Ergänzung zum bestehenden Vertragsverhältnis:

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

F&I Makler GmbH & Co. KG

Schwanseestr. 29
99423 Weimar
MAK75737

nachstehend „Auftraggeber“ oder „AG“ genannt

und

Fonds Finanz Maklerservice GmbH
Riesstraße 25
80992 München

nachstehend „Auftragnehmer“ oder „AN“ genannt

Gegenstand dieser Vereinbarung und Dauer

1.1 Der Auftraggeber (kurz: „**AG**“) hat den Auftragnehmer (kurz: „**AN**“) anderweitig vertraglich („Vertrag“) mit der Erbringung verschiedener IT-Leistungen (auch kurz: **„Services“**) beauftragt. Die hiesige Vereinbarung („**AV-Vereinbarung**“) ergänzt den Vertrag um Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO. Die genaue Bezeichnung des Vertrages findet sich in **Anlage 1** zur hiesigen AV-Vereinbarung.

1.2 Soweit der AN im Rahmen der Leistungserbringung (1) personenbezogene Daten, die er vom AG erhält (kurz: **„Daten“**) verarbeitet und/oder (2) mit der Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen des AG beauftragt ist, bei der für den AN die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, erfolgt dies ausnahmslos im Auftrag des AG und im Sinne einer Auftragsverarbeitung nach Art. 28 DSGVO (kurz: **„AV“**).

1.3 Der AG bleibt insofern datenschutzrechtlich Verantwortlicher, d.h. „Herr der Daten“ und im Verhältnis zu den Betroffenen für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

1.4 Die hiesige AV-Vereinbarung regelt die Details der AV gemäß Art. 28 und Art. 29 DSGVO und geht betreffend der Verarbeitung der Daten durch den AN allen anderen Regelungen zwischen den Parteien vor. Sie ersetzt betreffend der Verarbeitung der Daten im Auftrag zugleich alle gegebenenfalls bestehenden älteren AV-Vereinbarungen (inklusive ab 25.05.2018 auch bisherige ADV-Vereinbarungen nach § 11 BDSG).

1.5 Als Beginn dieser AV-Vereinbarung wird der 25.05.2018 vereinbart. Dauer, Ende und Kündigungsmöglichkeiten der AV-Vereinbarung entsprechen denjenigen des Vertrags. Soweit es dort dazu keine Regelungen gibt, gilt das Folgende: Die Auftragsverarbeitung läuft unbefristet; sie kann von beiden Parteien mit einer Frist von 14 Tagen zum Ende eines Monats schriftlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

1.6 Soweit der AG betreffend der Daten nicht selbst der datenschutzrechtlich Verantwortliche ist, sondern eine andere Stelle (zum Beispiel, wenn der AG den hiesigen AN als Unterauftragnehmer einschaltet), sichert der AG zu, dass er berechtigt ist, betreffend der Daten die hiesige AV-Vereinbarung mit dem AN abzuschließen.

2. Einzelheiten zur Datenverarbeitung durch den AN im Auftrag des AG

2.1 Die datenschutzrechtlichen Details betreffend der vom AN zu erbringenden Services sind in **Anlage 1** dergestalt festgelegt, dass dort für jeden Service beschrieben ist

(1) Gegenstand, Art und Zweck der im Rahmen der Serviceerbringung erfolgenden Verarbeitung von personenbezogenen Daten,

(2) der Art der dabei verarbeiteten personenbezogenen Daten und

(3) die jeweiligen Kategorien der von dieser Datenverarbeitung Betroffenen.

2.2 Der AN verarbeitet die Daten ausschließlich im Rahmen dieser AV-Vereinbarung, insbesondere im Umfang nach den relevanten Vorgaben der **Anlage 1**, sowie etwaiger dokumentierter Einzelweisungen des AG nach Ziffer 2.3; Abweichungen sind nicht zulässig.

Zu anderen Verarbeitungen der Daten ist der AN insofern nur berechtigt, soweit er hierzu nach dem Recht der EU oder des EU-Staats, dem er unterliegt, gesetzlich verpflichtet ist; in einem solchen Fall teilt der AN diese rechtlichen Anforderungen dem AG vor der Verarbeitung schriftlich mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Mit Ausnahme vorstehend gesetzlicher Verpflichtungen darf der AN die Daten nicht zu anderen, insbesondere nicht zu eigenen Zwecken verwenden und keine Kopien oder Duplikate hiervon anfertigen.

2.3 Einzelweisungen des AGs müssen sich im Rahmen des vertraglich vereinbarten Leistungsumfangs halten. Einzelweisungen hat der AG schriftlich zu erteilen. Bei Gefahr in Verzug kann der AG eine Einzelweisung auch mündlich erteilen, der AG hat diese im Anschluss unverzüglich in Schriftform zu bestätigen. Der AN wird den AG unverzüglich informieren, wenn eine Einzelweisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. Der AN ist dann berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AG nach Überprüfung bestätigt oder geändert wird.

2.4 Der AN darf und muss die Daten nur auf Einzelweisung des AG oder soweit dies Teil der Leistung nach **Anlage 1** berichtigen, löschen oder deren Datenverarbeitung einschränken.

2.5. Sollte sich ein Betroffener wegen einer datenschutzrechtlichen Auskunft oder anderer ihm zustehenden Betroffenenrechte unmittelbar an den AN wenden, hat der AN den AG darüber unverzüglich zu informieren und vor jeglicher weiterer Tätigkeit und Kommunikation dessen Einzelweisung abzuwarten.

2.6. Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Personen vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch im Anschluss in geeigneter Weise zur Vertraulichkeit und dazu verpflichtet hat, die Daten nicht unbefugt zu verarbeiten.

2.7 Der AN kontrolliert bei sich die Einhaltung der datenschutzrechtlichen Vorschriften durch die jeweiligen Mitarbeiter sowie die Erfüllung der Pflichten aus dieser AV-Vereinbarung. Er weist dem AG auf dessen Aufforderung vorgenommene Kontrollen nach.

2.8 Der AN erstattet dem AG betreffend der Daten des AG unverzüglich ab Kenntnis schriftlich und unter Angabe von Details Meldung bei

(1) Verdacht auf Verletzungen des Datenschutzes der Daten,

(2) Verstöße gegen Datenschutz-Vorschriften oder gegen die im Auftrag getroffenen Festlegungen,

(3) Abweichungen der technischen und organisatorischen Maßnahmen des AN von den mit dem AG vereinbarten Anforderungen,

(4) Anfragen, Kontrollhandlungen, Untersuchungen oder anderen Maßnahmen einer Aufsichtsbehörde für den Datenschutz oder einer anderen Behörde (z.B. Polizei oder Gericht) beim AN.

Der AN unterstützt den AG bei seinen Pflichten nach Art. 33 und 34 DSGVO auf dessen Aufforderung und Kosten angemessen, wie zum Beispiel indem der AN dem AG sachkundige Ansprechpartner zur Seite stellt, relevante Unterlagen zugänglich machen oder Fragen des AG beantworten.

Meldungen nach Art. 33 oder 34 DSGVO für den AG darf und muss der AN nicht vornehmen.

2.9 Meldungen des AN nach Ziffer 2.8. enthalten

(1) eine Beschreibung der Art der Verletzung oder Abweichung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen Datensätze;

(2) eine Beschreibung der wahrscheinlichen Folgen der Verletzung oder Abweichung; und

(3) eine Beschreibung der vom AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, Abweichung oder Unregelmäßigkeit und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2.10 Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten (**„DSB“**) des AN sind in **Anlage 2** festgelegt. Ein Wechsel des DSB oder sonstige Änderungen der Angaben in **Anlage 2** hat der AN dem AG unverzüglich in Schriftform mitzuteilen.

2.11 Der AN unterstützt betreffend der Daten des AG den AG auf dessen Aufforderung und Kosten mit geeigneten technischen und organisatorischen Maßnahmen, den Betroffenenrechte nach Art. 12 bis 23 DSGVO nachzukommen sowie bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten des AG hinsichtlich der Sicherheit personenbezogener Daten sowie einer ggf. erforderlichen Datenschutz-Folgenabschätzung und vorherigen Konsultationen der Aufsichtsbehörden. Der AN hat dem AG darüber hinaus auf dessen Anforderung alle Auskünfte und Informationen zur Verfügung zu stellen, die der AG zur Erfüllung sonstiger ihn treffender gesetzlichen Vorgaben benötigt (etwa zur Erstellung des Verzeichnisses von Verarbeitungstätigkeiten).

3. Ort der Datenverarbeitung durch den AN

3.1 Der AN verarbeitet die Daten in einem Mitgliedsstaat der Europäischen Union (EU) oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR); maßgeblich ist dabei der Status des Landes im Zeitpunkt der jeweiligen Verarbeitung.

3.2 Soweit der AN (siehe zu Unterauftragnehmern Ziffer 4.) dagegen die Daten nicht im Gebiet der EU/ EWR verarbeitet oder von außerhalb dieses Gebiets auf die Daten zugreift, ist dies zulässig, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind.

4. Einschaltung von Unterauftragnehmern

4.1 Der AN darf sich bei der Leistungserbringung Unterauftragnehmern bedienen.

4.2 Die aktuell vom AN eingesetzten Unterauftragnehmer sind in **Anlage 3** genannt. Mit diesen besteht seitens des AG Einverständnis.

Falls der AN einen Unterauftragnehmer ersetzen oder einen zusätzlichen Subunternehmer einschalten möchte, wird der AN den AG darüber informieren. Der

AG ist sodann berechtigt, binnen dreißig (30) Tagen nach Erhalt der Mitteilung gegen die Unterbeauftragung Einspruch beim AN einzulegen, was schriftlich erfolgen muss. Erfolgt dies nicht, hat der AG den jeweiligen Unterauftragnehmer genehmigt. Erfolgt dagegen ein Einspruch und liegen für diesen nachvollziehbare Gründe vor, wird der AN wirtschaftlich sinnvolle Anstrengungen unternehmen, um die Leistung zu erbringen, ohne den neuen Unterauftragnehmer einzuschalten. Ist ihm dies nicht möglich, ist der AG berechtigt, den Teil der AV-Vereinbarung, der durch den betroffenen Unterauftragnehmer erbracht wird, durch schriftliche Mitteilung an den AN unter Einhaltung einer Frist von 14 Tagen außerordentlich zu kündigen.

Alternativ kann der AN dem AG einen anderen Unterauftragnehmer vorschlagen; für diesen Fall gelten die Regelungen des vorstehenden Unterabsatzes entsprechend.

Nach vorstehenden Regelungen zulässige Unterauftragnehmer hat der AN in die **Anlage 3** aufzunehmen und dem AG als aktualisierte Fassung zu übersenden.

4.3 Soweit Unterauftragnehmer mit Sitz außerhalb der EU bzw. des EWR eingeschaltet werden, muss der AN die Voraussetzungen der Art. 44 bis 49 DSGVO einhalten. Soweit der AG aufgrund aktueller Datenschutzvorgaben, insbesondere der deutschen Datenschutzbehörden, dazu Standarddatenschutzklauseln direkt mit dem Subunternehmer abzuschließen hat und der AN dazu seinen Betritt erklären muss, unterstützt der AN den AG dabei und der AG wird die EU-Standardvertragsklauseln entsprechend abschließen.

4.4 Der AN hat seine Verträge mit Unterauftragnehmer so zu gestalten, dass sie datenschutzrechtlich mindestens den Datenschutzbestimmungen der hiesigen AV-Vereinbarung und Art. 28 entsprechen.

4.5 Der AN ist verpflichtet, die Einhaltung der Pflichten bei den Unterauftragnehmern zu prüfen.

4.6 Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der AN gegenüber dem AG für die Einhaltung der Pflichten jenes Unterauftragnehmers wie für eigene Pflichtverletzungen.

4.7 Die Weiterleitung von Daten an Unterauftragnehmer oder deren Zugriff darauf ist erst dann zulässig, wenn der AN die Voraussetzungen nach dieser Vereinbarung geschaffen hat.

5. Vom AN getroffene technische und organisatorische Schutzmaßnahmen

5.1 Der AN hat die Sicherheit der Verarbeitung gem. Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen.

5.2 Das in **Anlage 4** beschriebene Datenschutzkonzept legt die Auswahl der vom AN getroffenen technischen und organisatorischen Maßnahmen (kurz: „**TOMs**“) fest. Der AG hat diese vor Unterzeichnung dieser Vereinbarung geprüft und als passend zum von ihm ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik beurteilt. Der AN ist verpflichtet, die TOMs während der Laufzeit dieser AV-Vereinbarung aufrecht zu erhalten.

5.3 Im Rahmen des technischen Fortschritts und der Weiterentwicklung ist es dem AN gestattet, einzelne TOMs anzupassen, soweit es sich um adäquate Maßnahmen handelt und zugleich das Sicherheitsniveau der in **Anlage 4** festgelegten TOMs nicht unterschritten wird. Auf Aufforderung des AG informiert der AN den AG über solche Änderungen.

6. Kontrollen des AG

6.1 Der AN erklärt sich damit einverstanden, dass der AG berechtigt ist, im erforderlichen Umfang die Einhaltung der Vorschriften über den Datenschutz, dieser AV-Vereinbarung samt ihrer Anlagen, insbesondere auch der vereinbarten TOMs nach **Anlage 4,** selbst oder durch Dritte zu kontrollieren, insbesondere durch Einholung von Auskünften sowie Kontrollen beim AN vor Ort. Kontrollen vor Ort haben zu den Geschäftszeiten des AN zu erfolgen und sind 2 Wochen vorab anzukündigen. Der AG wird bei Vor-Ort-Kontrollen auf die betrieblichen Abläufe des AN Rücksicht nehmen und dessen Betriebsablauf nicht stören.

Der AG ist verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des AN vertraulich zu behandeln; Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6.2 Der AN sichert zu, dass er, soweit erforderlich, bei Kontrollen des AG jeweils mitwirkt und den AG unterstützt, ihm insbesondere Zutritt gewährt sowie Unterlagen zur Verfügung zu stellt (Protokolle, Berichte des Datenschutzbeauftragten, Zertifizierungen, etc.).

6.3 Die Kosten von Kontrollen trägt vollständig der AG.

7. Beendigung der AV

7.1 Soweit im Vertrag vereinbart, hat der AN dem AG dessen Daten in einem für den AG lesbaren gängigen elektronischen Format herauszugeben, ansonsten auf gesonderte Einzelweisung diese Daten bei sich physikalisch zu löschen. Vorstehende Regelungen gelten entsprechend für personenbezogenes Test- und Ausschussmaterial.

7.2 Dokumentationen des AN, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung durch den AN dienen, sowie Unterlagen, die gesetzlichen Aufbewahrungspflichten des AN unterliegen, sind im jeweils erforderlichen Umfang von vorstehenden Regelungen ausgenommen.

8. Haftung und wechselseitige Information

8.1 Soweit im Zusammenhang mit der nach dieser AV-Vereinbarung erfolgenden Datenverarbeitung gegen AN oder AG Schadensersatzansprüche (Art. 82 DSGVO), Geldbußen (Art. 83 DSGVO) oder andere Sanktionen (Art. 84 DSGVO) angedroht oder geltend gemacht werden, haben sich AN und AG darüber jeweils unverzüglich wechselseitig zu informieren. Ohne vorherige Abstimmung mit der jeweils anderen Partei darf die jeweils betroffene Partei keine Stellungnahmen sowie kein Anerkenntnis oder eine vergleichbare Erklärung abgeben; werden sich AN und AG betreffend der Art und Weise der Abwehr nicht einig, liegt das Letztentscheidungsrecht beim AG als „Herr der Daten“. Zudem haben sich beide Parteien bei der Anspruchsabwehr zu unterstützen.

8.2 AG und AN haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

Der AN haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus der DSGVO resultierenden und speziell für AN auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AG handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des AG gehandelt hat.

Soweit der AG zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den AN vorbehalten.

Im Innenverhältnis zwischen AG und AN haftet der AN für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

- seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
- unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AG
- oder gegen diese Anweisungen gehandelt hat.

Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

8.3 Die Haftung des AN ist im Übrigen auf Vorsatz und grobe Fahrlässigkeit beschränkt. Vorstehende Einschränkungen gelten nicht im Falle der Verletzung des Lebens, des Körpers oder der Gesundheit oder bei der Verletzung von wesentlichen Rechten und Pflichten, die sich aus der Natur des Vertrages ergeben (Kardinalpflichten). In diesem Fall ist die Haftung der Höhe nach auf den typischerweise vorhersehbaren Schaden begrenzt.

9. Sonstige Bestimmungen

9.1 Die Einrede des Zurückbehaltungsrechts nach § 273 BGB an den Daten, Teilen davon sowie Datenträgern des AG wird ausgeschlossen.

9.2 Soweit die Daten beim AN durch Beschlagnahme oder Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der AN den AG unverzüglich darüber zu informieren. Der AN hat alle in diesem Zusammenhang Beteiligten zu informieren, dass ausschließlich der AG Verantwortlicher und „Herr der Daten“ ist.

9.3 Gesetzliche Regelungen im Sinne dieser AV-Vereinbarung umfassen auch Verordnungen der EU.

9.4 Soweit im kommerziellen Vertrag ein Gerichtsstand vereinbart wurde, gilt diese Vereinbarung auch für alle Ansprüche oder Angelegenheiten, die sich aus oder im Zusammenhang mit dieser AV-Vereinbarung ergeben.

9.5 Sollten einzelne Teile dieser AV-Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der AV-Vereinbarung im Übrigen nicht.

10. Anlagen

Folgende Anlagen sind verbindlicher Teil dieser AV-Vereinbarung:

Anlage 1: Details zum Auftragsverarbeitungsvertrag

Anlage 2: Angaben zum DSB des AN

Anlage 3: Liste von genehmigten Unterauftragnehmern

Anlage 4: Beschreibung der vom AN zum Schutz der Daten des AG getroffenen technischen und organisatorischen Maßnahmen

24.05.2018 10:34:14

Auftraggeber

F&I Makler GmbH & Co. KG

Auftragnehmer

Norbert Porazik **Markus Kiener**

Geschäftsführer
Fonds Finanz Maklerservice GmbH

ANLAGE 1: Details zum Auftragsverarbeitungsvertrag

1. Tabelle zu den Services

Lfd. Nr.	**Kurzbeschreibung der Leistungen/ Services, die der AN für den AG erbringt** **(In Kurzform)**	**Gegenstand, Art und Zweck der diesbezüglichen Verarbeitung von personenbezogenen Daten** (welche Leistungen betreffend die personenbezogenen Daten sind im Einzelnen zu erbringen: Erheben? Speichern? Übermitteln? Wie? Etc.)	**Speichert der AN bei sich die Daten des AG?**	**Kreis der Betroffenen** **(=die Personengruppen, deren Daten verarbeitet werden)** (Beispiele: Mitarbeiter des AG, Endkunden des AG, Azubis des AG, etc.)	**Art der personenbezogenen Daten, die der AN erhält/ verarbeitet** (=Kategorie der Daten, wie etwa „Adressdaten“ oder „Bestelldaten“, etc.	**Ort (Stadt/ Land), an dem der AN die Daten verarbeitet**
1	Vergleichsrechner - Versicherung	Verarbeitung von personenbezogenen Daten des Kunden des Vermittlers um Versicherungsvergleiche zu erstellen	Speicherung erfolgt beim Unterauftragnehmer SOFTFAIR GmbH	Daten von Kunden des AG	Je nach von Kunden gewähltem Produkt: • Stammdaten, • Adressdaten, • Kontakt-/Kommunikationsdaten, • Familienstand, • Gesundheitsdaten inkl. persönlicher Merkmale, • Daten zu Ausbildung und Beruf, • Kontodaten, • Daten von zu versichernden oder finanzierenden Gegenständen/ Objekten, • Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), • Kundenhistorie, • Planungs- und Steuerungsangaben, • Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)	Hamburg
2	Customer-Relation-Mana	AG gibt alle für seinen Vermittlungs-, Betreuungs-	Ja	Daten von Kunden des	Je nach vom AG hinterlegten Daten des Endkunden	München,

	gement-System (CRM)	und Verwaltungsauftrag notwendigen personenbezogenen Daten seiner Kunden in das CRM ein.	Für die Software „AkquiseCenter“ erfolgt die Datenverarbeitung durch den Unterauftragnehmer SOFTFAIR GmbH	AG	• Stammdaten, • Adressdaten, • Kontakt-/Kommunikationsdaten, • Familienstand, • Gesundheitsdaten inkl. persönlicher Merkmale, • Daten zu Ausbildung und Beruf, • Kontodaten, • Daten von zu versichernden oder finanzierenden Gegenständen/ Objekten, • Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), • Kundenhistorie, • Planungs- und Steuerungsangaben, • Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)	Hamburg
3	Anlageberatungssoftware	Geführter Investmentberatungsprozess, der AG bei der Vermittlung und Verwaltung von Finanzportfolios unterstützt. Ergebnisse der Beratung werden dem Kunden des AG dargestellt.	Ja	Daten von Kunden des AG	• Stammdaten, • Adressdaten, • Familienstand, Unterhaltsberechtigte, • Kontaktdaten, • Bonitätsdaten (finanzielle Verhältnisse, Gehalt), • Kontodaten, • Depotdaten, • Kenntnisse und Erfahrungen bzgl. Investments(fonds), • Ausweisdaten, • Steuerdaten	München
4	Kfz-Vergleichsrechner	Verarbeitung von personenbezogenen Daten des Kunden des Vermittlers um Versicherungsvergleiche im Bereich KfZ-Versicherung zu erstellen	Speicherung erfolgt beim Unterauftragnehmer NAFI GmbH	Daten von Kunden des AG	• Personenstammdaten der Anwender/Nutzer der Dienstleistung, • Personenstammdaten im Zusammenhang mit Versiche-rungen (z.B. Versicherung-snehmer, versicherte Personen, Fahrzeughalter, etc., • Kontaktdaten (z.B. Telefon, Telefax, Mobilnummer, E-Mail), • Kommunikationsdaten (z.B. IP-Adressen), • Daten für Tarifierung und Annahmeprüfung (je nach Versicherungssparte z.B. amtl. Kennzeichen, Anschrift des Versicherungsnehmers, etc.), • Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), • Kundenhistorie,	Höxter

					• Vertragsabrechnungs- und Zahlungsdaten (z.B. Bankverbindung)	
5	Gewerbeversicherung-Vergleichsrechner	Verarbeitung von personenbezogenen Daten des Kunden des Vermittlers um Versicherungsvergleiche im Bereich Gewerbeversicherung zu erstellen	Speicherung erfolgt beim Unterauftragnehmer Finanzchef24GmbH	Daten von Kunden des AG	• Stammdaten, • Adressdaten, • Kontodaten, • Daten der zu versichernden Gegenstände / Waren etc., • Vorversicherungsdaten	München
6	Informationsbereitstellung Beteiligungen-/Sachwertebereich	Informationsbereitstellung bzgl. getätigten Anlagen im Beteiligungen-/ Sachwertebereich je Endkunde	Speicherung erfolgt beim Unterauftragnehmer fundsaccess AG	Daten von Kunden des AG	• Stammdaten, • Adressdaten, • Kontodaten, • Vorhandene Anlage/Beteiligung	München
7	Angebotsplattform	Bereitstellung von Vergleichsrechnern; Prüfung und Optimierung eingereichter Anträge; Prüfung, inwieweit die eingereichten Anträge die Annahmerichtlinien der Produktgeber erfüllen; Weiterleitung eingereichter Anträge an Produktgeber	Speicherung erfolgt beim Unterauftragnehmer PROCHECK 24 GmbH	Daten von Kunden des AG	• Persönliche Daten wie Name, Geburtstag und -ort, Familienstand, Berufsgruppe und Nationalität, • Anschrift und Kontaktdaten (Telefon, Email), • Angaben zum Haushalt, • Wohn- bzw. Immobilieneigentum, • Angaben zur beruflichen Tätigkeit, • Angaben zur monatlichen Haushaltsrechnung (Einnahmen, Ausgaben), • Angaben zu ggf. bereits bestehenden Krediten, • Angaben zur aktuellen Kreditanfrage (Summe, Laufzeit, Absicherung), • Aktuelle Bankverbindung, • Angaben zum zu versichernden Fahrzeug, dem Fahrerkreis sowie dem Nutzungsumfang, • Angaben zu Vorverträgen, • Angaben zum Energieverbrauch	München

2. Weisungsberechtigte Funktion auf Seiten des AG

- Bei Einzelvermittler der Inhaber/Vermittler selbst
- bei Juristischen Personen oder Personengesellschaften, der/die Geschäftsführer bzw. Mitglieder des Vorstandes

3. Weisungsempfänger auf Seiten AN

Datenschutzbeauftragter, Mitglieder der Rechtsabteilung im Vertretungsfall

ANLAGE 2: Angaben zur Datenschutz-Organisation des AN

a. Datenschutzbeauftragter

X Beim AN ist ein Datenschutzbeauftragter bestellt (DSB). Name und Kontaktdaten Florian Kölbl, Riesstraße 25, 80992, datenschutz@fondsfinanz.de

O Es ist kein DSB bestellt. Grund _____

b. Verschwiegenheit u.a.

Sind alle Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, über die für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht, zur Verschwiegenheit und dazu verpflichtet, die Daten nicht unbefugt zu verarbeiten.

X Ja O Nein, Grund: _____

c. Datenschutz-Schulungen

In welcher Weise werden die Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, im Datenschutz geschult?

Art der Schulung: X Präsenzschulung X Web-based Training O Sonstiges: _____

Initialschulung bei Einstellung des Mitarbeiters, dazu jährliche Auffrischungsschulungen

ANLAGE 3: Liste von genehmigten Unterauftragnehmern

Werden Unterauftragnehmer eingesetzt? O Nein

X Ja, siehe dann im Folgenden

Soweit Unterauftragnehmer eingesetzt werden, sind diese abschließend in folgender Tabelle aufzulisten; gleiches gilt für Unter-Unterauftragnehmer (usw.):

Lfd. Nr.	Name des Unterauftragnehmers	Anschrift des Unterauftragnehmers	Aufgabe des Unterauftragnehmers (=welche Personenbezogene Daten des AG verarbeitet der Unterauftragnehmer/ hat Zugriff aus welchen Gründen?	Ort, an dem der Unterauftragnehmer die Daten verarbeitet
1	SOFTFAIR GmbH	Albert-Einstein-Ring 15, 22761 Hamburg;	Angebot Vergleichsrechner (siehe Anlage 1, Verfahren 1) und CRM-Software „AkquiseCenter“ (siehe Anlage 1, Verfahren 2)	Hamburg
2	NAFI GmbH	Lütmarser Straße 60, 37671 Höxter	Angebot Vergleichsrechner, Sparte Sachversicherung, Kfz (siehe Anlage 1, Verfahren 4)	Höxter
3	EDISOFT GmbH	Balanstraße 73 / Haus 11, 4.OG, 81541 München	Wartung Software “Advisor’s Studio” – Investmentplattform (siehe Anlage 1, Verfahren 3)	München
4	FINCON UNTERNEHMENSBERATUNG GMBH	Dorotheenstr. 64, 22301 Hamburg	Wartung CRM-Software „VENTA“ (siehe Anlage 1, Verfahren 2)	Hamburg
5	Finanzchef24 GmbH	Hohenlindener Str. 1, 81677 München	Angebot Vergleichsrechner, Sparte Sachversicherung, Gewerbeversicherung (siehe Anlage 1, Verfahren 5)	München
6	Fundsaccess AG	Lyonel-Feininger-Str. 28, 80807 München	Informationsbereitstellung bzgl. getätigten Anlagen im Beteiligungen-/ Sachwertebereich je Endkunde	München

			(siehe Anlage 1, Verfahren 6)	
7	PROCHECK24 GmbH	Landshuter Allee 8, 80637 München	Angebotsplattform für (Raten)Kredit, Girokonto, Tagesgeld, Kreditkarten, Kfz-Versicherungen, Strom, Gas und DSL (siehe Anlage 1, Verfahren 7)	München

ANLAGE 4:

Beschreibung der vom AN zum Schutz der Daten des AG getroffenen technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden nach Art. 32 DSGVO für folgende verantwortliche Stelle getroffen:

Fonds Finanz Maklerservice GmbH

Riesstraße 25

80992 München

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

1. Zutrittskontrolle

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

- Die Büroräume der Fonds Finanz befinden sich in einem Bürokomplex („Hauptgebäude“) mit mehreren Flügeln, in dem jeweils verschiedene Firmen ihre eigenen Büroabschnitte und –räume haben. Über eine Lobby im Hauptgebäude sind sternförmig die einzelnen Flügel und dortigen Räumlichkeiten zu erreichen.
- Die Räume der Fonds Finanz sind über den Zutritt ins Hauptgebäude und die dortige Lobby zu erreichen. Der Zutritt in die Lobby des Hauptgebäudes ist Montag bis Freitag von 06:15 Uhr bis 19:00 Uhr ohne Zutrittskarten möglich, außerhalb dieser Zeiten nur mit einer Zutrittskarte.
- Die Räume der Fonds Finanz sich jeweils für sich genommen in eigenen und abgeschlossenen Bereichen.
  - Der Zutritt zu den Vorräumen der Büroräume der Fonds Finanz im Haus D in der 2. und 4. Etage ist von 07:30 bis 18:30 Uhr offen, außerhalb dieser Zeiten nur mit einer Zutrittskarte möglich.

  - Der Zutritt zu den eigentlichen Bürotrakten im Haus D in allen Stockwerken (2., 4. und 5. Etage) sowie den Räumlichkeiten im Erdgeschoss im Haus A ist ausschließlich über die personalisierten elektronischen Zugangskarten möglich.
  - Besucher werden über die Klingel und dem vom Empfangspersonal oder der Empfangsvertretung zu betätigten elektrischen Türöffner in die 4. Etage hereingelassen. Die Personenkontrolle erfolgt am Eingang des Bürotrakts durch das Empfangspersonal. Alle Besucher werden begleitet.

- Zu den Bürotrakten der Fonds Finanz
  - Die Serverräume sind immer abgeschlossen. Nur besonders ermächtigtes IT-Personal erhält über den elektronischen Schlüssel (Token) Zugang zu den Serverräumen.
  - Die Switchräume sind immer abgeschlossen. Nur besonders ermächtigtes IT-Personal erhält über einen Schlüssel Zugang zu den Switchräumen. Die Schlüssel sind in einem gesicherten Schlüsselkasten aufbewahrt.
  - Die mechanischen Schlüssel zum Bürotrakt sowie für einzelne Räumlichkeiten werden in einem gesicherten Schlüsselkasten abgeschlossen aufbewahrt. Für den Schlüssel zum Schlüsselkasten gibt es eine spezielle Schlüsselregelung.
  - Die Vergabe der elektronischen Zugangskarte an die Mitarbeiter und an das Wach- und Reinigungspersonal erfolgt nach festgelegter Sicherheitsregelung. Der Erhalt und die Vergabe der Zugangskarten wird quittiert und dokumentiert.
  - Das Reinigungspersonal ist sorgfältig ausgewählt und auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung verpflichtet worden.

2. Zugangskontrolle

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

- Der zuständige Administrator richtet für jeden Mitarbeiter ein Benutzerkonto (Userkonto) ein. Der Benutzer (User) meldet sich bei Aufnahme der Arbeit über seine Benutzerkennung (Identifikation) und sein individuell eingerichtetes Passwort (Authentifizierung) am Betriebssystem ein.
- Das Passwort generiert jeder Benutzer selbst bei erstmaliger Anmeldung am System. Das Passwort ist geheim. Es gibt eine Passwort-Richtlinie: Das Kennwort muss regelmäßig gewechselt werden (alle 90 Tage) und mindestens aus einem Großbuchstaben, Kleinbuchstaben, Zahl sowie einem Sonderzeichen bestehen.
- Bei Unterbrechung der Arbeit wird der Bildschirm nach 5 Minuten Wartezeit automatisch gesperrt (Pausenschaltung) und kann nur mit erneuter Identifizierung und Authentifizierung des Benutzers am System überwunden werden.
- Die Benutzeranmeldungen und -abmeldungen werden systemseitig protokolliert. Die Protokolle werden ausgewertet.

- Auf allen Computern und File Servern wird automatisch eine Antiviren Software installiert.
- Alle Computer und alle Server der Fonds Finanz besitzen eine eigene Firewall. Es wird eine gesonderte Spam-Virus-Firewall für E-Mails eingesetzt.
- Der Einsatz von VPN Technologie ist gewährleistet.
- Alle Firmen-Smartphones sowie die Festplatten der Firmen-Laptops werden automatisch beim Einrichten verschlüsselt.
- Auf allen Computern sind die externe Schnittstellen gesperrt. Es gibt nur Lese-Rechte auf USB-Sticks und andere externe Speichermedien. Ausnahmen müssen beantragt werden und werden nach Nutzung erneut gesperrt.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffberechtigung unterliegende Daten zugreifen können, und dass personenbezogener Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert verändert oder entfernt werden können:

- Ein systembedingtes Rollen- und Berechtigungskonzepte ist durch die Zuordnung jedes Benutzers in ein vorbestimmtes Berechtigungsprofil gewährleistet. Über die jeweilige Anmeldung am System mit Benutzerkennung kann nur beschränkt (nach Rollen- und Gruppenzuordnung) auf die Laufwerke, Anwendungen und Dateien zugegriffen werden.
- Die Verwaltung der Benutzerrechte (Active Directory) erfolgt durch die jeweils berechtigten Systemadministratoren
- Alle Zugriffe auf den Server sind nachvollziehbar und protokolliert. Die Protokolle werden ausgewertet.
- Die Anzahl der Administratoren ist auf das Notwendigste reduziert.
- Die Einhaltung organisatorischer Rollen- und Berechtigungskonzepte ist durch die Aufstellung von Kompetenzkatalogen, interne Richtlinien, Rundschreiben und Arbeitsanweisungen gewährleistet.
- Durch Arbeitsanweisung an Mitarbeiter ist eine Regelung/Verbot des Einsatzes privater Datenträger im Unternehmen erfolgt. Es besteht eine allgemeine Richtlinie für die Nutzung von USB-Sticks, externen Festplatten und Smartphones im Unternehmen.
- Unternehmensweit sind Aktenvernichter aufgestellt und per Arbeitsanweisung zu nutzen. Die Entsorgung und Vernichtung erfolgt durch einen zertifizierten Dienstleister.
- Die schriftliche Regelung und Kontrolle externer Wartung und Fernwartung von Datenverarbeitungssytemen erfolgt durch die Erstellung und Protokollierung von Arbeitsscheinen und Wartungsprotokollen.

4. Trennungskontrolle

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

- Die logische Mandantentrennung ist bei allen Systemen gewährleistet. Daten, die für unterschiedliche Mandanten erhoben und gespeichert wurden, werden logisch separat verwaltet und getrennt verarbeitet, indem alle Mandanten dieselben Tabellen in einer einzigen, gemeinsamen Datenbank eines Datenbanksystems nutzen und dabei jeder Datensatz um ein Attribut für den jeweils zutreffenden Mandanten ergänzt wird. Die Applikation realisiert die Trennung, indem sie dieses Attribut auswertet. Die Änderung der Attribute ist nur bei einer entsprechenden Berechtigung möglich.
- Trennung von Produktiv- und Testsystem (Funktionstrennung).
- Festlegung von Datenbankrechten.

5. Pseudonymisierung & Verschlüsselung

- Die E-Mail-Verschlüsselung erfolgt über TLS (Transport Layer Security) Version 1.2.
- Die Kommunikation über externe Datenverbindungen werden erfolgt über ein Virtual Private Network oder über SSL-Verschlüsselung.
- Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

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

1. Weitergabekontrolle

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

- Daten werden nur an festgelegte berechtigte Empfänger weitergegeben.
- Auf funktionstüchtigen Datenträgern werden Daten durch mehrfaches überschreiben oder durch Formatierung des Datenträgers physikalisch gelöscht. Funktionsuntüchtige oder nur einmal beschreibbare Datenträger (CD-ROM, DVD) werden mechanisch zerstört.
- Die Kommunikation über externe Datenverbindungen erfolgt ausschließlich über ein Virtual Privat Network (VPN) Tunnel
- Die Abruf- und Übermittlungsvorgänge im E-Mail Server und im Intranet werden lückenlos dokumentiert. Auf der Datenbank wird jeder Abruf für einen kurzen Zeitraum gespeichert.
- Von Dritten empfangene Datenträger werden vor dem Einsatz einem Sicherheitscheck unterzogen (Viren)
- Die E-Mail-Verschlüsselung erfolgt über TLS (Transport Layer Security) Version 1.2.

2. Eingabekontrolle

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

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts durch den zuständigen und gesondert berechtigten Administrator.
- Formulare und Unterlagen (Daten auf Papier), von denen Daten in automatisierter Verarbeitung übernommen worden sind, werden nach den gesetzlichen Aufbewahrungsfristen archiviert und entsprechend den gesetzlichen Löschfristen vernichtet.
- Protokollierung der Nutzeraktivitäten in den Systemen. Die Protokolle werden ausgewertet.

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

1. Verfügbarkeitskontrolle

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

- In allen Büro- und Serverräumen sind die Brandschutzvorrichtungen eingehalten (Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte).
- Alle Serverräume sind mit Geräten zur Überwachung von Temperatur und Feuchtigkeit, Klimaanlagen, Schutzsteckdosenleisten und unterbrechungsfreier Stromversorgung ausgestattet.
- Die Serverräume sind alarmgesichert. Bei unberechtigten Zutritten zu den Serverräumen erfolgt eine Alarmmeldung. Die Überwachung der Serverräume im Gebäude erfolgt von außen zudem durch einen zertifizierten Sicherheitsdienst. Beim Auslösen des Alarms erfolgt eine Benachrichtigung samt Passwortabfrage an das Wachpersonal sowie an gesondert berechtigte Personen im Unternehmen.
- Die Sicherungen der Systeme (Backup- und Recovery) erfolgt auf virtueller und physikalischer Ebene. Zusätzlich ist eine Festplattenspiegelung bei kritischen IT-Systemen der Fonds Finanz im Einsatz.

2. Rasche Wiederherstellbarkeit

- Daten auf Serversystemen von der Fonds Finanz werden mindestens wöchentlich inkrementell und monatlich „voll“ gesichert.
- Das Einspielen von Backups wird regelmäßig getestet.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Auch nach einem Katastrophen-Fall sind die Datensicherungen verfügbar bzw. zugänglich.
- Die Backup-Datenträger sind in einem anderen Gebäude als der Originaldatenträger aufbewahrt. Es gibt einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

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

1. Datenschutz-Management

- Alle Mitarbeiter sind auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung verpflichtet. Sie werden regelmäßig, mindestens einmal jährlich, geschult

- Es ist ein interner Datenschutzbeauftragter benannt worden. Die Stelle hat aktuell der Teamleiter Recht inne. Die Vertretung übernehmen die übrigen Mitglieder der Rechtsabteilung
- Die Unternehmensleitung hat die Verantwortung für Datenschutz und Informationssicherheit übernommen, dies ist in Leitlinien festgelegt
- Es gibt Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten
- Es gibt einen Prozess zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA)
- Anfragen von Betroffenen werden fristgemäß durch die Rechtsabteilung bzw. dem Datenschutzbeauftragten bearbeitet
- Es gibt ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO

2. Incident-Response-Management

Für die Meldung von Datenschutzverstößen ist ein Incident Response Management etabliert. Es ist insbesondere durch interne Prozesse und Schulungen sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich gemeldet werden.

Die Wahrnehmung von Betroffenenrechte hinsichtlich Auskunft, Berichtigung, Sperrung, Löschung und Herausgabe personenbezogener Daten ist durch einen Prozess definiert, über den alle Mitarbeiter im Rahmen der Datenschutzschulungen informiert sind.

3. Datenschutzfreundliche Voreinstellungen

Im Rahmen der Entwicklung und Anschaffung von Software werden die Anforderungen gemäß Art. 25 Abs. 1 und 2 DSGVO berücksichtigt (privacy by default /privacy by design). Dazu sind interne Prozesse definiert und die einbezogenen Fachabteilungen geschult. Bei der Entwicklung von Applikationen gehören Vorgaben zu privacy by default /privacy by design zum Teil der Konzeption.

4. Auftragskontrolle

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

- Die Auswahl unserer Auftragnehmer erfolgt unter besonderen Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit). Es erfolgt eine vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen.

Für alle Auftragnehmer, die in unserem Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, liegt eine schriftliche Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO vor.

Die Fonds Finanz überprüft und kontrolliert den Auftragnehmer und seine Tätigkeit im Rahmen regelmäßiger Audits.

- Ist die Fonds Finanz Auftragnehmer, liegt ebenso eine schriftliche Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO vor.

Die Fonds Finanz verarbeitet personenbezogene Daten nur nach Weisung und Vorgaben der Auftraggeber, so wie in der Vereinbarung zur Auftragsverarbeitung festgelegt.

Wenn mit dem Auftraggeber vereinbart wurde, dass die Erteilung von Unteraufträgen (z.B. über Datenerfassungsarbeiten) zulässig ist, wird die Fonds Finanz mit den Unterauftragnehmern einen Vertrag schließen. In diesem Vertrag wird für die Fonds Finanz ein Kontrollrecht vereinbart.

- Die Fonds Finanz verpflichtet alle Mitarbeiter/innen auf das Datengeheimnis bzw. zur Vertraulichkeit. Es ist ein Datenschutzbeauftragter benannt. Es werden regelmäßige Unterweisungen zum Datenschutz durchgeführt

Stand: 22.05.2018