Vereinbarung

zwischen

.....

.....

.....

- Verantwortlicher - nachstehend Auftraggeber genannt –

und

CONTEMPLAS GmbH

Albert-Einsteinstr. 6

D - 87435 Kempten

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Hiermit schließen der Auftraggeber und der Auftragnehmer die untenstehende Vereinbarung zur Auftragsverarbeitung ab.

Digital unterschrieben von CONTEMPLAS GmbH
Datum: 2018.08.24 12:56:18 +02'00'

.....	Kempten, 24.8.2018
Ort, Datum, Unterschrift Auftraggeber	Ort, Datum, Unterschrift Auftragnehmer
.....	Thomas Seeholzer, Geschäftsführer
Name in Druckbuchstaben	

Bitte senden Sie das unterschriebene Dokument an auftragsverarbeitung@contemplas.com
oder via FAX an +49 831 5645328.

Vereinbarung zur Auftragsverarbeitung

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Gegenstand des Auftrags zum Datenumgang ist die Durchführung von Fernwartungen der Software der CONTEMPLAS GmbH und der damit verbundenen Hardware (Kameras, Kraftmessplatten und weitere Sensoren) durch den Auftragnehmer.

(2) Dauer
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 14 Tagen zum Ende des Monats gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalt

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Der Auftraggeber initiiert eine Fernwartung mit dem Auftragsnehmer indem ein Austausch einer Verbindungsnummer stattfindet. Der Auftragnehmer nutzt die aufgebaute Verbindung um das vom Auftraggeber beschriebene Problem zu beheben.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
- Personenstammdaten
- Kommunikationsdaten
- Video- und Bilddaten

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Kunden
- Ansprechpartner
- Beschäftigte

3. Technisch-organisatorische Maßnahmen

(1) 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.
(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(3) 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.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten

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

- Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Seeholzer, Geschäftsführer, +49831 25436920, datenschutz@contemplas.com benannt.
- Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.
- Der Auftragnehmer kontrolliert regelmäßig die 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

Eine Unterbeauftragung ist unzulässig.

7. Kontrollrecht des Auftraggebers

(1) 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.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- 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
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- 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.

9. 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.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) 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.
(2) 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.
(3) 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 Auftraggeber übergeben.

Anhang:

Technische und Organisatorische Maßnahmen (TOM)

- Die CONTEMPLAS-Mitarbeiter wurden mit einer schriftlichen Vereinbarung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes verpflichtet und über die ordnungsgemäße Behandlung personenbezogener Daten belehrt.

- Die Fernwartung erfolgt mit PCVisit (siehe *www.pcvisit.de*). Auf spezielle Anforderung des Auftraggebers kann ein anderes Tool verwendet werden, wobei die Überprüfung der Sicherheitsaspekte dann beim Auftraggeber liegt.

- Mit PCVisit erfolgt die Übertragung der Bildschirmabbildungen verschlüsselt (256 Bit AES-Verschlüsselung) und mit zusätzlichen Sicherheitsmechanismen
(siehe *http://www.pcvisit.de/nc/de/produkte/fernwartung/sicherheit-technologie*).

- Mit PCVisit erfolgt die Übertragung der verschlüsselten Daten über die Server des Herstellers (ausschließlich Standort Deutschland).

- Die CONTEMPLAS-Mitarbeiter befolgen bei der Fernwartung die "Fernwartung Policy" (siehe Anhang).

- Zutrittskontrolle: CONTEMPLAS gewährleistet, dass keine Unbefugten Zutritt zu Datenverarbeitungsanlagen bekommen.

- Unter-Auftragsverarbeiter werden nicht eingesetzt.

- Die Daten werden nicht in Drittländer übermittelt.

- Es werden nur in Ausnahmefällen personenbezogene Daten auf dem CONTEMPLAS Rechner bzw. Netzwerk gespeichert.

- In diesen Ausnahmefällen wird der Auftraggeber über Art und Umfang der Daten sowie die Aufbewahrungs- und Löschfristen schriftlich informiert
(siehe "Fernwartung Policy")

- Mitteilungspflicht bei Störungen oder Verletzungen des Schutzes personenbez. Daten
Über die Speicherung der o.a. Ausnahmefälle wird Protokoll geführt.

- Recht auf Auskunft/Löschung betroffener Personen
- entfällt - da die Daten nur kurzfristig für die Dauer einer detaillierten Analyse gespeichert und dann sofort wieder gelöscht werden

Fernwartung Policy

Begriffe (bzgl. DSGVO)

Auftraggeber : Der Anwender eines CONTEMPLAS-Systems
Auftragsverarbeiter: CONTEMPLAS GmbH
Mitarbeiter: CONTEMPLAS Mitarbeiter, der die Fernwartung durchführt

Vertraulichkeit und Datenschutz

- Der Mitarbeiter wurde über die DSGVO, insbesondere über den Begriff “personenbezogene Daten” belehrt.
- Der Mitarbeiter hat sich schriftlich zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes verpflichtet.

Fernwartung

- Die Fernwartung erfolgt mit PCVisit und damit verschlüsselt und über deutsche Server.
- Die komplette Fernwartung erfolgt ausschließlich über die verschlüsselten Kanäle der Fernwartungs-Software

Start und Ende einer Fernwartung

- Eine Fernwartungs-Session wird nur auf ausdrückliche Anforderung seitens des Auftraggebers vorgenommen.
- Zum Start muss der Auftraggeber eine von der Fernwartungs-Software erzeugte Codenummer eingeben, sonst kann kein Zugriff erfolgen
- Während der Zugriff erfolgt, wird eine entsprechende Statusmeldung beim Auftraggeber angezeigt
- Nach dem Beenden kann kein weiterer Zugriff erfolgen

Zugangskontrolle

- Der Mitarbeiter stellt sicher, dass keine unbefugten Personen die Fernwartung beobachten oder manipulieren können
- Wenn der Mitarbeiter während einer Fernwartung seinen PC verlassen muss, so wird der PC gelockt und er kann nur durch Kennworteingabe weiter verwendet werden

Vermeidung personenbezogener Daten

- Bei Testabläufen wird ausschließlich mit fiktiven Personen bzw. Personendaten gearbeitet

Datenübertragung

- Der Mitarbeiter erstellt keine Abbildungen vom Bildschirminhalt (Screenshot, Abfotografieren etc.)
- Der Mitarbeiter überträgt keine Dateien vom PC des Auftraggebers auf seinen PC bzw. das CONTEMPLAS Netzwerk.
- Backups werden ausschließlich auf dem Rechner bzw. im Netz des Auftraggebers erstellt

Ausnahmen: Dateien ohne personenbezogene Daten

- Vom System erzeugte Log-Dateien, die keine personenbezogenen Daten enthalten
- Reportdateien, die ausschließlich mit fiktiven Testdaten gefüllt sind
- Videodateien, die geprüft werden müssen, auf denen aber keine “echten” Personen erkennbar sind

Weitere Ausnahmen

Alle anderen Dateien dürfen nur mit ausdrücklicher Zustimmung seitens des Auftraggebers kopiert/gespeichert werden.

- Die Daten werden nur kurzfristig (z.B. 24 Stunden) zur Durchführung einer detaillierten Analyse gespeichert.
- Die Daten werden in einem per Kennwort gesicherten Speicherort abgelegt.

Wenn diese Daten nach dem Ende der Fernwartung für eine detaillierte Analyse gespeichert werden, so muss der Auftraggeber darüber schriftlich (Email) informiert werden.
Diese Information beinhaltet auch eine genaue Auskunft zur Dauer der Datenspeicherung (Löschfrist).