Vertrag über die Auftragsverarbeitung personenbezogener Daten

(Stand 3/2021)

zwischen	und
_____	**vfm Konzept GmbH**
_____	Schmiedpeunt 1, 91257 Pegnitz
vertreten durch	*vertreten durch*
_____	Geschäftsführer Robert Schmidt
im Folgenden: **Auftraggeber** (Verantwortlicher)	im Folgenden: **Auftragnehmer** (Auftragsverarbeiter)

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet gegebenenfalls personenbezogenen Daten im Auftrag des Auftraggebers im Rahmen folgender Tätigkeiten, die sich aus der Leistungsbeschreibung des **Vertrages über die Bereitstellung der Software „Keasy“ – SaaS-Vertrag** (Hauptvertrag) und ihm Rahmen der Nutzung der Anwendungen und bereitgestellter Dienste des Auftragnehmers ergeben:

- **Softwarepflege**

  Erarbeitung von Lösungen bei auftretenden Softwarefehlern in der Anwendersoftware. Als Softwarefehler werden dabei Störungen im Programmablauf verstanden, die geeignet sind, den Einsatz der Software im Betrieb des Auftraggebers mehr als nur unerheblich zu beeinträchtigen. Meldet der Auftraggeber einen entsprechenden Fehler, wird der

Auftragnehmer diesen Fehler im Rahmen der ihr zur Verfügung stehenden Mittel und Ressourcen schnellst möglich beheben. Im Rahmen der Fehlerbehebung kann es ggf. zur Verarbeitung personenbezogener Daten durch den Auftragnehmer kommen.

- **Support per Online-Support-Portal und telefonischer Support**

  Der Auftragnehmer stellt dem Auftraggeber unter einer bekannt gegebenen Web-Adresse ein Online Support-Portal zur Verfügung. Hier werden Dokumentationen zur Verfügung gestellt und Fragen beantwortet. Ebenso hat der Auftraggeber die Möglichkeit telefonischen Support bei Fragen zu den Vertrags-Produkten, zur Produkt-Dokumentation sowie zu Programmablauf und Anwendung der Vertrags-Produkte in Anspruch zu nehmen. Bei Fragen zu einem konkreten Vorgang kann es zur Verarbeitung von personenbezogenen Daten kommen.

- **Fernwartung**

  Der Auftragnehmer kann zudem eine Supportleistung per Fernwartung durchführen. Die Supportleistung Fernwartung beinhaltet das Prüfen der Daten mittels Zugriff auf die EDV-Anlage des Auftraggebers mit einem Fernzugang. Die Bereitstellung des Anschlusses und der notwendigen Kommunikationsgeräte und -einrichtungen für den Fernwartungszugang erfolgt durch den Auftraggeber und der Auftraggeber hat alle technischen und organisatorischen Maßnahmen selbst zu treffen, die erforderlich sind, Datenschutz und Datensicherheit zu gewährleisten. Unter Verwendung eines Fernzugriffs wird die Prüfung von Datenbeständen, Protokollen und Funktionsabläufen vorgenommen. Der Auftragnehmer und der Auftraggeber stimmen den Zeitpunkt des Fernzugriffs ab. Der Auftraggeber muss dabei dem Auftragnehmer den Zugriff zu seinem System durch Aktivieren des Remotezugangs ermöglichen. Der Fernzugriff wird im Rahmen einer einzelnen Sitzung nur mit Einverständnis und unter Aufsicht des Auftraggebers erfolgen. Der Vorgang kann durch den Auftraggeber oder den Auftragnehmer jederzeit abgebrochen werden; ebenso kann der Auftraggeber kontrollieren, welche Arbeiten im Rahmen des Fernzugangs durchgeführt werden, insbesondere welche Zugriffe auf personenbezogene oder sonstige Daten erfolgen. Im Rahmen der Fernwartung kann es zur Verarbeitung personenbezogener Daten kommen.

- **Keasy App**

  Der Auftragnehmer stellt dem Auftraggeber auf Wunsch die Keasy App zu Verfügung. Der Auftraggeber hat hierbei die Möglichkeit, Kundendaten, Vertragsdaten, Vorgangsdaten, Dokumente und Nachrichten an den Endkunden in die vom Auftragnehmer bereitgestellte keasy cloud hochzuladen. Der Endkunde des Auftraggebers hat damit die Möglichkeit mittels der App auf die in der cloud gespeicherten Daten zuzugreifen und sich anzeigen zu lassen. Weiterhin kann der Endkunde mittels der App Kontakt per E-Mail oder Telefon zum Auftraggeber aufzunehmen oder einen Schaden zu melden. Bei der Nutzung dieses Service werden sämtliche Daten, in vom Auftragnehmer verarbeitet und gespeichert. Die Verarbeitung und Speicherung erfolgt in Rechenzentren der Fa. Microsoft, welche in diesem Zusammenhang wiederum als Auftragsverarbeiter des Auftragnehmers (Unterauftragnehmer) tätig wird.

- **Zeitsprung-Portal**

  Der Auftragnehmer stellt dem Auftraggeber auf Wunsch ein IT-Dienstleistungsportal zur Verarbeitung von Kunden- und Vertrags- und Dokumentendaten (zeitsprung-Portal) zur Verfügung.

  In dem genannten Portal werden die Maklerportale der Gesellschaften im Namen und Zugang des Maklers technisch aufgerufen und dort enthaltene Daten heruntergeladen/ gespeichert.

Die abgerufenen Inhalte richten sich jeweils nach der vom Makler hinterlegten Konfiguration. Die Daten werden solange gespeichert, bis der Makler diese über die Keasy-Schnittstelle abruft oder im zeitsprung-Desktop aktiv löscht.

Die Einzelheiten regelt der zwischen den Parteien ggf. bestehende **Vertrag zum Dokumentenabruf per BiPRO 430.**

(2) Die vertraglich vereinbarten Dienstleistungen werden ausschließlich in einem Mitgliedstaat der EU oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standartdatenschutzklauseln, genehmigte Verhaltensregeln.)

(3) Die Dauer dieses Vertrages (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

3. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

(1) Art und Zweck der Verarbeitung von Daten

Die Verarbeitung personenbezogener Daten durch den Auftragnehmer umfasst 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 zu den unter Ziffer 2 und dem Hauptvertrag aufgeführten Zwecken der Leistungserbringung (Softwarepflege, Support, Fernwartung, Keasy App).

(2) Art der personenbezogenen Daten

- Stammdaten des Auftraggebers
- Personenstammdaten der Anwender/Nutzer der Dienstleistungen
- Personenstammdaten der Endkunden des Auftraggebers (Name, Geburtsdatum, Adress- und Kontaktdaten, Familienstand, Beruf)
- Kundenentwicklung (Kundenhistorie)
- Kommunikationsdaten
- Bankdaten
- Terminverwaltungsdaten
- Betreuungsinformationen
- Abrechnungsdaten
- Vertragsdaten
- Schadensdaten
- Leistungsdaten
- Gesundheitsdaten
- Risikodaten
- Bonitätsdaten
- Terminverwaltungsdaten

(3) Kategorien betroffener Personen

- Kunden
- Versicherungsnehmer

- Angehörige von Kunden und Versicherungsnehmern
- Interessenten
- Mitarbeiter des Auftraggebers
- Handelsvertreter des Auftraggebers
- Mitarbeiter von Versicherungen, Finanzdienstleistern, Banken, Bausparkassen, gesetzlichen Krankenkassen und sonstigen Dienstleistern
- Lieferanten

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(5) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(6) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(7) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten lauten:
Harald Oberst, vfm Konzept GmbH, datenschutzbeauftragter@vfm-gruppe.de, 09241 4844-44

Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

5. Technische und organisatorische Maßnahmen

(1) Die im **Anhang 1** beschriebenen Datensicherheitsmaßnahmen (technisch organisatorische Maßnahmen gem. Art. 28 Abs. 3 Buchst. c, 32 DSGVO) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen

hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer die in **Anlage 2** gelisteten Dienstleister als Unterauftragnehmer beauftragt. Der Auftragnehmer trägt dafür Sorge, dass die zwischen den Parteien getroffenen Vereinbarungen auch gegenüber dem Unterauftragnehmer gelten.

(2) Die Beauftragung von Unterauftragnehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, nur zulässig, soweit und solange der Unterauftragnehmer angemessene Datenschutzgarantien bietet.

(3) Zurzeit sind die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(4) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte von Betroffenen nach Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solchen Anfragen, sofern sie ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen in der Regel schriftlich oder in einem elektronisch dokumentierten Format. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die

gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

9. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Eine solche Weisung bedarf der Textform.

(2) Weisungsberechtigt ist die Geschäftsleitung des Auftraggebers sowie von diesem in Textform bekanntgegebene Ansprechpartner.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

11. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13. Sonderkündigungsrecht

Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellen einen schweren Verstoß dar.

14. Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

	Pegnitz, 01.03.2021
Ort, Datum	Ort, Datum
	
Auftraggeber	Auftragnehmer

Anlage 1 Vertrag über die Auftragsverarbeitung personenbezogener Daten

Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Vertraulichkeit

a) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Durch die Mitarbeiter am Empfang erfolgt die Zutrittskontrolle für das gesamte Verwaltungsgebäude. Für die einzelnen Räumlichkeiten wird der Zutritt zu den dort sitzenden Mitarbeitern kontrolliert.
- Unbefugte können grundsätzlich nur in Begleitung eines Mitarbeiters die Räumlichkeiten betreten und sich dort aufhalten, wenn ein entsprechender Anlass gegeben ist.
- Es existieren sowohl Sicherheitsschlösser wie auch eine Schlüsselregelung.
- Server sind in abgeschlossenen Räumen oder Schränken untergebracht. Der Zutritt zu Serverräumen und Schränken ist nur der Geschäftsleitung und den Mitarbeitern der IT-Abteilung gestattet.
- Datensicherungen auf portable Sicherungsmedien (z.B. CD/DVD, Bänder) sind in zutrittsgeschützten Räumen untergebracht und werden in einem feuerfesten Tresor verwahrt.

b) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Der Zugang zu Datenverarbeitungssystemen ist durch Benutzername und Passwort geschützt.
- Es existieren betriebliche Passwortregeln. In diesem Zusammenhang wird eine bestimmte Passwortlänge- und Komplexität gefordert.
- Entfallen Zugangsberechtigungen, so werden diese umgehend entzogen.
- Es existieren betriebliche Sicherheitsrichtlinien. Danach ist der Arbeitsplatzrechner vor Verlassen zu sperren. Eine automatische Sperrung nach einer bestimmten Zeitdauer erfolgt automatisch.
- Es werden Logs der Benutzeranmeldungen erstellt und Schreibprotokollierungen bei Datenzugriffen durchgeführt.
- Arbeitsplatzrechner werden durch Anti-Viren-Software geschützt.
- Das Reinigungspersonal wird auf den Datenschutz und Vertraulichkeit verpflichtet.

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.

- Es sind ausschließlich Personen, mit der Datenverarbeitung im Rahmen der vereinbarten Auftragsverarbeitung betraut, die berechtigt sind, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen. In diesem Zusammenhang bestehen Regelungen zur Vergabe von Zugriffsberechtigungen.
- Papierunterlagen können beim Verlassen des Arbeitsplatzes in Schränken weggeschlossen werden.
- Als Schutz gegen den unberechtigten Zugriff Dritter aus dem Internet ist eine Firewall installiert.
- Die technischen Sicherheitseinrichtungen werden regelmäßig überprüft.

d) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Personenbezogene Daten verschiedener Auftraggeber werden getrennt voneinander verarbeitet.

2. Integrität

a) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder 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.

- Die Verwendung von externen Datenträgern außerhalb der geschützten Unternehmensumgebung ist grundsätzlich untersagt.
- Die datenschutzgerechte Datenvernichtung ist gewährleistet.
- Elektronischer Datenaustausch im Unternehmen erfolgt über gesicherte Leitungen: isolierte Glasfaserleitungen zwischen den Standorten in Pegnitz, im Übrigen existieren VPN-verschlüsselte Leitungen.
- Der Mailversand an Dritte erfolgt in verschlüsselter Form: soweit der empfangende Server eine Verschlüsselung unterstützt, erfolgt dies automatisch, nicht obligatorisch;
- Es besteht eine Verpflichtung der Mitarbeiter auf das Datengeheimnis und zur Verschwiegenheit durch eine Erklärung, die zu den Personalakten genommen wird;

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Zur nachträglichen Überprüfung der Datenzugriffe erfolgt eine Schreibprotokollierung.
- Administrationstätigkeiten werden ebenfalls protokolliert.

3. Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Maßnahmen zur Vermeidung von Datenverlusten durch den Einsatz von Microsoft Data Protection Manager zu anwendungsspezifischen Sicherungen, Dateisicherung, Systemsicherung, mehrstufige tägliche Datensicherung (kurz-, mittel-, langfristig – mindestens 15 Minuten-Intervalle).
- Regelmäßige Unterweisung der Mitarbeiter in die einzuhaltenden Sicherheitsmaßnahmen im Umgang mit Daten über die Kommunikation der im Mitarbeiterhandbuch niedergelegten verbindlichen IT-Sicherheitsrichtlinien sowie wie über eine jährliche Schulung zu Datenschutzthemen;
- Schriftliche Erklärung der Mitarbeiter über die Aufklärung zu den einzuhaltenden Sicherheitsmaßnahmen (Mitarbeiter erklären dies im Rahmen der „Erklärung Mitarbeiterhandbuch“, dessen Bestandteil die IT-Sicherheitsrichtlinien sind);
- Überprüfung von Datenträgern auf Viren durch ESET-Virenschutz;
- Sicherheitskopien mittelfristig auf Festplatten im zugangsgesicherten Serverraum und langfristig Datensicherung auf Band (Lagerung im Tresor, siehe oben);
- Speicher-, Zugriffs- und Leistungskapazitäten werden durch Vorhalten der entsprechenden Hardware gewährleistet und einer ständigen Überprüfung durch die IT unterzogen;
- Eine vorbeugende Sicherung über DELL Pro Plus Vertrag: Infrastruktur-Fehlermeldungen erfolgen bereits im Vorfeld vor Eintritts eines möglichen Zwischenfalles (Frühwarnsystem).

b) Unverzügliche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall unverzüglich wiederhergestellt werden können.

- Es erfolgt ein regelmäßiges Back-Up der Daten (Intervall 15 Min.) sowie eine redundante Datenspeicherung.
- Es werden Cloud Services (betreffend Nutzung Skype, Share Point, MS Teams).
- Es wird ständig eine doppelte IT-Infrastruktur vorgehalten.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

- Es existieren IT-Sicherheitsrichtlinien, die regelmäßig überprüft werden und die an sich ändernde Bedingungen angepasst werden.

b) Incident Response-Management

- Es gibt eine Prozessbeschreibung zur Behandlung von Datenpannen.
- Die Mitarbeiter sind über den Ablauf der Behandlung von Datenpannen informiert.

c) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Aus der Leistungsbeschreibung, die als Grundlage der Auftragsverarbeitung zwischen Auftragnehmer und Auftraggeber vereinbart wurde, gehen Art, Umfang und Zweck der Datenverarbeitung klar hervor.
- Die mit der Umsetzung der Auftragsverarbeitung befassten Mitarbeiter sind über den Leistungsumfang informiert.
- Für die vereinbarte Auftragsverarbeitung werden ggf. Cloud-Lösungen eingesetzt. Die genutzten Rechenzentren befinden sich in der EU. Die Cloud-Datenkommunikation ist verschlüsselt.
- Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt.

Anlage 2 zum Vertrag über die Auftragsverarbeitung personenbezogener Daten

Unterauftragsnehmer i.S.d. Vertrages zur Auftragsverarbeitung

1. **SysEleven GmbH**
   Boxhagener Straße 80, 10245 Berlin
   - Hosting / Betrieb Rechenzentrum

2. **Soft-Trade GmbH**
   Arneburger Straße 24, 39576 Stendal
   - Vertriebspartner und externer Dienstleister für Support/Softwarepflege

3. **Sunrise IT-Services, Inh. Frank Wernicke**
   Uhlandstraße 29, 63225 Langen
   - Externer Dienstleister für Support/Softwarepflege

4. **zeitsprung GmbH & Co. KG**
   Göppinger Str. 1, 75179 Pforzheim
   - externer Dienstleister Dokumentendownload

5. **Microsoft Ireland Corporations Ltd.**
   Carmenhall Road, Sandyford, Dublin 18, Ireland
   - Betrieb Rechenzentrum