung und zum Transport gewahrt bleiben. Dies gilt insbesondere für die Sicherheit der Vertraulichkeit und Integrität der Daten.

3. Berichtigung, Einschränkung und Löschung von Daten

(a) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner des Auftragnehmers im Bereich Datenschutz, wird der externe Datenschutzbeauftragte des Auftraggebers benannt:

STRASEV UG
Frank Severin
Diekweg 16
26160 Bad Zwischenahn
Tel: 0151-175 16302
eMail: frank.severin@strasev.de.

(b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dem Auftragnehmer unterstehen zur Erfüllung seiner Aufgaben-stellung Mitarbeiter des Auftraggebers. Der Auftragnehmer hat in seinem Arbeitsgebiet darauf zu achten das die Bestimmungen zur Datensicherheit und zur Datenvertraulichkeit gewahrt bleiben.

(c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(f) Der Auftragnehmer kontrolliert regelmäßig seine internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5. Unterauftragsverhältnisse

(a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören 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.

(b) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher, schriftlicher, bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

6. Kontrollrechte des Auftraggebers

(a) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder, durch im Einzelfall zu benennende Prüfer, durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(b) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers, nach Art. 28 DSGVO, überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und unterwirft sich den technischen & organisatorischen Maßnahmen des Auftraggebers.

7. Mitteilung bei Verstößen des Auftragnehmers

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

1) 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 ermöglicht.

2) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

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

4) Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

5) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Weisungsbefugnis des Auftraggebers

(a) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).

(b) 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. Löschung und Rückgabe von personenbezogenen Daten

(a) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(b) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder, nach vorheriger Zustimmung, datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen, über das Vertragsende hinaus,

aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftrag-geber übergeben.

_____ Ort, Datum	_____ Ort, Datum
..... Auftraggeber	..... Auftragnehmer

Anlagen:

1. Auflistung der beauftragten Dienstleistungen
2. Technische und organisatorische Maßnahmen
3. Anerkannte Unterauftragsnehmer
4. weisungsberechtigte Personen

Anhang 1
Auflistung der beauftragten Dienstleistungen

Gegenstand der Verarbeitung:

Art und Zweck der Verarbeitung

Art der personenbezogenen Daten

Kategorien der betroffenen Daten

Anhang 2
Technische und organisatorische Maßnahmen

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

(a) **Zutrittskontrolle**

1) elektronischer Schlüssel protokolliert,
2) Schließsystem alarmgesichert,
3) protokollierte Schlüsselvergabe,
4) Wachdienst
5) Serverraum verschlossen

(b) **Zugangskontrolle**

1) Keine unbefugte Systembenutzung durch Kennwortsicherung
2) Aktive Firewall
3) Nutzung von Virenscanner auf dem jeweils neuesten Update-Status

(c) **Zugriffskontrolle**

1) Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch:

   - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
   - Protokollierung von Zugriffen

(d) **Trennungskontrolle**

1) Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B.:
   - Test-Normalbetrieb
   - Pseudonymisierung
     (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
     Personenbezogene Daten werden so pseudonymisiert, dass eine Weiterverarbeitung ohne Hinzuziehung zusätzlicher Informationen nicht mehr möglich ist.

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

(a) SSL Verschlüsselung
(b) Nutzungsprotokollierung
(c) Benutzerdefiniertes Login
(d) Kontaktdatenkontrolle über persönliches Login

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

(a) Verfügbarkeitskontrolle
Die Datensicherung erfolgt in einer Cloud

(b) Tägliche Backups garantieren das bei Verlust die Funktionsfähigkeit von EDV-Systemen keine Daten verloren gehen dadurch ist auch eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO) gegeben.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

(a) Datenschutz-Management;
(b) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) Opt-in/ Opt-Out-Funktion
(c) Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anhang 3
Anerkannte Unterauftragsnehmer

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Firma:
Strasse u. HausNr.:
PLZ u. Ort:
Tel:
eMail:

Anhang 4
Weisungsberechtigte Personen

Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position
Name Mitarbeiter	Position