Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

zwischen

- nachstehend Auftraggeber genannt-

und dem Auftragsverarbeiter

Finance Key Systems GmbH & Co. KG
Franziskanerhof
Uhlstraße 19 -23
50321 Brühl

- nachstehend Auftragnehmer genannt-

1. Gegenstand / Leistungsumfang

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst folgende Tätigkeiten, die sich aus der Leistungsbeschreibung und der Nutzung bereitgestellter Dienste und Anwendungen des Auftragnehmers ergeben:

Softwarelösungen
Die Vereinbarung umfasst die komplette Softwarepalette von Finance Key Systems. Eine Liste der Softwaremodule kann auf der Webseite des Auftragnehmers eingesehen werden. (www.financekey.de)

Maklerhomepage, Lead Schnittstellen, Bonitätsprüfung, Schnittstellen zu Versicherungsunternehmen
Bei der Nutzung dieser Anwendungen werden sämtliche Daten übertragen, die für die Erfüllung der vereinbarten Dienstleistungen notwendig sind. Diese Daten werden im Rechenzentrum des Auftragnehmers verarbeitet und gespeichert.

Rechenkerne von Gesellschaften
Für die Bereitstellung von aktuellen Tarifinformationen werden die von der jeweiligen Gesellschaft festgelegten Daten an einen Server der Gesellschaft zum Zwecke der Berechnung, Angebots- und Antragsstellung übertragen.

Dokumentenservices
Bei der Nutzung von BiPRO Dokumenten Anwendungen werden Dokumente für Kunden des Auftraggebers über einen Abholdienst gesammelt und bis zur Abholung des Auftraggebers im Rechenzentrum des Auftragnehmers aufbereitet und zwischengespeichert.

Migrationsprojekte
Bei Migrationsprojekten werden Kundendaten verarbeitet und gespeichert.

FK-Software GmbH
Zur Bereitstellung der Dienste für den Auftraggeber werden an diese Firmen Daten übermittelt.
Diese Firmen nutzen die gleiche Servertechnologie und greifen auf das gleiche IT Personal zurück.

Support
Bei Supportanfragen an den Auftragnehmer aufgrund einer Frage zu einem konkreten Vorgang
(zum Beispiel Störungen bei der Schnittstellennutzung) werden ggf. personenbezogene Daten verarbeitet.

2. Dauer
Diese Vereinbarung gilt ab dem 10.05.2018 und kann von beiden Parteien mit einer Frist von 3 Monaten gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Alle anderen ggf. bestehenden Vereinbarungen werden hierdurch ersetzt.

3. Kategorien betroffener Personen
- Interessenten
- Versicherungsnehmer
- mitversicherte Personen
- Kontoinhaber
- Vermittlerdaten
- Vermittler-Mitarbeiterdaten
- Vermittler-Untervermittlerdaten
- weitere Geschäftspartner

4. Art der Daten
- Kundendaten (Name, Vorname, Geburtsdatum, Geschlecht, Anschrift)
- Kommunikationsdaten
- Zahlungsdaten
- Risikodaten zum Versicherungsvertrag
- Gesundheitsdaten
- Schadendaten
- Vermittlerabrechnungs-, Beitragsberechnungs-, Zahlungs- und Mahndaten
- Benutzerkennungen, Lizenzdaten
- Internetnutzungs- und Kommunikationsdaten
- Pflichtauskunftsangaben von Dritten (z.B. Vorversicherer, Bonität)

5. Zweck der Verarbeitung
- Verwaltung bestehender Verträge
- Schadenbearbeitung
- E-Mail Kommunikation
- Support
- Kalender- und Terminverwaltung
- Erstellung von Courtageabrechnungen
- Erstellung von Statistiken
- Webauftritt / Betrieb einer Internetseite
- Verarbeiten und Speichern von Dokumenten

6. Örtlichkeit
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers

7. Technisch-organisatorische Maßnahmen
Der Auftragnehmer trifft für seinen Verantwortungsbereich die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten. Alle TOMs unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, adäquate Maßnahmen zur Erhöhung des Sicherheitsniveaus umzusetzen. Die Maßnahmen und wesentliche Änderungen werden dokumentiert.

8. Auskunft, Berichtigung, Einschränkung und Löschung von Daten
Der Auftragnehmer darf Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers oder einer betroffenen Person berichtigen, löschen oder deren Verarbeitung einschränken.
Soweit vom Leistungsumfang umfasst, ist Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft unmittelbar durch den Auftragnehmer sicher zu stellen.

9. Qualitätssicherung und sonstige Pflichten des Auftragnehmers
Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieses Auftrages gesetzlichen Pflichten gemäß Art. 28-33 DSGVO zu wahren. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Dessen aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit allen für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

c) Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

f) Der Auftragnehmer unterstützt den Auftraggeber nach besten Kräften, wenn dieser Kontrollen, Haftungsansprüchen oder einem anderen Anspruch im Zusammenhang mit dieser Vereinbarung ausgesetzt ist. Der Auftraggeber ist zur Übernahme der daraus entstehenden Mehrkosten verpflichtet.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen.

h) Sollten Daten beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.

Der Auftragnehmer ist außerdem verpflichtet alle Verantwortlichen darüber zu informieren, dass Eigentum und Hoheit an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DSGVO liegen.

10. Pflichten des Auftraggebers
Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO und insoweit zur Umsetzung der gesetzlichen Vorschriften verpflichtet:

a) Der Auftraggeber ist alleine für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Auftraggeber trägt Sorge, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
b) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

11. Unterauftragsverhältnisse
Als Unterauftragsverhältnisse im Sinne dieser Regelung 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-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von
Dokumenten und 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 Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

a) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen.
Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zwischen Auftragnehmer und Unterauftragnehmer.

b) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

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

12. Kontrollrechte des Auftraggebers
Der Auftragnehmer gestattet dem Auftraggeber oder einem Bevollmächtigten, sich nach Anmeldung zu Prüfzwecken in den Betriebsräumen
zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze zu überzeugen.

Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er z.B. bei der Prüfung von Ergebnissen Fehler oder Unregelmäßigkeiten feststellt. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

13. Mitteilung bei Verstößen
Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.:

a) Sicherstellung eines angemessenen Schutzniveaus, das Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigt und eine Feststellung von relevanten Verletzungsereignissen ermöglicht.
b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
c) Den Auftraggeber im Rahmen seiner Informationspflicht gegenüber Betroffenen zu unterstützen.
d) Den Auftraggeber für dessen Folgeabschätzung zu unterstützen.
e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

14. Weisungsbefugnis des Auftraggebers
Mündliche Weisungen bestätigt der Auftraggeber unverzüglich, mindestens in Textform.
Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, dass eine Weisung gegen geltendes Recht verstößt. Der Auftragnehmer ist zur Aussetzung der Weisung berechtigt, bis sie geändert oder bestätigt wird.

15. Löschung und Rückgabe von personenbezogenen Daten
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.

Nach Beendigung der Auftragsdatenverarbeitung hat der Auftragnehmer sämtliche in seinem Besitz befindliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände datenschutzgerecht zu vernichten, soweit dem keine gesetzlichen Pflichten entgegenstehen. Das Protokoll der Löschung ist auf Anforderung vorzulegen

16. Schlussbestimmungen / salvatorische Klausel
a) Der Auftragnehmer ist verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus, Stillschweigen über alle in diesem Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.

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

c) 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.

d) 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.
e) Existieren mehrere wirksame und durchführbare Bestimmungen, so muss die Bestimmung gewählt werden, welche den Schutz der personenbezogenen Daten im Sinne dieses Vertrages am besten gewährleistet.

17. Rechtswahl, Gerichtsstand

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

	Brühl, den
.	Finance Key Systems GmbH & Co. KG

Technische und organisatorische Maßnahmen (TOM)

Finance Key Sytems GmbH & Co. KG, Uhlstrasse 19-23, 50321 Brühl

Maßnahmen zur Vertraulichkeit

Beschreibung der Zutrittskontrolle/Zugangskontrollen:
Die physikalische Speicherung erfolgt bei Hosting über Financekey durch den Service Provider STRATO AG (www.strato.de) und 1blu AG (www.1blu.de) Auf Wunsch können hier die Vereinbarung von Financekey und Strato AG sowie Financekey und 1blu AG zugesendet werden.

Beschreibung der Zugriffskontrolle:
Erstellen und Einsatz eines Berechtigungskonzepts
Sichere Löschung von Datenträgern vor deren Wiederverwendung
Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
Sichere Aufbewahrung von Datenträgern

Beschreibung der Weitergabekontrolle:
E-Mail-Verschlüsselung mit S/MIME Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen

Beschreibung des Trennungsgebots:
Logische Mandantentrennung (softwareseitig)
Trennung von Produktiv- und Testsystem
Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Beschreibung der Pseudonymisierung:
Trennung von Kontaktdaten und anderen Daten
Trennung von Kundenstammdaten und Auftragsdaten
Weitere Pseudonymisierung findet nicht statt

Beschreibung der Verschlüsselung:
Verschlüsselte Datenübertragung (E-Mailverschlüsselung nach TLS oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels SSL/SFTP)

Maßnahmen zur Integrität

Beschreibung der Eingabekontrolle:
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
Protokollierung der Eingabe, Änderung und Löschung von Daten
Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

Maßnahmen zur Verfügbarkeit und Belastbarkeit

Beschreibung der Verfügbarkeitskontrolle:
Einsatz von Antivirensoftware
Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Erstellen eines Backup- & Recoverykonzepts
Feuer- und Rauchmeldeanlagen
Erstellung und Anwendung von IT-Notfallplänen
Redundante Datenhaltung (RAID System, zusätzlich Backup an einen anderen Ort und nochmaliges Backup auf einen verschlüsselten Server im Rechenzentrum)
Schutzsteckdosenleisten in Serverräumen
Unterbrechungsfreie Stromversorgung (USV)

Beschreibung der raschen Wiederherstellbarkeit:
Regelmäßige und dokumentierte Datenwiederherstellungen
IT-Notfallpläne und Wiederanlaufpläne

Weitere Maßnahmen zum Datenschutz

Beschreibung der Auftragskontrolle:
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO
Benennung eines Datenschutzbeauftragten
Schulungen aller zugriffsberechtigten Mitarbeiter
Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

Beschreibung des Managementsystems zum Datenschutz:
Durchführung regelmäßiger interner Audits
Einsatz von softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis, tool.dsgvo-vorlagen)