Vereinbarung
über die Verarbeitung personenbezogener Daten
(Auftragsverarbeitung)

zwischen

Name: .....
Straße: .....
PLZ Ort: .....

- nachstehend Auftraggeber genannt -

und

Name: **1st Vision GmbH**
Straße: Wieseneckstraße 26
PLZ Ort: 90571 Schwaig

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Diese Vereinbarung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht und insbesondere aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet (Anlage 1). Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen (im Einzelnen in Anlage 1 aufgeführt) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Als solche Tätigkeiten kommen insbesondere ein Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/ Backup-Datei – vor allem im Zusammenhang mit Supportanfragen – in Betracht, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden, in Anlage 1 aufgeführten Hauptvertrages.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt

oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeitung: Verarbeitung umfasst 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) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware und bietet im Rahmen seiner Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Ferner bietet er Softwarelösungen auch im Rahmen von Hosting, ASP, SaaS oder Cloud basierender Angebote an. Im Rahmen dieser Tätigkeiten kann in besonderen Konstellationen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des Hauptvertrages konkretisiert. Die Hauptverträge sind ferner in Anhang 1 zu dieser Vereinbarung, unter Nennung der jeweils betroffenen Datenkategorien, aufgeführt. Die Auflistung wird von den Parteien bei Wegfall oder Neuabschluss eines weiteren Hauptvertrages, der auch Auftragsverarbeitung zum Gegenstand hat, fortlaufend aktualisiert.

(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortliche Stelle ist, gegeben ist.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten ergeben. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des anwendbaren

Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet insbesondere

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Anlage 2 diesem Vertrag beigefügt.

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

(4) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der gesetzlichen Pflichten, die den Auftraggeber als Verantwortlichen treffen (u.a. bei der Wahrnehmung von Betroffenenrechten, der Durchführung von Kontrollen durch die zuständige Datenschutzaufsichtsbehörde sowie bei der Erfüllung gesetzlicher Informationspflichten gegenüber Betroffenen und Datenschutzbehörden). Der Auftraggeber erstattet dem Auftragnehmer durch die Unterstützung entstehende Kosten und Aufwand. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, in vollem Umfang erstattet.

(6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und auf Verlangen in geeigneter Weise nachzuweisen.

(8) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes bedarf der vorherigen Zustimmung des Auftraggebers.

§ 4 Pflichten und Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer verantwortlich (Verantwortlicher). Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftraggeber trägt hierdurch anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.

(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber, soweit diese angeblich unrechtmäßigen Verarbeitungen auf Vorsatz oder Fahrlässigkeit des Auftraggebers beruhen, den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten), erstattet der Auftraggeber dem Auftragnehmer Kosten und Aufwand. Die Parteien verständigen sich über den erwarteten Umfang von Kosten und Aufwand.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

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

(6) 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.

§ 5 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht und trägt bei zu Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

(3) Die Häufigkeit der Kontrollen soll, maximal einmal jährlich erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.

(4) Nach Wahl des Auftraggebers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort Kontrolle durch die Vorlage eines geeigneten Testats, von Berichten oder Berichtsauszügen des externen Datenschutzbeauftragten erbracht werden ("Zertifizierungsurkunde"). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß beiliegender Anlage 2 zu überzeugen.

Beim Auftragnehmer ist als fachkundiger externer Datenschutzbeauftragter benannt und bei der zuständigen Aufsichtsbehörde gemeldet:

Name:	B.i N BusinessCoaching+Consulting Jens Wiemeyer
Adresse:	Oberer Krankenhausweg 11, 91220 Schnaittach
Telefon:	+49 (0)9153 9700 575
E-Mail:	jens.wiemeyer@b-in.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Auf Anfrage des Auftraggebers ist der aktuelle Fachkundenachweis zur Verfügung zu stellen.

§ 6 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen die in der Anlage 3 benannten weiteren Auftragsverarbeiter (Subunternehmer) einschaltet. Über eine Änderung der in der Anlage 3 genannten Subunternehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Im Übrigen ist die Beauftragung von Subunternehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden. Im Fall der Einschaltung von im Sinne der §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmen als Subunternehmer erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung.

(3) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

§ 7 Informationspflichten

(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 als „verantwortlicher Stelle“ im Sinne des anwendbaren Datenschutzrechts liegen.

(2) Bei Störungen, Verdacht auf Verletzungen des Schutzes personenbezogener Daten oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Die Meldung an den Auftraggeber über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer trifft in diesem Fall unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen des Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

Meldungen an die Behörde bezüglich Datenschutzverletzungen/-verstöße, darf der Auftragnehmer nur nach vorheriger Weisung selbst durchführen.

(3) 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 Datenpannenn, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Unterstützung des Auftraggebers bei dessen technischen und organisatorischen Maßnahmen,
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
c) und 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.

§ 8 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des letztbestehenden Hauptvertrages.

(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder herauszugeben. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Datenschutzrechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. gesetzliche Aufbewahrungspflicht).

(3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

§ 9 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

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

(3) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist das Amtsgericht Hersbruck.

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

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 1
Umfang, Art und Zweck der Datenverarbeitung

I. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

Bei Verwendung der Software werden zwingend Daten der registrierten Benutzer verarbeitet. Hierzu gehören Namen und E-Mail-Adresse. Weitere Daten können optional angegeben werden.

Ferner werden neben diesen Registrierungsdaten auch Nutzungsdaten verarbeitet. Dazu gehört insbesondere, welcher User wann welche Daten eingegeben, verändert oder gelöscht hat.

Ansonsten ist es dem Auftraggeber überlassen, welche Datenarten er bei der Verwendung der Software verarbeitet. Hierauf hat der Auftragnehmer keinen unmittelbaren Einfluss

II. Kreis der Betroffenen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Mitarbeiter, ehemalige Mitarbeiter (Ruheständler)
- Auszubildende und Praktikanten
- Interessenten und Kunden
- Lieferanten
- Ausgeschiedene Mitarbeiter von Kunden und Lieferanten

Kategorien personenbezogener Daten:

- Name und Vorname
- Adresse
- Geburtsdatum
- Telefon- und Kontaktadressen (Email)
- Bankdaten und Kontonummern

III. Gegenstand und Zweck der Datenverarbeitung

Den Zweck bestimmt der Auftraggeber in seiner jeweiligen Beauftragung.

Anlage 2
Technische und organisatorische Maßnahmen

Um die von ihm verarbeiteten personenbezogenen Daten zu schützen, hat der Auftragnehmer angemessene technische und organisatorische Sicherheitsmaßnahmen, einschließlich der folgenden Maßnahmen umgesetzt:

1. Vertraulichkeit

Zutrittskontrolle

1st Vision gewährleistet folgende Maßnahmen, um unbefugten Personen den Zutritt zu den Büros und damit zu den Datenverarbeitungsanlagen von 1st Vision zu verwehren:

- Automatisches Zugangskontrollsystem über elektronische Zutrittskarten (Transponder-Schließsystem)
- Regelung zu geschlossenen Fenstern (1.OG)
- Manuelles Schließsystem mit Schüsselberechtigung nur für festgelegte Mitarbeiter
- Personenkontrolle / Besucherregelung über Empfangsmitarbeiter
- Schlüsselausgabe - Regelung für Bürozutritt und Keller
- Sorgfältige Auswahl von Serviceunternehmen zur Raumreinigung und Verpflichtung auf Geheimhaltung
- Trennung von (Haupt-)Gebäude und Büro durch zusätzliches Türsystem
- Verschließbare Schränke
- Videoüberwachung im (Haupt-)Gebäude-Eintrittsbereich und zur Überwachung der Parkplätze, eine (Haupt-)Gebäudeüberwachung mittels eines Sicherheitsdienstes mit Wachpersonal durch den Vermieter

Sofern der Kunde eine Hardware in seinem Rechenzentrum oder einem Rechenzentrum seiner Wahl einsetzt, ist die Zutrittskontrolle nicht von 1st Vision zu leisten, sondern wird durch den jeweiligen Dienstleister sichergestellt. 1st Vision sorgt für eine sorgfältige Auswahl des unterbeauftragten Dienstleisters (Subunternehmer).

Zugangskontrolle

1st Vision gewährleistet folgende Maßnahmen, um den Zugang zu Datenverarbeitungssystemen vor Unbefugten zu schützen und deren autorisierte Nutzung sicherzustellen:

- Benutzerrechte-Verwaltung und -Zuordnung
- Erstellung von Benutzerprofile, sowie eine einheitliche Regelung zur Erteilung, Entzug und Sperrung von Benutzerrechten
- Zuordnung der Benutzerprofile zu IT-Systemen
- Passwortvergabe nach Passwort-Richtlinie (→Mindestlänge, technische Erzwingung einer Komplexität)
- Authentifikation mit Benutzername und Passwort

- Einsatz von VPN-Technologien
- Einsatz von Antivirus-Software auf Clients und Server
- Einsatz von Firewall-Systemen
- Einsatz von Intrusion-Detection-Systemen (IDS)
- Einsatz von verschlüsselten, mobilen Datenträgern nach Bedarf
- Regelmäßige Überprüfung der Richtlinien und der Aktualität von Berechtigungen erfolgt mindestens einmal im Jahr

Zugriffskontrolle

1st Vision gewährleistet folgende Maßnahmen, damit Berechtigte ausschließlich auf die Daten zugreifen können, für die sie autorisiert sind und bei der Datenverarbeitung personenbezogene Daten nicht unbefugt erhoben, verarbeitet oder gelöscht werden können:

- Erstellen eines Berechtigungskonzepts
- Im Falle des Remote-Zugriffs erfolgt eine Aufschaltung auf einen bereits angemeldeten Bildschirm durch den Mitarbeiter des Auftraggebers
- Verwaltung der Rechte durch Systemadministrator, wobei die Anzahl der Administratoren auf das Notwendigste reduziert sind
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten in der Software
- Einschränkungen des Zugriffs auf Protokolle
- Sichere Aufbewahrung von Datenträgern in verschließbaren Schränken
- Physische Lösung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. entsprechend zertifizierten Dienstleistern
- Protokollierung der Vernichtung

Trennung

1st Vision gewährleistet folgende Maßnahmen, um die zu unterschiedlichen Zwecken erhobenen Daten getrennt voneinander zu verarbeiten:

- Erstellung eines Berechtigungskonzeptes
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Versehen der Datensätze mit Zweckattributen / Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Pseudonymisierung & Verschlüsselung

Kommt eine Pseudonymisierung oder Verschlüsselung von Daten zum Einsatz?

=> Nein

2. Integrität

Eingabekontrolle

1st Vision gewährleistet im Rahmen der Systemfunktionen im Standard der Hersteller Sage GmbH und CAS Software AG die nachträgliche Überprüfung und Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme erhoben, verarbeitet oder gelöscht wurden.

Weitergabekontrolle

1st Vision gewährleistet folgende Maßnahmen zur Sicherstellung einer befugten elektronischen Übertragung und Übermittlung von personenbezogene Daten:

- Einrichtungen von Standleitungen bzw. VPN-Tunnel-Technik
- Email-Verschlüsselung
- Physische Lösung von Datenträgern und ordnungsgemäße Vernichtung von Datenträgern nach DIN 32757 über die http://www.rowe-recycling.de/leistungen/akten-und-datentraegervernichtung.html

3. Verfügbarkeit und Belastbarkeit

1st Vision gewährleistet folgende Maßnahmen, damit die Datenverarbeitung von personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Auswahl der Hardware und Software auf Grund der Mindestempfehlung der Hersteller nach Stand der Technik und der vorhandenen Praxiserfahrungen
- Erstellung eines Backup- & Recovery-Konzeptes und Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Festplatten-Spiegelung (RAID 1 / RAID 5)
- Feuer- und Rauchmeldeanlagen
- Klimaanlage in Serverräumen
- Notfallplan zur Wiederherstellung
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen / über der Wassergrenze im 1.OG
- Testen von Datenwiederherstellung
- Unterbrechungsfreie Stromversorgung (USV)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1st Vision gewährleistet folgende Maßnahmen zu organisatorischen Sicherstellung im Umgang mit personenbezogenen Daten im Unternehmen:

- Datenschutzmanagement bestehend aus:
    - Richtlinie zum Datenschutz (für Beschäftigte)
    - IT-Richtlinie für Nutzer
    - Richtlinie für Speicherorte
    - Notfallplan
- Mindestens einmal jährlich erfolgt eine Schulung zum Datenschutz
- Überwachung und Beratung durch einen bestellten Datenschutzbeauftragten
- Verpflichtung zum vertraulichen Umgang mit personenbezogenen Daten bei der Arbeitsaufnahme für alle Mitarbeiter

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

Schutzziel: *Es muss sichergestellt werden, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen des Betroffenen, personenbezogene Daten unkontrolliert an Dritte zugänglich gemacht werden (Beispiel: App).*

Umsetzung bei Dienstleister:

- Die im Einsatz befindlichen Werkzeuge werden im Hinblick der Konfiguration auf den Benutzer und das Einsatzszenarium beschränkt und damit sichergestellt, dass der Zugang und der Umfang auf das erforderliche Maß hin ausgelegt sind.

6. Auftragskontrolle

Schutzziel: *Personenbezogene Daten, die im Auftrag verarbeitet werden, werden nur entsprechend den Weisungen des Auftraggebers verarbeitet.*

Beispiele: *Eindeutige Vertragsgestaltung, Weisungsmäßige Auftragsdatenverarbeitung, Kriterien der Auswahl des Auftragnehmers, Sichere Fernwartung.*

Umsetzung bei Dienstleister:

- Im Falle des Remote-Zugriffs erfolgt eine Aufschaltung auf einen bereits angemeldeten Bildschirm durch den Mitarbeiter des Auftraggebers. Dieser hat jederzeit eine wirksame Kontrolle der Fernwartungsarbeiten, durch Einsatz einer speziellen Software, die es dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor zu verfolgen, zu kontrollieren und jederzeit zu intervenieren.

Anlage 3
Weitere Auftragsverarbeiter

Gemäß § 6.1 stimmt der Auftraggeber mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer weitere Auftragsverarbeiter im Rahmen der Datenverarbeitungstätigkeiten einsetzt. Die Unternehmen entsprechen der Deklarierung in der jeweiligen zugrunde liegenden Beauftragung.

Die Hauptsubunternemer sind wie folgend:

Weiterer Auftragsverarbeiter (Hauptsubunternehmer)	**Der weitere Auftragsverarbeiter unterstützt in folgenden Datenverarbeitungstätigkeiten**
Sage GmbH Franklinstraße 61 - 63 60486 Frankfurt/Main 069/50007-0; info@sage.de Geschäftsführer: Rainer Downar und Heino Erdmann	3rd Level Support für das in Anlage 1 Abs. III für das von der Sage GmbH gelieferte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.
CAS Software AG CAS-Weg 1-5 76131 Karlsruhe 0721 9638-0 Vorstandsvorsitzender: Martin Hubschneider	3rd Level Support für das in Anlage 1 Abs. III für das von der CAS Software AG gelieferte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.
<u>Hosting:</u> **Timme Hosting GmbH & Co. KG** Ovelgönner Weg 43, 21335 Lüneburg **bisping & bisping GmbH & Co.KG** Oskar-Sembach-Ring 10, 91207 Lauf **Hetzner Online GmbH** Industriestr. 25, 91710 Gunzenhausen **ODN GmbH** Hermann-Glockner-Straße 7, 90763 Fürth **1 & 1 Internet AG** Elgendorfer Str. 57, 56410 Montabaur **mw online service UG** (Haftungsbeschränkt) Bauhofstr. 4, 90571 Schwaig	3rd Level Support für das in Anlage 1 Abs. III gelieferte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Kenn Dienstleistungen Leinpfad 60 71642 Ludwigsburg 07141 9136711; info@kdl-hr.de Geschäftsführer: Ronald Kenn	3rd Level Support für das in Anlage 1 Abs. III für das von Kenn Dienstleistungen gelieferte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.