Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (EU-DSGVO)

zwischen dem

Kunden:

Kundennummer	.....
Firma	.....
Firmenzusatz	.....
Straße / Nr.	.....
Land / PLZ / Ort	.....

.....

- als **Verantwortlicher** - (nachstehend *Auftraggeber* genannt)

und der

4Mis GmbH
Abt. Personal-Planer.de
vertreten durch den Geschäftsführer Herr Mark Stiller
An der Burgmühle 2
53881 Euskirchen
Deutschland

.....

- als **Auftragsverarbeiter** - (nachstehend *Auftragnehmer* genannt)

Präambel

Dieser Auftragsverarbeitungs-Vertrag (kurz: „*AV-Vertrag*“ genannt) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Hauptvertrag (Angebot, Preis- & Leistungsverzeichnis (PLV), AGB) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertragsverhältnis in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogene Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer (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 über das Kundencenter (KC) https://kc.personal-planer.de des Auftragnehmers in elektronischer Form erfolgen.

(4) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(5) Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers (Art. 4 Abs. 2 EU-DSGVO).

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

§2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand des Vertrages ist die Bereitstellung einer webbasierten Personalverwaltungs-Dienstleistung, sowie der damit im Zusammenhang stehenden Leistungen wie z.B. Zeiterfassungsterminals und Zutrittssysteme. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach gebuchten Modul und vereinbartem Leistungsumfang – unter Nutzung der Dienstleistung u.a. die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

(2) Die Einzelheiten ergeben sich aus dem Hauptvertrag / den Hauptverträgen, die unter der o.g. Kundennummer zusammengefasst sind. Die Vereinbarung zur Auftragsverarbeitung findet Anwendung auf das gesamte Dienstleistungsverhältnis.

(3) Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der EU-DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung i.S.d. Art. 28 Abs. 1 EU-DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(4) In **Ergänzung** zu dem/den zwischen den Parteien geschlossenen Vertrag/Verträgen konkretisieren die Vertragsparteien mit vorliegendem Auftragsverarbeitungsvertrag die gegenseitigen Pflichten im generellen Umgang mit den Daten des Auftraggebers.

§3 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten

(1) Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.

(2) Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

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

(4) Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

(5) Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 EU-DSGVO erfüllt sind.

(6) Sofern eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erfolgt, stellt der Auftragnehmer sicher, dass die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind. Hierzu werden insbesondere geeignete Garantien gemäß Art. 46 EU-DSGVO vereinbart, insbesondere durch den Abschluss der jeweils gültigen EU-Standardvertragsklauseln. Soweit erforderlich führt der Auftragnehmer eine Bewertung der Drittlandübermittlung (Transfer Impact Assessment) durch und dokumentiert die Ergebnisse.

(7) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zweckgebunden und nur in dem Umfang, der zur Erfüllung der vertraglich vereinbarten Leistungen erforderlich ist. Eine darüberhinausgehende Verarbeitung erfolgt nicht, sofern keine gesetzliche Verpflichtung hierzu besteht oder eine ausdrückliche Weisung des Auftraggebers vorliegt.

(8) Der Auftragnehmer bestätigt dem Auftraggeber auf Verlangen die Durchführung der Löschung oder Rückgabe personenbezogener Daten schriftlich oder in Textform.

KI-gestützte Verarbeitungssysteme

(9) Der Auftragnehmer ist berechtigt, im Rahmen der vertraglich vereinbarten Leistungen KI-gestützte oder algorithmische Verfahren zur Analyse, Strukturierung, Optimierung und Unterstützung der Datenverarbeitung einzusetzen. Dies umfasst insbesondere Verfahren zur automatisierten Personal-Einsatzplanung sowie KI-gestützte Assistenzfunktionen zur Beantwortung systembezogener Anwenderfragen. Eine darüberhinausgehende eigenständige Zweckänderung der Datenverarbeitung erfolgt nicht.

(10) Eine Verwendung personenbezogener Daten des Auftraggebers zur allgemeinen Modellverbesserung, zum Training globaler KI-Modelle oder zur Weiterentwicklung produktübergreifender Systeme erfolgt ausschließlich in anonymisierter Form im Sinne des Erwägungsgrundes 26 EU-DSGVO, sodass ein Personenbezug nicht mehr herstellbar ist. Eine Verarbeitung zu Trainingszwecken mit personenbezogenen Echtdaten erfolgt nur auf Grundlage einer gesonderten vertraglichen Vereinbarung oder ausdrücklichen Weisung des Auftraggebers.

(11) Der Auftragnehmer kann im Rahmen der vertraglich vereinbarten Leistungen ein KI-gestütztes Assistenzsystem einsetzen, welches Supportanfragen analysiert und automatisierte Handlungsempfehlungen oder Antwortvorschläge generiert. Das System greift ausschließlich auf die Daten des jeweiligen Auftraggebers innerhalb dessen Systemumgebung zu. Eine mandantenübergreifende Zusammenführung personenbezogener Daten findet nicht statt.

(12) Personenbezogene Daten aus Supportanfragen, Formularen oder sonstigen Kommunikationsvorgängen werden nicht zur allgemeinen oder mandantenübergreifenden Modellverbesserung verwendet. Eine Nutzung zu Trainingszwecken erfolgt ausschließlich

- entweder in anonymisierter Form im Sinne des Erwägungsgrundes 26 EU-DSGVO, sodass ein Personenbezug nicht mehr herstellbar ist.
- oder auf Grundlage einer gesonderten vertraglichen Vereinbarung mit dem Auftraggeber.

Eine dauerhafte Speicherung personenbezogener Echtdaten in Trainingsmodellen erfolgt nicht.

(13) Der Auftragnehmer kann im Rahmen der vertraglich vereinbarten Leistungen algorithmische oder KI-gestützte Verfahren zur Erstellung von Einsatz- oder Dienstplanvorschlägen einsetzen. Die Systeme berücksichtigen dabei ausschließlich die durch den Auftraggeber bereitgestellten Parameter (z.B. Qualifikationen, Arbeitszeiten, Verfügbarkeiten, Ruhezeiten, Abwesendheiten usw.). Die generierten Planungen stellen Entscheidungsvorschläge dar. Die verbindliche Freigabe und Verantwortung für die finale Planung verbleibt beim Auftraggeber.

(14) Es erfolgen keine ausschließlich automatisierten Entscheidungen im Sinne des Art. 22 EU-DSGVO mit rechtlicher Wirkung gegenüber betroffenen Personen, sofern der Auftraggeber keine ausdrückliche gegenteilige Weisung erteilt. Eine menschliche Überprüfung der KI-generierten Planung ist vorgesehen.

(15) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass KI-gestützte Planungsmechanismen keine systematischen Benachteiligungen oder Diskriminierungen einzelner Personengruppen verursachen. Die Entscheidungslogik basiert ausschließlich auf arbeitsorganisatorischen Parametern und nicht auf personenbezogenen Merkmalen, die nicht für die Planung erforderlich sind.

§4 Art der Daten und Kreis der Betroffenen (Art. 28 Abs. 3 S. 1 EU-DSGVO)

(1) Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers sind folgende:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, insbesondere Adressdaten, Angebotsdaten, Authentifizierungsdaten, Bankverbindungsdaten, Bestelldaten, Mitarbeiterdaten, Nutzungsdaten, Stammdaten, Vertragsdaten, Kontaktdaten, wie Telefon-	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten	Kunden und Ansprechpartner (u.a. Mitarbeiter oder andere bevollmächtige Personen des Kunden)

, Fax- und E-Mail-Daten, Kontakthistorie sowie weitere Daten die zur Vertragserfüllung notwendig sind. Abrechnungsdaten (z.B. Bankverbindung), Daten zu Internet-Dienstleistungen, und die gesamte Fax-, Brief-, E-Mail- und Telefon-Korrespondenz.		
Verarbeitet werden Vertragsdaten und Leistungsdaten soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Beispiele: Vertrags- und Abrechnungsdaten, Daten zur Personalverwaltung und -steuerung; Arbeitszeiterfassungsdaten sowie Zutrittskontrolldaten; Terminverwaltungsdaten; Daten im Rahmen der Unternehmenskommunikation und IT-Systemnutzung und der hierbei gesetzlich erforderlichen Protokollierung, sowie Videoüberwachungsdaten der Arbeitsplätze und die gesamte Fax-, E-Mail-, Brief- und Telefon-Korrespondenz.	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten	Arbeitnehmer, Auszubildende, Rehabilitanden, Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind, Bewerber, Ausgeschiedene und Praktikanten.
Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, insbesondere Adressdaten, Kontaktdaten wie Telefon-, Fax- und E-Mail-Daten, Kontakthistorie sowie weitere Daten die zur geplanten Vertragsausführung notwendig sind und die gesamte Fax-, Brief-, E-Mail- und Telefon-Korrespondenz	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten	Interessentendaten
Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Lieferhistorie, (Lieferanten / Dienstleister / Vermittler / Makler / Agenturen / Vermieter) insbesondere Kontaktdaten, wie Telefon-, Fax- und E-Mail-Daten, Kontakt- und Auftragshistorie sowie weitere Daten die zur Vertragserfüllung notwendig sind.	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten	Lieferantendaten
Personenstammdaten, insbesondere Adressdaten und Kontaktdaten, wie Telefon- und E-Mail-Daten, Zutritts- und Besuchshistorie sowie Videoüberwachungsdaten	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbrei-	Besucherdaten

	tung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten	

(2) Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrages. Der AV-Vertrag endet automatisch spätestens einen Monat nach Beendigung der Vertragsbeziehung, ohne dass es einer gesonderten Kündigung bedarf, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht darüberhinausgehende Verpflichtungen ergeben. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

(4) Wird dieser Auftragsverarbeitungsvertrag (AV-Vertrag) unabhängig vom Hauptvertrag beendet oder verliert er aus sonstigen Gründen seine Wirksamkeit, ist der Auftragnehmer ab dem Zeitpunkt des Wirksamwerdens der Beendigung nicht mehr berechtigt, personenbezogene Daten des Auftraggebers zu verarbeiten.

Ab diesem Zeitpunkt erfolgt eine unverzügliche vollständige Sperrung des Zugriffs auf das System sowie eine Verarbeitungssperre sämtlicher personenbezogener Daten.

Der Auftragnehmer wird dem Auftraggeber für einen Zeitraum von maximal 30 Kalendertagen nach Wirksamwerden der Beendigung die Möglichkeit einräumen, die gespeicherten Daten im Wege eines Datenexports abzurufen, sofern und soweit dies datenschutzrechtlich zulässig ist.

Erfolgt innerhalb dieses Zeitraums kein Abschluss eines neuen wirksamen Auftragsverarbeitungsvertrages oder keine schriftliche Weisung zur Datenherausgabe, werden sämtliche gespeicherten personenbezogenen Daten einschließlich etwaiger Sicherungskopien datenschutzgerecht gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass ohne wirksamen Auftragsverarbeitungsvertrag eine weitere Bereitstellung oder Verarbeitung personenbezogener Daten rechtlich unzulässig ist.

§5 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst, abhängig vom gebuchten Produkt, Hosting-Leistungen für das Personal-Management-System „Personal-Planer.de“, Vermietung und Verkauf und Vermietung von Hardware zur Zeiterfassung und Zutrittskontrolle, Bereitstellung von Storagespeicher für die Dokumentenverwaltung, Erstellung, Speicherung und Versand von E-Mails, sowie Dienstleistungen, die in einem individuellen Vertrag festgehalten werden.

(2) Zu einem Datenträgeraustausch gemäß Art. 28 Abs. 3 lit. g EU-DSGVO zwischen den Beteiligten dieser Auftragsverarbeitung kommt es nicht. Insoweit ist eine Rückgabe nicht zu regeln.

(3) Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortung des für die Verarbeitung Verantwortlichen« im Sinne des Art. 24 EU-DSGVO).

(4) Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

(5) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(6) KI-generierte Antworten und Handlungsempfehlungen werden revisionssicher protokolliert. Der Auftraggeber kann nachvollziehen, wann eine KI-gestützte Antwort erzeugt wurde und auf welcher Datenbasis diese beruht. Die finale Entscheidungshoheit über die Umsetzung verbleibt beim Auftraggeber bzw. dessen Nutzern.

(7) Der Einsatz KI-gestützter Systeme erfolgt ausschließlich im Rahmen der Auftragsverarbeitung gemäß Art. 28 EU-DSGVO. Der Auftragnehmer trifft keine eigenständigen Entscheidungen über Zwecke oder Mittel der Verarbeitung. Eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 EU-DSGVO wird hierdurch nicht begründet.

§6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der Weisung bis zu deren Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(3) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO unter Berücksichtigung von Art. 5 Abs. 1 und 2 DSGVO, um ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherzustellen. Dabei werden insbesondere der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner gesetzlichen Verpflichtungen gemäß Art. 28 Abs. 3 DSGVO bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen nach Kapitel III DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(5) Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung personenbezogener Daten befassten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung des Vertragsverhältnisses fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten.

(7) Der Auftragnehmer trifft im Falle einer Datenschutzverletzung unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für betroffene Personen und stimmt sich hierbei mit dem Auftraggeber ab. Er unterstützt den Auftraggeber bei der Erfüllung etwaiger Informationspflichten nach Art. 33 und 34 DSGVO.

(8) Der Auftragnehmer benennt dem Auftraggeber einen Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen.

(9) Der Auftragnehmer gewährleistet, seinen gesetzlichen Verpflichtungen nachzukommen, insbesondere – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten zu bestellen und ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzusetzen.

(10) Der Auftragnehmer verwendet die ihm überlassenen personenbezogenen Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistungen.

(11) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung vertragsgegenständlicher Daten ein, sofern der Auftraggeber dies anweist und keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(12) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person gemäß Art. 82 DSGVO unterstützt der Auftragnehmer den Auftraggeber im Rahmen seiner gesetzlichen Verpflichtungen.

§7 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO. Der Auftraggeber stellt den Auftragnehmer hiermit von sämtlichen Forderungen Dritter rechtsverbindlich frei, soweit die Pflichtverletzung ausschließlich im Verantwortungsbereich des Auftraggebers liegt und kein Verstoß des Auftragnehmers gegen DSGVO oder diesen Vertrag vorliegt. Sämtliche Auslagen des Auftragnehmers, trägt der Auftraggeber.

(3) Der Auftraggeber ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

(4) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(5) Die Daten werden nach dem Ende des jeweiligen Vertrages gelöscht. Es obliegt dem Auftraggeber, rechtzeitig - vor Vertragende - sich beim Auftragnehmer bezüglich der Herausgabe der Daten schriftlich zu melden.

(6) Der Auftraggeber wird darüber informiert, sofern innerhalb der vertraglich vereinbarten Leistungen KI-gestützte Verfahren eingesetzt werden, die personenbezogene Daten analysieren oder verarbeiten. Der Auftragnehmer stellt auf Anfrage Informationen zur Funktionsweise und zu den grundlegenden Entscheidungslogiken der eingesetzten Systeme zur Verfügung, soweit dies technisch möglich und unter Wahrung von Geschäftsgeheimnissen zulässig ist.

(7) Dem Auftraggeber obliegen die sich aus Art. 24 EU-DSGVO und Art. 13 und 14 EU-DSGVO resultierenden Informationspflichten.

(8) Sofern der Auftraggeber KI-gestützte Planungssysteme oder sonstige KI-Assistenzfunktionen im Rahmen seiner Personalorganisation einsetzt, obliegt ihm die datenschutzrechtliche und arbeitsrechtliche Transparenz gegenüber den hiervon betroffenen Beschäftigten.

Der Auftraggeber verpflichtet sich insbesondere, die Informationspflichten gemäß Art. 13 und 14 EU-DSGVO zu erfüllen und – soweit einschlägig – über das Bestehen KI-gestützter Verarbeitungsprozesse, deren Zweck, Funktionsweise sowie die maßgeblichen Entscheidungsparameter in verständlicher Form zu informieren.

Sofern KI-gestützte Systeme Entscheidungsvorschläge im Zusammenhang mit Einsatz-, Schicht- oder Aufgabenplanungen generieren, stellt der Auftraggeber sicher, dass eine angemessene menschliche Überprüfung erfolgt und keine ausschließlich automatisierten Entscheidungen im Sinne des Art. 22 EU-DSGVO ohne entsprechende Rechtsgrundlage getroffen werden.

Weitergehende Transparenz- oder Informationspflichten nach anwendbarem Recht, insbesondere nach der Verordnung (EU) 2024/1689 (EU AI Act), erfüllt der Auftraggeber in eigener Verantwortung.

§8 Weisungsbefugnisse, Berichtigung, Löschung und Sperrung, Rechte Betroffener (Art. 29 i.V.m. 28 EU-DSGVO sowie Kapitel III der EU-DSGVO)

(1) Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragnehmers insbesondere auch zu Berichtigung, Sperrung, Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftragnehmer hierzu gegen Erstattung der anfallenden Kosten verpflichtet. Dem Auftraggeber steht in diesem Fall ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung gemäß Art. 29 i.V.m. 28 EU-DSGVO zu.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(3) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten. Ist der Auftraggeber auf Grund geltender Datenschutzgesetze verpflichtet, Auskünfte zur Erhebung, Verarbeitung und / oder Nutzung von Daten zu erteilen, wird der Auftragnehmer den Auftraggeber dabei soweit notwendig bei der Bereitstellung dieser Informationen unterstützen. Eine diesbezügliche Anfrage hat der Auftraggeber schriftlich an den Auftragnehmer zu richten und diesem die hierdurch entstandenen Kosten zu erstatten.

(4) Sämtliche Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und für die Dauer des Vertragsverhältnisses sowie darüber hinaus entsprechend gesetzlicher Aufbewahrungspflichten aufbewahrt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§9 Anfragen betroffener Personen

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

(2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen Soweit die Unterstützung über die gesetzlich geschuldete Mitwirkung hinausgeht oder durch besondere Weisungen, individuelle Anforderungen oder außergewöhnlichen Aufwand verursacht wird, ist der Auftragnehmer berechtigt, den hierdurch entstehenden zusätzlichen Aufwand gemäß dem jeweils gültigen Preis- und Leistungsverzeichnis gesondert zu berechnen.

§10 Technische und organisatorische Maßnahmen (Art. 32 EU-DSGVO)

(1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, um den Anforderungen der EU-DSGVO zu entsprechen.

(2) Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Er muss den Auftraggeber hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO 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. Wesentliche Änderungen sind zu dokumentieren.

§11 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten auf geeignete Weise nach. Hierzu kann der Auftragnehmer insbesondere aktuelle Zertifizierungen, Auditberichte, Testate, Penetrationstest-Zusammenfassungen oder vergleichbare Nachweise zur Verfügung stellen.

2. Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen durch den Auftragnehmer zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten, unabhängigen Dritten überprüfen zu lassen. Die Überprüfung erfolgt grundsätzlich:

   - nach vorheriger schriftlicher Ankündigung mit angemessener Vorlaufzeit (in der Regel von 3 Wochen),
   - zu den üblichen Geschäftszeiten,
   - ohne unangemessene Beeinträchtigung des Geschäftsbetriebs des Auftragnehmers,
   - unter Wahrung der Vertraulichkeit von Geschäftsgeheimnissen und Daten anderer Kunden.

3. Vor-Ort-Inspektionen sind auf das zur Überprüfung der Einhaltung dieses Vertrages erforderliche Maß zu beschränken. Sie erfolgen grundsätzlich nicht häufiger als einmal pro Kalenderjahr, sofern kein besonderer Anlass vorliegt. Ein besonderer Anlass liegt insbesondere vor bei:

   - einem erheblichen Datenschutzvorfall,
   - konkreten Anhaltspunkten für Vertragsverletzungen,
   - behördlichen Anordnungen oder Prüfungen.

4. Soweit möglich, ist eine Überprüfung vorrangig auf Basis bereitgestellter Unterlagen, Zertifizierungen oder Auditberichte durchzuführen. Eine Vor-Ort-Inspektion erfolgt nur, sofern die berechtigten Prüfinteressen des Auftraggebers nicht durch die Vorlage geeigneter Nachweise angemessen erfüllt werden können.

5. Der Auftragnehmer kann eine angemessene Vergütung für den durch die Prüfung verursachten zusätzlichen Aufwand verlangen, soweit es sich nicht um eine gesetzlich zwingend geschuldete Unterstützung gemäß Art. 28 Abs. 3 lit. h DSGVO handelt. Die Vergütung darf nicht dazu führen, dass das gesetzliche Kontrollrecht faktisch vereitelt wird.

6. Der Auftragnehmer ist berechtigt, die Durchführung der Prüfung von der Unterzeichnung einer angemessenen Vertraulichkeitsvereinbarung abhängig zu machen. Prüfer, die in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer stehen, können aus sachlichem Grund abgelehnt werden.

7. Datenschutzaufsichtsbehörden bleiben von den vorstehenden Einschränkungen unberührt.

§12 Unterauftragsverhältnisse (Art. 28 Abs. 2 u. 4 EU-DSGVO) (Subunternehmer)

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Betrieb, Wartung und Installation der Rechenzentrumsinfrastruktur und Telekommunikationsdienstleistungen, Unternehmen zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

(2) Die Auftragnehmer trägt dafür Sorge, dass dem Auftraggeber eine aktuelle Liste der eingesetzten Unterauftragnehmer im Kundencenter (KC) stets zum Abruf zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragnehmern ergeht hierüber eine Information an den Auftraggeber.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Bereitstellung der Server-Infrastruktur an den Standorten **Nürnberg** und **Falkenstein** (**BRD**) Vorhalten einer betriebsbereiten Notfall-Server-Infrastruktur am Standort **Helsinki** (**Finnland**) im Hetzner-eigenen Datacenter-Park in Tuusula. *Auf Grund der gefährdeten Versorgungssicherheit (Strom & Gas) der BRD seit Sommer 2022. Es werden derzeit nur verschlüsselte Backups auf diesen Notfall-Systemen gespeichert, welche im Ernstfall die Kundenversionen samt aller Daten und Dateien zur Verfügung stellen könnten. Diese Systeme werden nur bei einem mittelbar drohenden Ausfall der Datacenter Nürnberg und Falkenstein (BRD) aktiv eingesetzt und zur Nutzung freigeschaltet.*
Host Europe GmbH c/o Spaces Gertrudenstraße 30-36 50667 Köln Deutschland	Bereitstellung der Server-Infrastruktur am Standort **Köln** (**BRD**)

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(5) Der Auftraggeber kann gegen die Hinzuziehung oder Ersetzung eines Subunternehmers aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information schriftlich oder in Textform widersprechen.

Im Falle eines berechtigten Widerspruchs werden die Parteien eine einvernehmliche Lösung anstreben. Sofern keine Einigung erzielt wird, steht dem Auftraggeber ein außerordentliches Kündigungsrecht hinsichtlich der von der Subunternehmerbeauftragung betroffenen Leistungen zu. Die Leistungserbringung bleibt bis zur Klärung unverändert.

§13 Vergütung von Unterstützungs- und Prüfleistungen

(1) Die vertraglich vereinbarte Vergütung umfasst die gesetzlich geschuldete Mitwirkung und Unterstützung des Auftragnehmers gemäß Art. 28 Abs. 3 DSGVO im üblichen und an-gemessenen Umfang.

(2) Soweit Unterstützungsleistungen über die gesetzlich geschuldete Mitwirkung hinausgehen oder durch besondere Weisungen, individuelle Anforderungen, Sonderprüfungen, Vor-Ort-Inspektionen, umfangreiche Auswertungen, Datenexporte außerhalb standardisierter Funktionen oder sonstigen zusätzlichen Aufwand des Auftraggebers verursacht werden, ist der Auftragnehmer berechtigt, den hierdurch entstehenden zusätzlichen Aufwand gesondert zu berechnen.

(3) Die Abrechnung erfolgt auf Grundlage des jeweils gültigen Preis- und Leistungsverzeichnisses des Auftragnehmers.

(4) Die Vergütung darf das gesetzliche Kontroll- und Unterstützungsrecht des Auftraggebers nicht faktisch vereiteln.

§14 Systembetrieb und Verantwortungsabgrenzung

(1) Der Auftragnehmer stellt die technische Systemumgebung gemäß dem Hauptvertrag bereit. Eine inhaltliche Prüfung der durch den Auftraggeber eingegebenen personenbezogenen Daten oder der durch den Auftraggeber vorgenommenen Konfigurationen erfolgt nicht.

(2) Der Auftraggeber ist für die sachliche Richtigkeit, Vollständigkeit und Rechtmäßigkeit der eingegebenen Daten sowie für die ordnungsgemäße Nutzung der bereitgestellten Funktionen verantwortlich.

(3) Der Auftragnehmer schuldet keine rechtliche Prüfung arbeitsrechtlicher, sozialrechtlicher oder sonstiger regulatorischer Anforderungen im Zusammenhang mit der Nutzung des Systems.

(4) Automatisiert generierte Auswertungen, Analysen oder Planungsvorschläge stellen unverbindliche Systemergebnisse dar. Die finale fachliche und rechtliche Bewertung obliegt ausschließlich dem Auftraggeber.

§15 Informationspflichten, Schriftformklausel, Rechtswahl, Sonstiges

(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*« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) im Kundencenter (KC) des Auftragnehmers erfolgen kann, 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) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen (kurz AGB) des Auftragnehmers.

(5) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG). Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Köln, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

§16 Haftung und Schadensersatz

(1) Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

Der Auftraggeber stellt den Auftragnehmer im Innenverhältnis von sämtlichen Ansprüchen Dritter frei, soweit diese auf einer rechtswidrigen Verarbeitung beruhen, die ausschließlich im Verantwortungsbereich des Auftraggebers liegt. Die Freistellung gilt nicht, soweit der Auftragnehmer gegen ihm obliegende Pflichten aus der EU-DSGVO oder aus diesem Vertrag verstoßen hat. Die gesetzlichen Haftungsregelungen nach Art. 82 EU-DSGVO bleiben im Übrigen unberührt.

§17. Auftragserteilung des Auftraggebers

Der Unterzeichner, seines Zeichens Inhaber, Geschäftsführer, Prokurist bzw. zeichnungsberechtigte Person schließt hiermit rechtsverbindlich den vorgenannten AV-Vertrag und bestätigt, dass er/sie den AV-Vertrag gelesen und akzeptiert hat. Der AV-Vertrag kommt mit Annahmebestätigung durch die 4Mis GmbH zustande.

Unterschrift: (Auftragnehmer)	
Ort, Datum / Position / Funktion	Stempel
Name in Druckbuchstaben	Unterschrift

1. Unterschrift: (Auftraggeber)	
Ort, Datum / Position / Funktion	Stempel
Name in Druckbuchstaben	Unterschrift

2. Unterschrift: (Auftraggeber) (optional)	
Ort, Datum / Position / Funktion	Stempel
Name in Druckbuchstaben	Unterschrift

Anlage 1:

Technische und organisatorische Maßnahmen nach Art. 32 EU-DSGVO

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.

Der Provider erbringt ausschließlich Dienstleistungen höchster Qualität und Sicherheit. Die Sicherheit der Kundendaten und die Verfügbarkeit der Dienstleistungen werden unter anderem durch die folgenden Maßnahmen sichergestellt:

a. Physische Sicherheit durch bauliche, betriebliche und technische Maßnahmen:

- 24 Stunden, 7 Tage pro Woche, 365 Tage im Jahr Sicherheitspersonal vor Ort
- Elektronische Zutrittskontrollsysteme
- Videoüberwachung vor und im Gebäudekomplex
- Rauch-, Staub- und Wassermelder mit Aufschaltung bei der örtlichen Feuerwehr
- Argongas- oder Inergen-Brandbekämpfungsanlage
- Einbruchsmeldeanlage mit Aufschaltung bei einem Sicherheitsdienst
- Klimatisierung über 2 getrennte Kühlkreisläufe (n+1)
- redundante Stromzuführung durch Energieversorger (Nord/Süd-Einspeisung)
- redundante (n+1) unterbrechungsfreie und gefilterte Stromversorgung durch USV-Batterien
- leistungsstarker Diesel-Notstrom-Generator

b. Sicherheit und Verfügbarkeit der internen Netzwerkinfrastruktur:

- Segmentierung der Netzwerke und strikte Trennung der unterschiedlicher Datenströme (IP-, Management-, Backup-LAN usw.)
- tägliches Backup der eigenen Systeme
- Einsatz von Firewalls an relevanten Netzwerkpunkten
- Netzwerküberwachung durch hauseigenes NOC („Network Operation Center“)
- ausschließliche Verwendung von Markenkomponenten

c. Verfügbarkeit der externen Netzwerkanbindung:

- carrier-neutrale und dreifach-redundante IP-Anbindung
- redundante Glasfaserzuführung durch unterschiedliche Lieferanten der physikalischen Zugangsleitungen

Vertraulichkeit (Art. 32 Abs. 1 EU-DSGVO)

- **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:

  - Alle Mitarbeiter der 4Mis GmbH sind zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.
  - Der Kunde hat die Möglichkeit, die 4Mis GmbH für bestimmte Administrationsaufgaben zu beauftragen und die 4Mis GmbH sorgt für das Monitoring und die Wartung der Systeme. Die Administrationszugriffe werden adäquat protokolliert.
  - Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
  - Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
  - Einrichtung eines Benutzerstammsatzes pro User
  - Verschlüsselung von Datenträgern
  - Personenbezogene Anmeldungen mit Login-Historie
  - Zugriffs- und Zeitgesteuerte Profile je User
  - Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte) je Mitarbeiter.
  - Bedarfsorientierte Zugriffsausgestaltung. Berechtigungskonzept der Zugriffsrechte sowie deren Überwachung und Protokollierung:
    - Auswertungen
    - Kenntnisnahme
    - Eintragungen
    - Veränderung
    - Löschung

- **Zutrittskontrolle**

  Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen die personenbezogenen Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden:

  - Zugänge zu den Büroräumen grundsätzlich verschlossen
  - elektronisches Zutrittskontrollsystem mit Protokollierung
  - Besucherregelung: Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines 4Mis GmbH Mitarbeiters
  - Dokumentierte Verfahrensweise für Ausgabe und Rückgabe der Zugangsmittel
  - Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels
  - Einbruch- und Kontaktmelde-Alarmanlage
  - Videoüberwachung der gesamten Büroräumlichkeiten sowie den Eingangsbereichen
  - Videoüberwachung der angemieteten Bereiche in den Rechenzentren
  - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden
  - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

- **Zugangskontrolle**

  Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Die 4Mis GmbH stellt die Datenverarbeitungsanlagen den Kunden zur Nutzung bereit
- Dies beinhaltet die Vermietung von Hard- und Software, sowie weitere Dienste entsprechend der jeweiligen Vereinbarung.
- Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitetet werden („Herr der Daten“)
- Die 4Mis GmbH sorgt für die technische Einsatzbereitschaft der Systeme entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden.
- Die Entscheidung über Zwecke, Inhalte und konkrete Ausgestaltung der Datenverarbeitung liegt ausschließlich beim Auftraggeber.

  Der Auftragnehmer stellt die technische Infrastruktur sowie die vertraglich vereinbarten Funktionen zur Verfügung und verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers gemäß Art. 28 DSGVO.
- Der Auftragnehmer bestimmt weder die Zwecke der Verarbeitung noch die inhaltliche Auswahl der durch den Auftraggeber eingegebenen personenbezogenen Daten..
- Es haben nur wenige ausgewählte Administratoren Zugang zu den Servern. Jeder dieser Administratoren hat eine individuelle Benutzerkennung und erhält ausschließlich über das 4Mis-Netzwerk Zugang. Es bestehen Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter/-Schlüssel.
- Firewall, Intrusion Detection System
- Dokumentierte Vergabe-Richtlinie für Benutzer-IDs und Kennworte
- Verbindung zum Rechenzentrum nur über VPN
- Whitelist für zugelassene IP-Adressen
- Zwei-Faktor-Authentifizierung

- **Trennungskontrolle**

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

  - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen
  - Grundsätzlich liegt eine physikalische oder logische Trennung einzelner Kundensysteme vor. Jeder Kunde hat eine für sich vom System getrennte Datenbank.
  - Es existiert ein Berechtigungskonzept auf den Systemen.
  - Firmendaten (Buchhaltung, Personalverwaltung etc.) physikalisch getrennt
  - Trennung von Entwicklungs-, Test-, Backup- und Produktionsumgebungen

- **Verschlüsselungsmaßnahmen**

  Personenbezogene Daten werden bei der Übertragung unter Verwendung dem Stand der Technik entsprechender Verschlüsselungsverfahren (insbesondere TLS in aktueller Version) geschützt. Soweit technisch möglich und dem Stand der Technik entsprechend, erfolgt eine Verschlüsselung personenbezogener Daten auch im Ruhezustand (Data-at-Rest), insbesondere bei Datensicherungen und mobilen Datenträgern.

Integrität (Art. 32 Abs. 1 EU-DSGVO)

- **Weitergabekontrolle**

  Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger 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 4Mis GmbH verfügt über organisatorische Maßnahmen, welche den Zugriff auf die Systeme regelt um den Systembetrieb sicherzustellen.
  - Sämtliche Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Support-Mitarbeiter. Die Anzahl der Mitarbeiter, werden von der 4Mis GmbH möglichst gering gehalten. Bei Änderungen durch 4Mis-Mitarbeiter werden die Support-Zugriffe adäquat protokolliert.
  - SSL-Verschlüsselung der übertragenden Daten
  - VPN-Tunnelverbindung (VPN = Virtual Private Network)
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 EU-DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Die 4Mis GmbH hat keinen Zugriff auf durch den Kunden verarbeitete personenbezogene Daten – außer der Kunde beauftragt die 4Mis GmbH mit Aufgaben in seiner Kundenversion. Bei Änderungen durch die 4Mis GmbH werden die Supportzugriffe adäquat protokolliert. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Support-Mitarbeiter. Sämtliche Zugriffe finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
  - Protokollierung sämtliche Zugriffe und Datenveränderungen
  - Identifizierung / Authentifizierung
  - Regelungen für Datenträgervernichtung

- **Eingabekontrolle**

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

  - Wie bereits oben ausgeführt, erfolgt die Datenverarbeitung durch den Kunden. Die 4Mis GmbH hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann. Bei Änderungen durch die 4Mis GmbH werden die Administrationszugriffe adäquat protokolliert.
  - Protokollierungs- und Protokollauswertungssystem aller Einsichten, Eingaben, Änderungen und Löschungen
  - Regelungen zum Zugriff und zur Löschung der Protokolle

Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art. 32 Abs. 1 EU-DSGVO)

- **Verfügbarkeitskontrolle**

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

  - Alle Server stehen in Rechenzentren in Deutschland.
  - Die autonome Stromversorgung der Data Center erfolgt über eigene Trafostationen. Die Stromversorgung und Netzersatzanlage garantieren höchste Ausfallsicherheit.
  - Der gesamte Energieverbrauch der Data Center wird über eine unterbrechungsfreie Stromversorgung (USV) sichergestellt. Im Falle eines Stromausfalls garantiert die USV-Anlage eine unterbrechungsfreie Umschaltung auf eines der Notstrom-Dieselaggregate. Daneben filtert die USV vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.
  - Eine leistungsstarke Netzersatzanlage (Dieselaggregat) versorgt bei Stromausfall das gesamte jeweilige Data Center und die Kühlsysteme mit konstanter Energie.
  - Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern.
  - Klimaanlagen
  - Datenbanken befinden sich auf Cluster-Server-Systemen.
  - Rechenzentren sind DIN ISO 27001-zertifiziert
  - Schutzmaßnahmen:
    - Zutrittskotrollsysteme
    - Videoüberwachung
    - Redundante unterbrechungsfreie Stromversorgung
    - Überspannungsschutz
    - Schutz gegen Feuer und Wassereintritt
    - Monitoring der Leitungskapazitäten
    - Intrusion Detection System (DoS/DDoS-Angriffe)
  - Redundante IT-Infrastruktur (z.B. durch Virtualisierung)
  - Spiegeln von Festplattenspeicher, z.B. RAID-Verfahren bei allen relevanten Systemen.
  - Ersatz- und Austauschkomponenten vor Ort vorhanden
  - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten in ein anderes Data Center.
  - Prüfung der Rücksicherung/Wiederherstellung
  - Einheitliche Beschaffungsstrategie für Soft- und Hardware
  - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
  - Geo-Redundantes Backup-Verfahren (Sicherungsserver liegen in unterschiedlichen Datacentern)
  - Notfallplan
  - Unterbrechungsfreie Stromversorgung (USV und Dieselgeneratoren)

- **Rasche Wiederherstellbarkeit**

  Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 & Art. 25 Abs. 1 EU-DSGVO)

- **Auftragskontrolle**

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

  - Eindeutige Vertragsgestaltung
  - Formalisierte Auftragserteilung (Auftragsformular)
  - Kontrolle der Vertragsausführung
  - Verpflichtung der Mitarbeiter auf das Datengeheimnis
  - Die 4Mis GmbH hat einen Datenschutzbeauftragten formal bestellt.
  - Die Auftraggeber erhalten bei der 4Mis GmbH im Rahmen der Auftragsdatenverarbeitung ein Kontrollrecht.

- **Datenschutz-Management**

  Es ist ein Datenschutzmanagementsystem implementiert, mit dessen Hilfe die Nachweispflichten der EU-DSGVO und des BDSG-neu umgesetzt werden:

  - Rechtsgrundlagen der Verarbeitung, Art.6 EU-DSGVO
  - Erteilung der Einwilligung, Art.7 EU-DSGVO
  - Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art.12 EU-DSGVO
  - Einhaltung der Informationspflichten, Art.13 EU-DSGVO
  - Datenschutz durch Technik, Art.25 EU-DSGVO
  - Auskunftsrecht der betroffenen Person, Art.15 EU-DSGVO
  - Recht auf Berichtigung, Art.16 EU-DSGVO
  - Recht auf Löschung, Art.17 EU-DSGVO
  - Umsetzung der Speicherbegrenzung, Art.5 EU-DSGVO
  - Umsetzung der Sicherheit der Verarbeitung, Art.32 EU-DSGVO
  - Auflistung aller Auftragsverarbeiter, Art.30 Abs.2 EU-DSGVO
  - Umgang mit Datenschutzverletzungen, Art.33 EU-DSGVO
  - Darstellung der Meldepflicht an Aufsichtsbehörden, Art.33 EU-DSGVO
  - Verwendung von Werkzeug Zertifizierung, Art.42 EU-DSGVO
  - Risikobewertung / Datenschutzfolgenabschätzung, Art.35 EU-DSGVO
  - Dokumentation von Audits
  - Dokumentation von Awareness-Maßnahmen

- **KI-Systeme**

  Bei Einsatz KI-gestützter Systeme stellt der Auftragnehmer sicher, dass

  - Trainings- und Produktivdaten logisch getrennt verarbeitet werden,
  - keine unkontrollierte Datenpersistenz außerhalb der vereinbarten Systemumgebung erfolgt,
  - Zugriffe auf KI-Auswertungssysteme protokolliert werden,
  - Eingaben (Prompts) und Ausgaben (Outputs) revisionssicher nachvollziehbar sind,
  - geeignete technische Maßnahmen zur Verhinderung von Datenabfluss (z.B. durch Prompt-Injection oder unbefugte Modellabfragen) implementiert sind.

- **Incident-Response-Management**

  Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen, eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)**

  Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen und Planung bereits berücksichtigt (Art. 25 Abs. 2 EU-DSGVO).

Anlage 2:
KI-gestützte Verarbeitungssysteme

1. Gegenstand

Diese Anlage konkretisiert die datenschutzrechtlichen Rahmenbedingungen für den Einsatz KI-gestützter oder algorithmischer Systeme im Rahmen der vertraglich vereinbarten Leistungen.

---

2. Art der eingesetzten KI-Systeme

Der Auftragnehmer kann folgende KI-gestützte Verfahren einsetzen:

a) KI-Assistenzsystem zur Analyse und Beantwortung von Supportanfragen

b) KI-gestützte Einsatz- und Dienstplanvorschlagssysteme

Die Systeme generieren ausschließlich Entscheidungsvorschläge oder Handlungsempfehlungen.

---

3. Keine ausschließlich automatisierten Entscheidungen

Die Systeme treffen keine ausschließlich automatisierten Entscheidungen im Sinne des Art. 22 EU-DSGVO mit rechtlicher Wirkung gegenüber betroffenen Personen.

Die finale Entscheidungshoheit verbleibt beim Auftraggeber.

---

4. Mandantentrennung

Eine mandantenübergreifende Zusammenführung personenbezogener Daten findet nicht statt.

Trainings- und Produktivdaten werden logisch getrennt verarbeitet.

---

5. Trainingsdaten

Eine Nutzung personenbezogener Daten zu Trainingszwecken erfolgt ausschließlich:

- in anonymisierter Form im Sinne des Erwägungsgrundes 26 EU-DSGVO oder
- auf Grundlage einer gesonderten schriftlichen Vereinbarung mit dem Auftraggeber.

Eine dauerhafte Speicherung personenbezogener Echtdaten in Trainingsmodellen erfolgt nicht.

---

6. Transparenz

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage Informationen über:

- Funktionsweise der eingesetzten KI-Systeme
- berücksichtigte Entscheidungsparameter
- technische Schutzmaßnahmen

zur Verfügung, soweit dies technisch möglich und unter Wahrung von Geschäftsgeheimnissen zulässig ist.

---

7. Diskriminierungsvermeidung

Die eingesetzten Systeme berücksichtigen ausschließlich arbeitsorganisatorisch relevante Parameter. Unzulässige oder diskriminierende Merkmale werden nicht verwendet.

---

8. Protokollierung

KI-generierte Ausgaben und relevante Systemzugriffe werden revisionssicher protokolliert.

---

9. Technische Schutzmaßnahmen

Es gelten ergänzend die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen.

---

10. Menschliche Aufsicht

Das KI-gestützte Planungssystem generiert ausschließlich unverbindliche Planungsvorschläge. Eine automatische verbindliche Einsatz- oder Schichtzuweisung erfolgt nicht.

Die finale Entscheidung und Freigabe des Dienstplans obliegt ausschließlich dem Auftraggeber oder dessen autorisierten Nutzern.

Das System ist so ausgestaltet, dass eine wirksame menschliche Kontrolle („Human Oversight“) jederzeit gewährleistet ist und eine inhaltliche Überprüfung sowie Anpassung der Vorschläge vor verbindlicher Umsetzung erfolgt.

Der Auftraggeber bleibt für die rechtliche Bewertung und Einhaltung etwaiger regulatorischer Anforderungen im Zusammenhang mit dem konkreten Einsatz des Systems verantwortlich..
