Vereinbarung gemäß Art. 28 DS-GVO

zwischen dem/der

……

……
- Verantwortlicher - nachstehend Auftraggeber genannt –

und der

EDV-BV output management GmbH & Co. KG
Wernberger Str. 8 a
92536 Pfreimd

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

Dieser Ergänzungsvertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den zwischen Auftraggeber und Auftragnehmer geschlossenen Vertragsverhältnissen ergeben, auf die hier verwiesen wird. Er findet Anwendung auf alle Tätigkeiten, die mit diesen Vertragsverhältnissen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieses Ergänzungsvertrages richtet sich nach der Laufzeit der geschlossenen Vertragsverhältnisse.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in den zwischen Auftraggeber und Auftragnehmer geschlossenen Vertragsverhältnissen beschrieben, auf die hier verwiesen wird.

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.

(2) Art der Daten

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten
- ☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(3) Kategorien betroffener Personen

- ☒ Kunden/Mandanten
- ☒ Interessenten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☒ Handelsvertreter
- ☒ Ansprechpartner
- ☐ ...

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. Art. 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 des Auftragnehmers

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

a) Als Datenschutzbeauftragter ist beim Auftragnehmer
Rechtsanwalt Kurt Mieschala, rechtsanwalt@mieschala.de
bestellt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e) 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.

f) 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.

g) 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) 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.

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

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma (Unterauftragnehmer)	**Anschrift/Land**	**Leistung**
Steigauf Daten Systeme GmbH	Otto-Hahn-Str. 13a 85521 Riemerling	Supportunterstützung DocuWare Archiv
DocuWare Europe GmbH	Therese-Giehse-Platz 2 82110 Germering	Supportunterstützung DocuWare Archiv
K7 IT-Solutions GmbH	Wetterkreuz 3 91058 Erlangen	Supportunterstützung Belegerkennung, InnoScan
Risus GmbH	In den Klostergärten 4 65549 Limburg	Supportunterstützung DocuWare-Navision-Schnittstelle
Varelmann Beratungsgesell-schaft mbH	Uhlhornsweg 99 26129 Oldenburg	Supportunterstützung DocuWare-SAP-Schnittstelle
Sattel Business Solutions GmbH	Kiesgräble 25 89129 Langenau	Supportunterstützung Belegerkennung RecSolution
Quadient Germany GmbH & Co.KG	Landsberger Str. 154 80339 München	Supportunterstützung Output Management
ARTEC IT Solutions AG	Robert-Bosch-Str. 38 61184 Karben	Supportunterstützung E-Mail-Archiv-Appliance
Parashift AG	Hauptstraße134 4450 Sissach / Schweiz	Belegerkennung

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte 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;

☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(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.

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 und

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.

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. Die Löschung ist auf Anforderung schriftlich zu bestätigen.

(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.

.....	.....
Datum, Unterschrift Auftraggeber	Datum, Unterschrift Auftragnehmer

Anlagen: 1. Technisch-organisatorische Maßnahmen beim Auftragsverarbeiter

Anlage 1 – Technisch-organisatorische Maßnahmen – Sicherheit der Verarbeitung bei EDV-BV output management GmbH & Co. KG

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle

  Die Zutritte sind geregelt, die Schlüsselausgabe wird hausintern dokumentiert. Während und außerhalb der Geschäftszeiten ist die Eingangstüre verschlossen.

- Zugangskontrolle

  Die Passwörter werden nach Bedarf geändert werden und genügen zeitgemäßen Komplexitätsanforderungen.
  Alle Arbeitsplätze im Büro werden bei Verlassen des Arbeitsplatzes gesperrt, so dass auch der Zugriff auf einen nicht besetzten Arbeitsplatz schwer möglich ist. Firewall-Technik (Software-Firewall) und Antiviren-Software ist im Einsatz. Datenträger in Notebooks/Laptops sind verschlüsselt. Inhalte mobiler Datenträger haben eine passwortgeschützte Zugangskontrolle. Benutzerrechte und den IT Systemen zugeordnete Benutzerprofile werden nach jeweils konkreter Anforderung vergeben.

- Zugriffskontrolle

  Die Daten auf der Ablagestruktur sind mit Rechtegruppen so abgesichert, dass jeder Mitarbeiter nur auf die für seine Arbeit relevanten Daten zugreifen kann. Diese Rechte werden in regelmäßigen Abständen überprüft. Es existiert ein Berechtigungskonzept. Die Anzahl der Administratoren wird auf das Notwendigste reduziert. Es sind Aktenvernichter im Einsatz, die eine Vernichtung nach DIN 66399 gewährleisten. Es existiert eine Passwortrichtlinie, Passwörter müssen nach Bedarf gewechselt werden. Datenträger werden sicher aufbewahrt.

- Trennungskontrolle

  Der Auftragnehmer hat Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken ergriffen, beispielsweise durch Nutzung der Mandantenfähigkeit oder durch eine entsprechende Funktionstrennung (Produktion / Test).

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

  Soweit vom Auftraggeber im Einzelfall schriftlich angewiesen, werden Daten pseudonymisiert.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle

  Fernzugriffe auf das System des Auftraggebers erfolgen ausschließlich über eine geschlüsselte Verbindung.
  Notebooks und mobile Datenträger mit personenbezogenen Daten sind passwortgeschützt und / oder verschlüsselt. Das Mitbringen privater Datenträger ist untersagt.

- Eingabekontrolle

  Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines Berechtigungskonzepts.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

  Der Auftragnehmer hat Maßnahmen ergriffen, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, insbesondere:

  - die Nutzung von Festplatten-Spiegelungen, z.B. RAID-Verfahren,
  - eine hinreichend ausgelegte unterbrechungsfreie Stromversorgung (USV),
  - es werden Schutzsteckdosenleisten verwendet,
  - es sind Feuerlöschgeräte verfügbar,
  - Verwendung von Cloud-Servern in sicheren und klimatisierten Rechenzentren,
  - den Einsatz entsprechender Virenschutz- / Firewall-Lösungen,

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

  Datensicherungen werden an einem sicheren, ausgelagerten Ort (Cloud-Server) verwahrt.

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

- Datenschutz-Management:

  - Es finden regelmäßig Sensibilisierungsmaßnahmen zum Datenschutz für MitarbeiterInnen statt.
  - Es ist ein Datenschutzbeauftragter benannt.
  - Es gibt Regelungen über die Sicherung des Datenbestands
  - Es existiert ein Datenschutzkonzept
  - Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden
  - Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert.

- Incident-Response-Management:

  - Die Mitarbeiter sind bzgl. des Erkennens einer Datenpanne geschult.

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):

  Das Unternehmen hat sowohl technisch, als auch durch datenschutzfreundliche Voreinstellungen Maßnahmen ergriffen, um sicherzustellen, dass den Vorgaben des Art. 25 Abs. 2 DS-GVO Genüge getan wird.

- Auftragskontrolle

  - Auftragnehmer werden unter Sorgfaltsgesichtspunkten (insbesondere im Hinblick auf Datensicherheit) ausgewählt.
  - es erfolgen schriftliche Weisungen an den Auftragnehmer (z.B. durch Verträge zur Auftragsverarbeitung).
  - es findet eine vorherige Prüfung und Dokumentation der beim Auftragnehmer vorhandenen Maßnahmen zur Sicherheit der Verarbeitung statt.
  - die MitarbeiterInnen wurden zur Vertraulichkeit verpflichtet.
  - es ist sichergestellt, dass die Daten nach Beendigung des Auftrags vernichtet werden.