Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

zwischen

-nachstehend Auftraggeber genannt und

dem Auftragsverarbeiter

KAB Maklerservice GmbH
Kolumbusstraße 31
53881 Euskirchen

- nachstehend Auftragsnehmer genannt

§ 1 Einleitung, Geltungsbereich und 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 in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

§ 2 Gegenstand der Vereinbarung

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst folgende Tätigkeiten, die sich aus der Leistungsbeschreibung und im Rahmen der Nutzung der Anwendung(en) und bereitgestellter Dienste des Auftragnehmers ergeben:

- Onlinetarifierung
  Berechnung von Versicherungstarifen über Online-Schnittstellen, die von Versicherungsunternehmen oder beauftragten Dienstleistern über das Internet bereitgestellt werden. Hierfür erfolgt eine Übertragung aller für eine Tarifierung und Angebotserstellung benötigte Daten in Rechenzentren (gemäß § 6 Leistungsort) des Auftragnehmers oder beauftragen Dienstleistern, wo sie verarbeitet und gespeichert werden.

- Onlineanträge
  Elektronische Übermittlung von Versicherungsanträgen an Versicherer oder vom Auftragnehmer beauftragte Dienstleister in der vom Versicherer gewünschten Form (z.B. an Schnittstellen/Web-Service, E-Mail, Fax).
  Hierfür erfolgt eine Übertragung aller für einen Antrag benötigten Daten in Rechenzentren gemäß § 6

- Leistungsort) des Auftragnehmers oder beauftragten Dienstleistern, wo sie verarbeitet und gespeichert werden.

- Abruf von elektronischen Versicherungsbestätigung (eVB) über Online-Schnittstellen, die von Versicherungsunternehmen oder vom Versicherer beauftragte Dienstleister über das Internet bereitgestellt werden.

- Hierfür erfolgt eine Übertragung aller für eine eVB benötigten Daten in Rechenzentren (gemäß § 6 Leistungsort) des Auftragnehmers oder beauftragten Dienstleister, wo sie verarbeitet und gespeichert werden.

- Web-Anwendungen / Web-Services

- Bei Nutzung von Web-Anwendungen des Auftragnehmers werden sämtliche Daten, die für die Erfüllung der vereinbarten Dienstleistungen notwendig sind und eingegeben bzw. übertragen werden, in Rechenzentren (gemäß § 6 Leistungsort) des Auftragnehmers oder beauftragten Dienstleister verarbeitet und gespeichert. Dies betrifft insbesondere Daten des Auftraggebers, Anwender-/Nutzerdaten,Maklerdaten, Tarifierungsdaten, Vertragsdaten, Kundendaten, Dokumente etc.

- Schnittstellen
  Bereitstellung von Schnittstellen zu Anwendungen und zu Funktionen zur Nutzung durch den Auftraggeber bzw. vom Auftraggeber autorisierte Dritte. Über die Schnittstellen können sämtliche Daten (Tarifierungsdaten, Vertragsdaten, Kundendaten, Dokumente) transferiert werden.

2. Mittels der im Vertrag zur Zusammenarbeit beauftragten Dienstleistungen/Softwareprodukte Dokumentenservice ist seitens des Auftraggebers die Leistung zur Speicherung, Verwaltung, Verarbeitung, Korrektur, Anpassung, Auswertung beauftragt und werden im ausschließlichen Rahmen der Zweckbestimmung der Erfüllung der vertraglichen Pflichten verarbeitet. Alle nicht damit einhergehenden zweckbezogenen Verarbeitungen sind ausgeschlossen, sofern diese nicht durch den Auftraggeber mit geltendem Recht vereinbarten Weisungen beauftragt wurden.

3. Konkretisierung des Auftragsinhaltes:
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / Datenkategorien: Personendaten (bspw. Name, Anschrift, Kontaktdaten, Geburtsdatum, Geschlecht), Kundenbeziehungen (bspw. Familienverhältnisse zwischen Kunden) und Vertragsbeziehungen (bspw. Risikoträger, Mitversicherungsnehmer), Kommunikationsdaten (bspw. Telefonnummer, E-Mail Adresse, Fax-Nr., Mobil- Nr.), Vertragsdaten (bspw. Versicherungsbeginn, Versicherungsablauf, versichertes Risiko, Jahresprämie, Zahlweise), Versicherungsrisikodaten (bspw. Fahrzeugdaten, Gebäudedaten, Standortinformationen, Aufbauarten, Ausstattungsmerkmale, versicherte Personen), Daten von Vorversicherungen, Daten aus Bonitätsprüfungen, Produktinformationen (bspw. Art und Ausprägung versicherter Leistungen), Abrechnungs-, Planungs- und Steuerungsdaten (bspw. Provisionshöhe, Provisionsart, Abrechnungsart, Abrechnungshöhe, Zahlweise), Auskunftsangaben (bspw. Registrierungsinformationen, Zugriffszeiten, Bearbeitungszeiten), Abrechnungsdaten (bspw. Fälligkeit, Beitragsrückstand, Beitragshöhe, Mahnbetrag), Vorgangsdaten (bspw. Geschäftsvorfallart, Beschreibung, Zeitpunkt, Bearbeiter), Dokumente (bspw. Schriftwechsel, Schreiben, Policen, Nachträge, Mahnungen, Rechnungen, Vertragsstand, Bedingungen, GDV-Daten, Inkassolisten), Gesundheitsdaten / Gesundheitsangaben (bspw. Arztbericht, Gesundheitsfragen, Gesundheitsantworten, Risikoeinschätzungen, Ablehnungen).

4. Konkretisierung der betroffenen Personen:
Interessenten, Versicherungsnehmer, mitversicherte Personen, Kontoinhaber, Geschädigte, Schädiger, Vermittlerdaten, Vermittler-Mitarbeiterdaten, Vermittler-Untervermittlerdaten, Geschäftspartner **Zweck** der unter (2) und (3) genannten Verarbeitungen ist es, die Dienstleistungen und Produkte vom Auftragnehmer für den Auftraggeber nutzbar zu machen und diese zu betreiben.

- Nutzung des Maklerverwaltungsprogrammes, mit welchem der Auftraggeber die vorgenannten Datenkategorien seiner Kunden verarbeiten (bspw. Eingeben, verwalten, korrigieren, speichern, bearbeiten, auswerten, löschen, bereitstellen) kann.

- Nutzung der Vergleichs- und Onlinerechner, mit welchem der Auftraggeber die vorgenannten Datenkategorien seiner Kunden zur Berechnung von Vergleichsangeboten und zur Erstellung von Versicherungsanträgen zur Weiterleitung an die Versicherungsgesellschaften nutzen kann.

- Erstellung von Angeboten und Anträge
- Support
- Erstellung von Courtageabrechnungen Verwaltung bestehender Verträge Kommunikation
- Verwaltung der angeschlossenen Vermittler

5. Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag zur Zusammenarbeit.

6. Die Verarbeitung beginnt mit dem Vertragsbeginn des Hauptvertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

§ 3 Weisungen

1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird.

2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen folgendermaßen:

Weisungsbefugt sind alle beim Auftraggeber angestellten und tätigen Personen. Zur Annahme von Weisungen sind alle beim Auftragnehmer angestellten und tätigen Personen der Geschäftsleitung, schriftlich explizit benannte Kundenbetreuer sowie der Datenschutzbeauftragte befugt.

3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen

4. 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.

5. Der Auftragnehmer und der Auftraggeber haben erteilte / ausgesprochene Weisungen und deren Umsetzung zu dokumentieren.

§ 4 Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich. 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 Vereinbarung 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 persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierende, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 24 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 6 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken. Für die Ermöglichung von Kontrollen durch den Auftraggeber, kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

6. Der Auftraggeber verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten die Vertraulichkeit zu wahren. Er verpflichtet sich zur Geheimhaltung und Verschwiegenheit der zur Kenntnis gelangten Informationen und Betriebsabläufe. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.

7. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann. Der Auftragnehmer behält sich vor, eine stichprobenartige Überprüfung durch Vorlage der Einwilligungserklärung vorzunehmen.

8. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. Datenschutzrechtlicher Bestimmungen feststellt.

§ 5 Leistungsort

1. Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in Anhang 3 dargestellt. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.

2. Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

3. Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU/ EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

4. Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochennach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

5. Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. Sicheren "Drittstaat" erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

6. Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DS-GVO wird durch den Auftragnehmer gewährleistet.

7. Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

8. Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 6 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht durch das Recht der Union oder des Mitgliedstaates, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist (bspw. bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 DSGVO).

2. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten die Vertraulichkeit zu wahren. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.

3. Er sichert ferner zu, dass er die mit der Durchführung der Arbeiten befassten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und sie, soweit sie nicht die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet.

4. Soweit eine Mitwirkungsleistung des Auftragnehmers für die Wahrung von Betroffenenrechten gemäß Art. 12-22 DSGVO durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Mitwirkungsleistungen nach Weisung des Auftraggebers erbringen. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber unterrichten, wenn Betroffene derartige Rechte gegenüber dem Auftragnehmer geltend machen.

5. Ferner unterstützt der Auftragnehmer den Auftraggeber in dem jeweils erforderlichen Umfang dabei, die dem Auftraggeber obliegenden Pflichten,
a. ein dem Risiko angemessenes Schutzniveau zu gewährleisten
b. eine Verletzung des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
c. den Auftraggeber im Rahmen seiner Informationspflicht gegenüber Betroffenen zu unterstützen,
d. eine Datenschutzfolgenabschätzung durchzuführen und ggf. vor Verarbeitung die zuständige Aufsichtsbehörde zu konsultieren zu erfüllen.

6. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in den Art. 24-36 DSGVO niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen – die vom Auftraggeber oder einem von diesem beauftragten Prüfer ermöglichen und dazu beitragen.

7. Der Auftragnehmer teilt dem Auftraggeber zudem unverzüglich Störungen, Verstöße gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie einen 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 34 DSGVO.

8. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung dieser Pflichten angemessen unterstützen.

9. Ist der Auftragnehmer der Auffassung, dass eine vom Auftraggeber erteilte Weisung gegen gesetzliche Vorschriften verstößt, wird er den Auftraggeber unverzüglich darüber informieren. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisungen solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten

11. Datenschutzbeauftragter des Auftragsverarbeiters ist auf der Seite. www.kab-maklerservice.de unter der Rubrik „Datenschutz“ hinterlegt und jederzeit freizugänglich abrufbar.

§ 7 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.

3. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

4. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung notwendig sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5. Nach Beendigung der Auftragsverarbeitung hat der Auftragnehmer sämtliche in seinem Besitz befindliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände datenschutzgerecht zu vernichten.

§ 8 Technische und organisatorische Maßnahmen

1. Die in der Anlage „Technische und organisatorische Maßnahmen“ beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

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

4. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein und Ausgänge werden dokumentiert.

§ 9 Unterauftragsverhältnisse

1. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer (weiteren Auftragsverarbeiter) hinzuzieht.

2. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

3. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 5 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet.

4. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 36 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Nachfrage vorzulegen.

5. Unterauftragsverhältnisse im Sinne dieses Vertrages sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistungen 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.

6. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsdatenverarbeiter) beauftragen. Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs., 2-4 DSGVO zwischen Auftragnehmer und Unterauftragnehmer.

7. Eine Liste der Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten und deren Umfang wird auf Wunsch zur Verfügung gestellt.

§ 10 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 grundsätzlich als Gesamtschuldner (Art. 82 DSGVO), der Auftragnehmer jedoch nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der EU-DSGVI nicht nachgekommen ist oder unter Nichtbeachtung rechtmäßig erteilter Anweisungen des Auftraggebers oder gegen solche Anweisungen gehandelt hat.

2. Sollte der Auftragnehmer oder ein Subunternehmer (weiterer Auftragsverarbeiter) aufgrund der Umsetzung einer Weisung des Auftraggebers (einschließlich der im Vertrag vereinbarten) von einem Betroffenen mit der Behauptung in Anspruch genommen werden, das ihm wegen eines Verstoßes gegen die EU-DSGVO ein materieller oder immaterieller Schaden entstanden ist, oder eine Aufsichtsbehörde infolgedessen eine Geldbuße gegen den Auftragnehmer oder einen Subunternehmer verhängen oder androhen, stellt der Auftraggeber den in Anspruch Genommenen vollumfänglich von einer solchen Inanspruchnahme frei. Der Freistellungsanspruch umfasst dabei auch die angemessenen Kosten der Rechtsverteidigung. Entsprechendes gilt, wenn die Inanspruchnahme auf deine Verletzung der vertraglichen oder gesetzlichen Pflichten des Auftraggebers zurückzuführen ist.

§ 11 Sonstiges

- Beider Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von technischen und organisatorischen Maßnahmen, Prozess- und Produktbeschreibungen, Verarbeitungsverfahren, technischen Schnittstellen, Zugangsinformationen, 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.

- Für Nebenabreden ist die Schriftform erforderlich.

§ 12 Salvatorische Klausel

1. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen des Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

2. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

3. Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

4. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 15 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der personenbezogenen Daten im Sinne dieses Vertrages am besten gewährleistet.

§ 13 Rechtswahl, Gerichtsstand

Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag gilt das deutsche Recht, Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen: Technische und organisatorische Maßnahmen

Unterschriften

KAB Maklerservice GmbH

Kolumbusstraße 31

53881 Euskirchen

Anlage 1 Technische und organisatorische Maßnahmen
Präambel:

Dieser Anhang konkretisiert die im Vertrag zur Auftragsverarbeitung getroffenen technischen und organisatorischen Maßnahmen. Dabei werden in diesem Zusammenhang insbesondere der aktuelle Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung berücksichtigt.

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

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst die folgenden Maßnahmen:

- Türsicherung (elektrische Türöffner usw.)
- Gebäudesicherung (Zäune, Pforten)
- Alarmsicherung
- Manuelles Schließsystem und Sicherheitsschlösser, Türen mit Knauf Außenseite
- Schlüsselverwaltung / Dokumentation der Schlüsselvergabe
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen
- Datenträgern
- Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst
- die folgenden Maßnahmen:
- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des
- Kennworts)
- Software Firewall
- Hardware Firewall
- Anti-Viren Software
- Persönlicher und individueller User-Log-In bei Anmeldung am System
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Webapplication-Firewall
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Single Sign-on auf Website
- Protokollierung des Zugangs
- Login mit Benutzername + Passwort
- Endpoint-Security-Systeme (z. B. Schutz von externen Schnittstellen (USB)) inkl.
- Versiegelung
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Maßnahmen:

Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Maßnahmen zur Trennungskontrolle:

Separierung von Datenbanken
Logische bzw. technische Trennung von Daten
Benutzerprofile / Trennung von Nutzerkonten
Unterschiedliche Zugriffsberechtigungen

Es findet eine Pseudonymisierung von Datensätzen statt. Dies umfasst die folgenden Maßnahmen:

- Eine Pseudonymisierung findet nicht statt

Integrität (Art. 32 Abs. 1 b DS-GVO)
Es findet eine Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt. Dies umfasst die folgenden Maßnahmen:

- Verschlüsselung
- Verschlüsselung von E-Mails bzw. E-Mail Anhängen
- Gesicherter Filetransfer per SFTP
- Gesicherter Datentransport per SSL (HTTPS)
- Verschlüsselung von externen Festplatten
- Paßwortgesichertes WLAN
- Fernwartungskonzept mit Verschlüsselung und Einmal-Paßwort
- Regelung zum Umgang mit mobilen Speichermedien
- Getunnelte Datenfernverbindungen (VPN = Virtuelles privates Netzwerk)
- Data Loss Prevention System

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt. Dies umfasst die folgenden Maßnahmen:

- Dokumentenmanagement,Dokumentenlenkung
- Zugriffsrechte
- Systemseitige Protokollierung

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b DS-GVO) Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:

- Backup-Strategie (offline)
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Überspannungsschutz
- Schutz vor Diebstahl
- Virenschutz / Firewall
- Aufbewahrungsprozess für Back-ups (brandgeschützter Safe)
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Feuerlöscher Serverraum im Bürobetrieb
- klimatisierter Serverraum
- Redundante, örtlich getrennte Datenaufbewahrung
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Schutzsteckdosenleisten Serverraum
- Getrennte Partitionen für Betriebssysteme und Daten

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgende Maßnahmen gewährleistet:

- Notfallmanagement inkl. Notfallpläne

Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DS-GVO). Folgende Maßnahmen wurden getroffen:

- Einfache Datenlöschung (ohne Überschreiben)
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- Entmagnetisierung von physischen Datenträgern (Festplatten /
- Datenbändern) Sorgfältige Auswahl von Entsorgungsdienstleistern

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz. Dies wird durch folgende Maßnahmen unterstützt:

- Datenschutz-Management
- Regelmäßige Datenschutzschulungen der Mitarbeiter
- Auftragskontrolle für Auftragsverarbeiter (AV)

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Interne Verhaltensregeln
- Auftragskontrolle für Auftragsverarbeiter (AV)