Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

Name

Firma

Position

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

VKNet GmbH, Im Wiesaztal 1, 72770 Reutlingen

- Auftragsverarbeiter - nachstehend VKNet bzw. Auftragnehmer genannt

Präambel

Der Auftragnehmer erbringt gegenüber des Auftraggebers verschiedene Dienstleitungen (im Folgenden „Leistungen“ genannt) im Rahmen einer gesonderten, auf Grundlage seiner Voraussetzungen in schriftlich oder in elektronischer Form abgegebenen Allgemeinen Geschäftsbedingungen (im Folgenden „Hauptvertrag“ genannt).

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

1.1.2 Der Auftragnehmer verarbeitet im Rahmen der Erbringung der von ihm aufgrund des Hauptvertrages geschuldeten Leistungen personenbezogener Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSVGO.

1.1.3 Dieser Vertrag regelt die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer im Rahmen der Erfüllung, auf Grundlage des Hauptvertrags, für den Auftraggeber verarbeitet.

1.2 Dauer

1.2.1 Die Dauer richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus Bestimmungen nicht darüber hinausgehende Verpflichtungen ergeben.

2. Konkretisierung des Auftragsinhalts

2.1 Umfang und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem jeweiligen Hauptvertrag.

2.2 Art der personenbezogenen Daten:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs-, Buchungs- und Zahlungsdaten
- vom Kunden im System gespeicherte Daten

2.3 Kategorien betroffener Personen:

- Beschäftigte des Auftraggebers
- Kunden des Auftraggebers
- sonstige Geschäftskontakte des Auftraggebers

2.4 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Leistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Rechte und Pflichten des Auftragnehmers sowie Weisungsbefugnisse

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrags und der Weisung des Auftragsgebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Art. 28 Abs. 3 DSGVO vor.
Für die Beurteilung der Zuverlässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Person nach den Art. 12 bis Art. 22 DSGVO ist allein der Auftraggeber verantwortlich.
Der Auftragsnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze (z.B. Datenschutzvorschriften) verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftragsgebers nicht erstellt.

3.3 Sofern vom Auftraggeber mittels Weisung verlangt und keine berechtigten Interessen des Auftragnehmers entgegenstehen, hat der Auftragnehmer die Daten unmittelbar zu löschen oder deren Verarbeitung einzuschränken.
Die vorstehenden Löschungspflichten gelten nicht für Datenkopieren, die in regelmäßigen erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragnehmers enthalten sind und deren isolierte Löschung einen erheblichen Aufwand für den Auftragnehmer bedeuten würde.
Sollte vom Auftraggeber eine sofortige Löschung solcher Sicherungskopien verlangt werden, welche außerhalb des angewandten Sicherungs-Zyklus, spätestens nach einem Jahr gelöscht oder überschrieben werden, muss der Auftraggeber die hierdurch verursachten Kosten erstatten. Dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.
Die Wiederherstellung und jede sonstige Verwendung solcher Kopien bis zu ihrer automatischen Löschung bzw. Überschreibung ist auch nach Vertragsbeendigung unzulässig.

3.4 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber ersteilen, soweit der Auftraggeber nicht gesetzlich zur Auftragserteilung verpflichtet ist.

3.5 Der Auftragnehmer verpflichtet sich bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu bewahren. Diese besteht auch nach Beendigung des Vertrags fort.

3.6 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 DSVGO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

4. Rechte und Pflichten des Auftraggebers sowie Weisungsbefugnisse

4.1 Die Weisungen werden anfänglich durch einen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher- oder elektronischer Form (Textform) an die Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden.
Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber nach dem Hauptvertrag schuldet, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten.
Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht dem Auftragnehmer ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

4.2 Der Auftraggeber ist berechtigt, sich wie unter **Nr.5** festgelegt, vor und während der Datenverarbeitung, aber in angemessenere weise (nicht häufiger als alle 12 Monate) unter Berücksichtigung einer angemessenen Vorlaufzeit sowie zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs, sich von den technischen und organisatorischen und Datenschutz sowie Datensicherheitsmaßnahmen, Verpflichtungen und Vereinbarungen zu überzeugen.
Sollte der Auftraggeber einen Dritten zur Überprüfung (Art. 28 Abs. 3 DSVGO) beauftragen, welcher in einem Wettbewerbsverhältnis zu dem Auftragnehmer steht, hat der Auftragnehmer ein Einspruchsrecht.
Der Auftragnehmer sichert zu, soweit erforderlich, bei diesen Kontrollen unterstützend mitzuwirken. Für den hierfür entstehenden Mehraufwand steht dem Auftragnehmer eine zusätzliche Vergütung zu.

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

4.4 Der Aufraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrags bestehen.

4.5 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

4.6 Der Auftraggeber listet weitere weisungsbefugte Personen in **Anlage 3** auf.

5. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

5.1 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder bei dem ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.
Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer allgemein gestattet, Art. 28 Abs. 2 DSGVO. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung im Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Auftragnehmer muss dafür Sorge tragen, dass er Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

6.3 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

6.4 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 DSGVO). Sofern dem Vertrag mit einem Subunternehmer dessen eigene Vertragsbedingungen zugrunde liegen, müssen Vertragsbedingungen entweder vom Auftragnehmer genehmigt oder mindestens das Schutzniveau des vorliegenden Vertrages erreichen. Der Auftraggeber hat das Recht, auf Verlangen Einsicht in die relevanten Vertragsbedingungen zu nehmen.

6.5 Die Weiterleitung von Daten an einen Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

6.6 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

6.7 Die zurzeit für den Auftragnehmer mit der Verarbeitung von personenbezogenen Daten beschäftigten Subunternehmer ergeben sich aus der Tabelle aus **Anlage 2**.

Grundlage der Beauftragung dieser Subunternehmer sind ihre jeweiligen Standardbedingungen (einschließlich ihrer Standard-Maßnahmen zum technischen und organisatorischen Schutz der jeweils verarbeiteten Daten), die auf den o.g. Websites veröffentlicht sind. Mit der Beauftragung dieser Subunternehmer sowie deren jeweiligen Standardbedingungen erklärt sich der Auftraggeber einverstanden.

7. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. C DSGVO)

7.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug und Art, Umfang, Umstände und Zweck der Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

7.2 Das als Anhang beigefügte Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Aufragnehmer dar.

7.3 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, einer Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und Verarbeitung durchzuführen (Art. 32 Abs. 1 DSGVO)

7.4 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

7.5 Die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind in **Anlage 1** beschrieben.

8. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 DSGVO)

8.1 Nach Vertragsbeendigung hat der Auftragnehmer sämtliche im Besitz des Auftragnehmers sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Bis zur Vertragsbeendigung kann der Auftraggeber die Daten über die durch den Auftragnehmer bereitgestellten Standard-Schnittstellen selbst über das Internet abrufen und bei sich speichern. Der Auftraggeber kann vom Auftragnehmer auch die Bereitstellung der Daten in anderer Form verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch

verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

9. Verschiedenes

9.1 Für Nebenabreden zu diesem Vertrag ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

9.2 Bei etwaigen Wiedersprüchen gehen Regelungen dieses Vertrages über die Auftragsverarbeitung von personenbezogenen Daten den Regelungen des Hauptvertrages vor.

9.3 Sollten die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

9.4 Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

9.5 Es gilt deutsches Recht unter Ausschluss eventueller Verweisungen auf andere Rechtsordnungen und unter Ausschluss des UN Kaufrechts.

9.6 Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag beim Sitz des Auftragnehmers.

10. Anfragen betroffener Personen

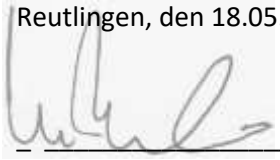
10.1 Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betreffenden Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

11. Haftung und Schadenersatz

11.1 Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Unterschriften

…….., den …….. Reutlingen, den 18.05.2018



_____ _____

Auftraggeber Auftragnehmer

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.
Gesichert durch: Schlüssel, elektrische Türöffner, Alarmanlagen, Videoanlagen;

1.2 **Zugangskontrolle**
Keine unbefugte Benutzung von Datenverarbeitungssystemen.
Gesichert durch: sichere Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern, Einsatz von Firewalls und Anti-Viren-Software

1.3 **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.
Gesichert durch: Systemberechtigungen und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

1.4 **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
Umgesetzt durch: Mandantenfähigkeit, getrennte Datenbanken, getrennte virtuelle Systeme

1.5 **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
Umgesetzt durch: Transportverschlüsselung, Passwörter, elektronische Signatur

2.2 **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
Umgesetzt durch: Benutzeridentifikation, Eingabevalidierung, Protokollierung und Überwachung, Auswertung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
Umgesetzt durch: Brandschutzanlage, Überspannungsschutz, Unterbrechungsfreie Stromversorgung (USV), Backup-Strategie (online/offline, onsite/offsite), Backup-Verfahren, Spiegeln von Festplatten (Raid-System), Getrennte Aufbewahrung, Virenschutz, Firewall

3.2 **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DSGVO)
Maßnahmen zur geregelten und zügigen Wiederherstellung von Daten und Services nach einem Vorfall.
Umgesetzt durch: Regelmäßige Backups, Meldewege, Notfallpläne

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

4.1 **Datenschutz-Management**
Organisationsstruktur und Prozesse um nachvollziehbaren Schutz von Daten zu ermöglichen
Umgesetzt durch: Dokumentation der Prozesse im Verarbeitungsverzeichnis

4.2 **Incident-Response-Management**
Prozesse um die rasche und zielgerichtete Behandlung von (Datenschutz-) Vorfällen zu ermöglichen. Dies umfasst insbesondere das Melden von Datenschutzverstößen.
Umgesetzt durch: Verpflichtung aller Mitarbeiter, Datenverstöße unverzüglich an die Geschäftsleitung zu melden.

4.3 **Datenschutzfreundliche** Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Technische und organisatorische Maßnahmen um die Datenschutzgrundsätze (gemäß Art. 5 DSGVO) wirksam umzusetzen.
Umgesetzt durch: Maßnahmen zur Datenminimierung, Anonymisierung/Pseudonymisierung

4.4 **Auftragskontrolle**
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
Umgesetzt durch: Keine Verwendung der Daten zu eigenen Zwecken

Anlage 2 – Subunternehmer

Subunternehmer des Auftragnehmers

Zurzeit sind für den Auftragnehmer keine Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt.

Anlage 3 – weitere weisungsbefugte Personen des Auftraggebers

Name	Position	E-Mail