Vertrag zur Auftragsverarbeitung gem. Art. 28 EU-DSGVO

Diese Vereinbarung wird getroffen zwischen dem Verantwortlichen

Firma:	
Straße:	
PLZ Ort:	
Gesetzlich vertreten durch:	

- nachstehend „**Auftraggeber**“ genannt -

und dem Auftragsverarbeiter

schrempp edv GmbH – Rainer-Haungs-Straße 7 – 77933 Lahr
Gesetzlich vertreten durch die Geschäftsführer:
Brigitta Schrempp, Stefan Basler

- nachstehend „**Auftragnehmer**“ genannt –

- nachstehend sind Auftraggeber und Auftragnehmer zusammen die **Vertragspartner** –

§ 1 Begriffsbestimmungen (Art. 4 DS-GVO)

(1.) „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

(2.) „Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3.) „Verantwortlicher“ ist diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(4.) „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

§ 2 Inhalt der Vereinbarung (Art. 28 Abs. 3 DS-GVO)

(1.) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, welche sich aus dem bestehenden Vertragsverhältnis und den jeweils erteilten Einzelaufträgen und den darin festgelegten Pflichten ergeben. Sie findet Anwendung auf alle Tätigkeiten, die hiermit in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2.) In dieser Vereinbarung werden Gegenstand und Dauer der Verarbeitung (Ziffer 3), Art und Zweck der Verarbeitung (Ziffer 4), die Art der personenbezogenen Daten (Ziffer 5), die Kategorien betroffener Personen (Ziffer 6) und die Pflichten und Rechte der Vertragspartner (Ziffer 7 bis 17) beschrieben.

§ 3 Gegenstand und Dauer der Verarbeitung

(1.) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die durch das bestehende Vertragsverhältnis sowie durch die erteilten Einzelaufträge konkretisiert werden.

(2.) Ergänzend hierzu gilt folgende Beschreibung des Gegenstands der Verarbeitung:

• Hosting und / oder Bereitstellung von Softwareanwendungen in einem Rechenzentrum

• Systemdienstleistung ……..(z.B. Einrichtung, Pflege und Support der Software)

(3.) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des bestehenden Vertragsverhältnisses und der erteilten Einzelaufträge und tritt mit Unterzeichnung durch beide Vertragspartner in Kraft.

(4.) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat 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 Art. 44 ff. DS-GVO erfüllt sind.

§ 4 Art und Zweck der Verarbeitung

(1.) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag.

(2.) Ergänzend hierzu gilt folgende Beschreibung von Art und Zweck der Verarbeitung:

- Beratung
- Fernwartung bei Störungen und Fehlermeldungen der Software **SIVAS.ERP**
- Datensicherung / Backup
- Hilfe bei Software-Problemen
- Remote Zugriff
- Update - Service
- Prüfung der Datenbankeinträge
- Softwarepflege
- Installation und Konfiguration der Software **SIVAS.ERP**

§ 5 Art der personenbezogenen Daten

(1.) Die Art der verarbeiteten personenbezogenen Daten ergibt sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag.

(2.) Ergänzend hierzu gilt folgende Beschreibung der Art der verarbeiteten personenbezogenen Daten:

- Personenbezogene Daten, Adressdaten, Kontaktdaten etc.
- ggfs. Passwörter
- Kunden- und Interessentendaten
- Mitarbeiterdaten
- Umsatzdaten
- E-Mail / Posteingang

§ 6 Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieser Vereinbarung Betroffenen umfasst:

- Kunden
- Lieferanten
- Dienstleister
- Geschäftspartner
- Mitarbeiter
- Vertragspartner
- Ansprechpartner

§ 7 Weisung (Art. 28 Abs. 3 a))

(1.) Der Auftragnehmer darf Daten nur im Rahmen des Auftrags, d.h. im Rahmen der sich aus dem bestehenden Vertragsverhältnis und den erteilten Einzelaufträgen ergebenden Bestimmungen und Weisungen des Auftraggebers verarbeiten.

(2.) Der Auftraggeber ist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit und nach Beendigung dieser Vereinbarung Weisungen an den Auftragnehmer erteilen.

(3.) Jede Weisung des Auftraggebers bedarf der Schrift- oder Textform und muss nachvollziehbar dokumentiert werden. Es muss stets nachvollzogen werden können, wann von wem eine Weisung an den Auftragnehmer erteilt wurde. Der Auftragnehmer hat nur Weisungen in Schrift- oder Textform zu befolgen.

(4.) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

§ 8 Vertraulichkeit (Art. 28 Abs. 3 b))

(1.) Der Auftragnehmer gewährleistet und versichert, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2.) Der Auftragnehmer erbringt auf Anfrage den Nachweis über die Verpflichtung auf Vertraulichkeit.

§ 9 Technisch-organisatorische Maßnahmen des Auftragnehmers (Art. 28 Abs. 3 c))

(1.) Der Verantwortliche arbeitet nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2.) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat der Auftragnehmer geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3.) Bei der Beurteilung des angemessenen Schutzniveaus hat der Auftragnehmer die Risiken berücksichtigt, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(4.) Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(5.) Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragnehmer die in seinem Datenschutz- und Datensicherheitskonzept aufgeführten technisch-organisatorischen Maßnahmen getroffen. Das Datenschutz- und Datensicherheitskonzept des Auftragnehmers wird als verbindlich festgelegt. Die Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO ist in Anlage 1 aufgeführt.

§ 10 Einschaltung von weiteren Auftragsverarbeitern (Art. 28 Abs. 3 d))

(1) Der Auftraggeber erteilt hiermit sein ausdrückliches Einverständnis, dass der Auftragnehmer zur Begründung eines Unterauftragsverhältnisses nach Maßgabe der hier vereinbarten Regelung mit den in Anlage 2 genannten Unterauftragsverarbeitern berechtigt ist.

(2) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem weiteren Auftragsverarbeiter zu übertragen. Dies gilt insbesondere für die zwischen den Vertragspartnern festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

§ 11 Rechte der Betroffenen (Art. 28 Abs. 3 e))

(1.) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.

(2.) Der Auftragnehmer trifft insbesondere geeignete technische und organisatorische Maßnahmen, um dem Auftraggeber die Erfüllung seiner Pflichten gegenüber den Betroffenen zu ermöglichen.

§ 12 Unterstützung des Auftraggebers (Art. 28 Abs. 3 f))

(1.) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 DS-GVO genannten Pflichten zur Sicherheit der Verarbeitung personenbezogener Daten sowie zu etwa bestehenden Melde- und Benachrichtigungspflichten, durchzuführenden (DSFA) Datenschutz-Folgeabschätzungen und notwendigen vorherigen Konsultationen der Aufsichtsbehörde.

(2.) Der Auftragnehmer stellt ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicher, welche 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.

(3.) Der Auftragnehmer ist verpflichtet, eine Verletzung des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art. 33 DS-GVO und stellt ihm die etwa benötigten Informationen unverzüglich zur Verfügung.

(4.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen aus Art. 34 DS-GVO und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

(5.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa durchzuführender Datenschutz-Folgeabschätzungen gem. Art. 35 DS-GVO.

(6.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa notwendiger vorheriger Konsultationen der Aufsichtsbehörde.

§ 13 Abschluss der Erbringung der Verarbeitungsleistungen (Art. 28 Abs. 3 g))

(1.) Nach Beendigung des bestehenden Verhältnisses und des jeweiligen Einzelauftrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

(2.) Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

§ 14 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 h))

(1,) Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. Hierfür kann er insbesondere Selbstauskünfte des Auftragnehmers einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes persönlich überzeugen oder einen Dritten hiermit beauftragen.

(2.) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist insbesondere verpflichtet, die Umsetzung von angemessenen technischen und

organisatorischen Maßnahmen nachzuweisen. Der Nachweis über solche Maßnahmen, die nicht nur den konkreten Einzelauftrag betreffen, kann erfolgen durch:

a) die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-CVO;

§ 15 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, einschränken oder löschen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 16 Datenschutzbeauftragter und IT-Sicherheitsbeauftragter

(1.) Der Auftragnehmer ist gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet. Dieser Verpflichtung ist er nachgekommen. Der Datenschutzbeauftragte des Auftragnehmers übt seine Tätigkeit gem. Art. 38 und 39 DS-CVO aus. Die Kontaktdaten sind:

HUBER Datenschutz | Herr Herbert C. Huber | In den Wiesen 1 | D-77723 Gengenbach
Tel.: 0171/ 65 28 716 | E-Mail: Info@huberdatenschutz.de

(2.) Der Auftragnehmer hat einen IT-Sicherheitsbeauftragten bestellt. Die Kontaktdaten sind:

HUBER Datenschutz | Herr Herbert C. Huber | In den Wiesen 1 | D-77723 Gengenbach
Tel.: 0171/ 65 28 716 | E-Mail: Info@huberdatenschutz.de

§ 17 Dokumentationspflichten des Auftragnehmers

(1.) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag für den Auftraggeber durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a. den Namen und die Kontaktdaten des Auftragnehmers oder der Auftragnehmer und jedes Verantwortlichen, in dessen Auftrag der Auftragnehmer tätig ist, sowie gegebenenfalls des Vertreters des Auftraggebers oder des Auftragnehmers und eines etwaigen Datenschutzbeauftragten;

b. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO.

(2.) Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(3.) Der Auftraggeber oder der Auftragnehmer sowie gegebenenfalls der Vertreter des Auftraggebers oder des Auftragnehmers stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

§ 18 Informationspflichten, Schriftformklausel, Rechtswahl

(1.) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

(2.) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, mindestens in Textform, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3.) Es gilt deutsches Recht. Es gelten die Haftungsregeln gem. Art. 82 (DSGVO). Gerichtsstand ist der Sitz des Auftragnehmers.

(4.) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht

Lahr, den _____ **,den** _____

schrempp edv GmbH
(Auftragnehmer)

_____

Anlagen:

1. Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO der **schrempp edv GmbH**

2. Übersicht der Unterauftragnehmer

Anlage 1

Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO der schrempp edv GmbH

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

Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert.

1.1 Zutrittskontrolle

Der Auftragnehmer gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, auf der die personenbezogenen Daten verarbeitet oder genutzt werden, verwehrt wird. Dies geschieht durch:

- Alarmanlage zur Überwachung aller Eingangstüren
- Empfang besetzt während der Geschäftszeiten
- Sicherheitsschlösser
- Kameraüberwachung (Bewegungserkennung) der Eingangsbereiche während der Nicht-Bürozeiten
- Schlüsselregelung (Schlüsselausgabekonzept)
- Sorgfältige Auswahl des Reinigungspersonals
- Zutritt zum Gebäude und allen relevanten Räumen nur für Berechtigte, d.h. die jeweiligen Mitarbeiter, Besucher nur in Begleitung von berechtigten Mitarbeitern

1.2 Zugangskontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen, dass seine Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen. Dies geschieht durch:

- Zuordnung von Benutzerrechten
- Passwortvergabe, Passwortsicherheit u.a. Mindestlänge
- Einsatz von VPN-Verbindungen
- Verwendung fortlaufend aktualisierter Virenschutzsoftware
- Schutz des E-Mail-Verkehrs vor Viren und Spam
- Automatisierte Einspielung von Sicherheits-Patches
- Erstellen von Benutzerprofilen
- Authentifizierung mit Benutzername und Passwort
- Sperren bestimmter Ports
- Einsatz von Intrusion-Detection-Systeme
- Einsatz einer Hardwarefirewall

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

- Zugriff auf Systeme nur mit individuellen Benutzernamen und Kennwörtern
- Rollenbasiertes Berechtigungskonzept
- Anzahl Administratoren so gering wie möglich
- Rollenbasierte Administrationsrechte
- Sichere Aufbewahrung von Datenträgern (Datensicherungsfestplatten)
- Rechteverwaltung durch Administrator
- Einsatz von Aktenvernichtern/Dienstleister
- Ordnungsgemäße Vernichtung von Datenträgern

1.4 Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Getrennte Verarbeitung zweckgebundener Daten
- Die Daten unterschiedlicher Auftraggeber / Projekte werden soweit möglich auf unterschiedlichen Systemen verarbeitet
- Funktionstrennung von Produktiv- und Test- und Entwicklungsumgebung

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugeordnet werden.(Art. 4 Nr. 5 DS-GVO).

Prozesse, die mit personenbezogenen Daten arbeiten, sind bereits von Anfang an datenschutz-freundlich zu gestalten; die Pseudonymisierung kann hierfür ein wichtiger Bestandteil sein.
Maßnahmen zur Pseudonymisierung personenbezogener Daten:

a) Trennung von Kundenstammdaten und Kundenumsatzdaten
b) Verwendung von Personal-, Kunden-, Lieferanten-Kennziffern statt Namen

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

Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

2.1 Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Protokollierung von Stammdatenänderungen
- Vergabe von Änderungs-, Lösch- und Bearbeitungsrechten aufgrund eines Rollenberechtigungskonzeptes
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung der Serveraktivitäten
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer

2.2 Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Sichere Löschung von Datenträgern
- VPN-Tunnelverbindung bei externen Geräten
- Verbot der Nutzung privater Datenträger am Arbeitsplatz
- Sorgfältige Auswahl von Transportpersonal

2.3 Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

- Auftragnehmer hat Datenschutzbeauftragten benannt
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Kontrollrechte gegenüber dem Auftragnehmer
- Laufende Kontrolle des Auftragnehmers
- Schriftliche Weisungen an den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Vertragsende
- Verpflichtung der Mitarbeiter des Auftragnehmers auf den Datenschutz / Verschwiegenheitspflichten
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Eindeutige Vertragsgestaltung

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

Die Schutzziele Verfügbarkeit und Belastbarbarkeit werden durch die folgenden Maßnahmen sichergestellt:

3.1 Verfügbarkeitskontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen die unbeabsichtigte Zerstörung oder den Verlust personenbezogener Daten. Dies geschieht durch:

- Klimaanlage in Serverräumennicht unter sanitären Anlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherungen im anderem Brandabschnitt
- Virenschutz und Firewall-Konzepte
- Unterbrechungsfreie Stromversorgung (USV)
- geregeltes Backup Verfahren
- HA – System über mehrere Brandabschnitte
- Spiegelung von Festplatten (RAID) Systeme, VM System
- Regelmäßige Erstellung von Sicherheitskopien
- Erstellen eines Notfallplans
- geregeltes Backup- und Recoverykonzept
- Überspannungsfilter

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

Ein regelmäßiges Kontroll- und Evaluierungskonzept wird wie folgt umgesetzt:

- Regelmäßige Mitarbeiterschulungen- und Prüfungen
- Regelmäßiges Einspielen von Patches und Softwareupdates
- Jährliches Datenschutz-Audit
- Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recovery-Konzeptes im Serverbereich

Die schriftliche Dokumentation beinhaltet:

- Interne Verhaltensregeln
- Datensicherheitsbeschreibung
- Risikoanalyse
- Datensicherungs-Konzept

Verantwortlicher für die Erstellung, V1.0, 2022

H. C. Huber, Datenschutzbeauftragter

Anlage 2

Übersicht der Unterauftragnehmer

Unterauftragnehmer	Anschrift / Verarbeitungsort	Art der Dienstleistung
wetexx GmbH	Brambachstr. 12 77723 Gengenbach	Wartung und Servicemanagement
just-IT GmbH	Schwebelstr. 10 75172 Pforzheim	Support und Update-Service
Essential Bytes GmbH & Co. KG	Steinebühlstr. 30 D-77749 Hohberg	Wartung, Pflege und Service via Fernwartung
BALTICOM Software GmbH	Kampstr. 22 24601 Wankendorf	Support und Wartung