FINSOLIO

Anlage 3 – Auftragsverarbeitungsvertrag

nach Artikel 28 DSGVO

zwischen dem Verantwortlichen

Muster Baufiberater GmbH

Musterstr. 1a
01217 Dresden

– nachfolgend Auftraggeber genannt –

und der

Finsolio c/o Finanzmakler.online GmbH
Haydnstr. 20
01309 Dresden

– nachfolgend Auftragnehmer genannt –

– nachfolgend zusammen die „Parteien“ genannt –

Präambel

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. Gegenstand

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. Ort der Datenverarbeitung

Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts Anderes ergibt. Jede Verlagerung der Verarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in schriftlicher Form und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. Laufzeit

3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von drei Monaten gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrages bis zu der regulären Beendigung des Hauptvertrages/der Hauptverträge fort.

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. Weisung

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4.2 Falls Weisungen, die unter Ziffer 1 der Anlage dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.

4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. Unterstützungspflichten des Auftragnehmers

5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. Prüfungsrechte des Auftraggebers

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei.

6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. Datenschutzbeauftragter des Auftragnehmers

7.1 Der Auftragnehmer gewährleistet, dass er eine fachkundige und zuverlässige Person als Datenschutzbeauftragte(n) mit der Wahrnehmung der Aufgaben des Datenschutzes (§ 4g BDSG) schriftlich bestellt hat. Dieser/Diesem steht die zur Erledigung der Aufgaben erforderliche Zeit gem. § 4f Abs.5 BDSG zur Verfügung.

7.2 Der Auftragnehmer teilt dem Auftraggeber auf Nachfrage unverzüglich die betrieblichen Kontaktdaten des/der betrieblichen Datenschutzbeauftragten mit. Ein Wechsel

in der Person der/des Datenschutzbeauftragte(n) ist dem Auftraggeber schriftlich mitzuteilen.

8. Vertraulichkeit

8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis sowie die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. Technische und organisatorische Maßnahmen

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.

9.2 Die vollständig ausgefüllte Vorlage für technische und organisatorische Maßnahmen in der Anlage oder ein eigenes Sicherheitskonzept des Auftragnehmers wird als verbindlich festgelegt.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 5 vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind in schriftlicher Form oder einem elektronischen Format zu vereinbaren.

10. Informationspflichten des Auftragnehmers und Verletzung des Schutzes personenbezogener Daten

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

10.3 Sollten die personenbezogenen Daten die unter dieser Vereinbarung verarbeitet werden beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. Unterauftragnehmer

11.1 Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer erfolgt nur nach Zustimmung des Auftraggebers in schriftlicher oder elektronischer Form.

11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des

Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.4 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage unter der Ziffer 4 aufgeführten Unterauftragnehmer.

11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unteraufragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

12. Löschung und Rückgabe personenbezogener Daten

12.1 Der Auftragnehmer ist nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.

12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.

12.3 Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sowie ein Nachweis der Durchführung in schriftlicher Form sind dem Auftraggeber innerhalb von 48 Stunden nach Durchführung der Vorgänge zur Verfügung zu stellen.

13. Haftung

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

14. Schlussbestimmungen

14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.

14.2 Die Anlage oder im Falle mehrerer abgeschlossener Hauptverträge die Anlagen zu diesem Vertrag sind wesentlicher Bestandteil desselben.

14.3 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.

14.4 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.

_____ , _____	Dresden, _____
Ort, Datum	Ort, Datum
Firmenstempel	Firmenstempel
Unterschrift Auftraggeber Muster Baufiberater GmbH	Unterschrift Auftragnehmer Finanzmakler.online GmbH Geschäftsführer

FINSOLIO

Anlage zum Auftragsverarbeitungsvertrag

technische und organisatorische Maßnahmen zur Umsetzung und Einhaltung der Vorgaben des § 9 Bundesdatenschutzgesetz

vom 01.01.2024

zwischen

Muster Baufiberater GmbH

Musterstr. 1a
01217 Dresden

– nachfolgend Auftraggeber genannt –

und der

Finsolio c/o Finanzmakler.online GmbH
Haydnstr. 20
01309 Dresden

– nachfolgend Auftragnehmer genannt –

– nachfolgend zusammen die „Parteien“ genannt –

1. Gegenstand des Auftrages

1.1. Gegenstand des Auftrages

1.1.1 Im Rahmen von Auftragsdatenverarbeitungen im Sinne des § 11 BDSG erhebt, verarbeitet oder nutzt der Auftragnehmer vom Auftraggeber bereitgestellte personenbezogene Daten (des gegebenenfalls vom Auftraggeber abweichenden Datenherrn). Die Auftragsdaten unterliegen neben den allgemeinen Verschwiegenheitspflichten, den Bestimmungen des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung, den sonstigen datenschutzrechtlichen Vorschriften und in der Regel dem im Leistungsvertrag geregelten Bankgeheimnis.

1.1.2 Absatz 1.1.1 gilt entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

1.1.3 Die dabei erhobenen, verarbeiteten oder genutzten Daten unterliegen der ausschließlichen Datenherrschaft des Datenherrn, weisungsbefugt ist - neben dem Datenherrn selbst - der Auftraggeber (im Namen des Datenherrn). Sofern in weiteren Vertragsdokumenten keine weisungsbefugten Personen des Auftraggebers und/oder des Datenherrn benannt werden, sind grundsätzlich von Auftraggeber- und Datenherr Seite der Vorstand, der Leiter der Rechtsabteilung, der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte weisungsbefugt.

1.1.4 Der Auftragnehmer gewährleistet, dass die in dieser Rahmenvereinbarung festgehaltenen Pflichten auch von seinem Personal sowie seinen Unterauftragnehmern und Erfüllungsgehilfen, die für den Auftragnehmer tätig sind bzw. werden, zur Kenntnis genommen, umgesetzt und eingehalten werden.

1.15 Diese Rahmenvereinbarung wird ergänzt durch konkrete, auftragsbezogene Regelungen, Arbeitsanweisungen, Handbücher usw..

1.2. Umfang, Art (Art. 4 Nr. 2 DSGVO) und Zweck der Datenverarbeitung

1.2.1 Der Auftraggeber erteilt Weisungen über Art, Umfang und Verfahren der Datenverarbeitung.

1.2.2 Der Auftraggeber erteilt alle Aufträge zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gemäß § 11 Abs. 2 Satz 2 BDSG schriftlich. Dieses geschieht – soweit nicht in dieser Rahmenvereinbarung bereits schriftliche Festlegungen i.S.d. § 11 Abs. 2 Satz 2 BDSG erfolgen – durch die Einfügung entsprechender Festlegungen gemäß § 1 Abs. 2 Nr. 7 in den Leistungsverträgen.

1.2.3 Der Auftragnehmer sichert zu, die Verarbeitung der Daten zeitlich nicht vor Abschluss einer schriftlichen Vereinbarung im Sinne dieses Paragraphen aufzunehmen oder Auftragsdaten anderweitig zu verwenden.

1.2.4 Über die in dieser Rahmenvereinbarung sowie den sich auf sie beziehenden Leistungsverträgen hinausgehende Weisungen des Auftraggebers bedürfen der Textform. In begründeten Eilfällen können durch bevollmächtigte Personen des Auftraggebers Weisungen auch mündlich erteilt werden. Diese bedürfen der unverzüglichen Bestätigung in Textform.

1.2.5 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Bundesdatenschutzgesetz oder andere Vorschriften verstößt, hat er den Auftraggeber gemäß § 11 Absatz 3 BDSG unverzüglich darauf hinzuweisen. Bei offensichtlich gegen gesetzliche Bestimmungen verstoßenden Weisungen ist der Auftragnehmer berechtigt, die Weisungen zurückzuweisen und gegebenenfalls auch endgültig ihre Durchführung zu verweigern.

1.2.6 Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland, unabhängig davon, ob es sich um vertragliche Haupt- oder Nebenleistungen handelt, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

1.3. Art der Daten

Datenkategorie	Beispiele
Berufliche Kontakt- und (Arbeits-) Organisationsdaten	Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Personalnummern, Anwesenheit
Daten zu beruflichen Verhältnissen	Berufsbezeichnung, beruflicher Werdegang, Betriebszugehörigkeit, Aufgaben, Tätigkeiten, Log-File-Auswertung, Eintritts- und Austrittsdaten, Qualifikationen, Beurteilungen, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe
Private Kontakt- und Identifikationsdaten	Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Geburtsdatum/-ort, Identifikationsnummern, Nationalität
Vertragsdaten	gekaufte Produkte, Datum Kaufvertrag, Kaufpreis, Garantien

Daten zu persönlichen Verhältnissen	Daten zum Ehegatten oder Kindern, Familienstand, Portraitfoto, Ehrenamt
Bonitäts- und Bankdaten	Zahlungsverhalten, Bilanzen, Daten von Auskunfteien, Vermögensverhältnisse, Kontoverbindung, Kreditkartennummer
Besonders sensible personenbezogene Daten	Art. 9 Abs. 1 DSGVO: rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
Daten zu Kauf- und Bestandsimmobilien	Größe, Kaufpreis, Grundstücksgröße, Wohnfläche, Kubatur, Baujahr, Zustand
Dokumente zu allen o.g. Datenkategorien	Ausweise, Gehaltsabrechnungen

1.4. Kreis der Betroffenen

Betroffenengruppe	Beschreibung	Beispiele
Mitarbeiter des Auftraggebers/des Verantwortlichen	Eigene Mitarbeiter des Auftraggebers/ des Verantwortlichen	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
Mitarbeiter anderer Unternehmen	Mitarbeiter anderer Unternehmen, deren personenbezogene Daten für den Auftraggeber/den Verantwortlichen verarbeitet werden	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
Kunden des Auftraggebers/des Verantwortlichen	Jede Person, mit der eine Kunden-Geschäftsbeziehung besteht (mit der jeweiligen verantwortlichen Stelle)	Käufer, Versicherungsnehmer, Mieter, Kunden einer Dienstleistung
Sonstige Geschäftspartner	Jede natürliche Person, mit der eine Geschäftsbeziehung besteht (mit dem Auftraggeber) außer Kunden	Lieferanten, Importeure, Dienstleister, Vermittler, Freelancer
Außenstehende	Jede Person, die in keiner Geschäftsbeziehung mit der jeweiligen Konzerngesellschaft (verantwortlichen Stelle) steht	Besucher, Gäste, Interessenten
Kinder	Personen unter 16 Jahren	

2. Weisungsberechtigte Personen

2.1 Weisungsberechtigte Personen des Auftraggebers sind

(Name, Organisationseinheit, Funktion, Telefon, E-Mail-Adresse)

(Name, Organisationseinheit, Funktion, Telefon, E-Mail-Adresse)

2.2 Weisungsempfänger beim Auftragnehmer sind

Geschäftsführer, Sten Valandt, 0351-79993230, sten.valandt@finsolio.de

3. Datenschutzbeauftragter

3.1 Datenschutzbeauftragter des Auftraggebers ist

(Datenschutzbeauftragter eintragen, soweit vorhanden)

3.2 Datenschutzbeauftragter des Auftragnehmers ist

Geschäftsführer, Sten Valandt, 0351-79993230, sten.valandt@finsolio.de

4. Unterauftragnehmer

Nr.	Unterauftragnehmer (Name, Anschrift, Ansprechpartner)	Verarbeitete Datenkategorien	Beschreibung der Tätigkeit
1	Robotron Datenbank-Software GmbH, Stuttgarter Straße 29, 01129 Dresden	Ausschließlich Daten der Lizenznehmer, in Einzelfällen genannte Daten unter Ziffer 1.2 bis 1.4	Exklusiver IT-Entwickler und Servicedienstleister

5. Technische und organisatorische Maßnahmen

5.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Der Auftragnehmer hat folgende Maßnahmen zur Zutrittskontrolle zu treffen, sofern in den Räumen/Gebäuden des Auftragnehmers Auftragsdaten verarbeitet werden oder aus diesen Räumen/Gebäuden ein Zugang zu solchen Daten nicht ausgeschlossen ist:

1. Beschränkung der Zutrittsberechtigungen zu Bürogebäude, Rechenzentren und Serverräumen auf das erforderliche Mindestmaß.
2. Wirksame Kontrolle der Zutrittsberechtigungen durch ein adäquates Schließsystem (bspw. Sicherheitsschlüssel mit dokumentierter Schlüsselverwaltung, Elektronische
3. Schließanlagen mit dokumentierter Verwaltung der Berechtigungen)
4. Dokumentierte und nachvollziehbare Prozesse zur Erlangung, Veränderung und Rücknahme von Zutrittsberechtigungen.
5. Regelmäßige und dokumentierte Überprüfung der vergebenen Zutrittsberechtigungen
6. auf Aktualität angemessene Maßnahmen zur Prophylaxe vor und Detektierung von unbefugten Zutritten und Zutrittsversuchen (bspw. Regelmäßige Überprüfung der Einbruchssicherheit der Türen, Tore und Fenster, Einbruchmeldeanlage, Videoüberwachung, Wachdienst, Sicherheits-Patrouille)
7. Schriftliche Regelungen für Mitarbeiter und Besucher für den Umgang mit technischen Zutritts-Sicherungsmaßnahmen.

5.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Der Auftragnehmer hat folgende Maßnahmen zur Zugangskontrolle zu Systemen und Netzwerken, in denen Auftragsdaten verarbeitet werden oder über die der Zugang zu Auftragsdaten möglich ist, zu treffen:

1. Beschränkung der Zugangsberechtigungen zu DV-Systemen und nicht öffentlichen Netzwerken auf das erforderliche Mindestmaß.
2. Wirksame Kontrolle der Zugangsberechtigungen durch personalisierte und eindeutige Benutzerkennungen und einem sicheren Authentisierungsverfahren
3. Bei Verwendung von Passwörtern zur Authentisierung
    a) sind Vorgaben zu erlassen, die eine durchgängige Passwörterqualität von mindestens 8 Zeichen, 3 Komplexitätsgraden und einem Wechselturnus von maximal 180 Tagen gewährleisten.
    b) ist bei Administrations- oder Applikationsaccounts die vorstehende Komplexität durch eine Mindestlänge von mindestens 12 Zeichen zu erhöhen.
    c) sind Technische Prüfverfahren zur Sicherstellung der Passwortqualität einzusetzen.
4. Bei Verwendung von asymmetrischen Schlüsselverfahren (bspw. Zertifikate, Private-
5. Public-Key-Methode) zur Authentisierung, ist sicherzustellen, dass geheime (private) Schlüssel immer mit einem Passwort (Passphrase) geschützt werden. Die Anforderungen gem. vorstehender Ziffer 3b sind einzuhalten.
6. Dokumentierte und Nachvollziehbare Prozesse zur Erlangung, Veränderung und Rücknahme von Zugangsberechtigungen.
7. Regelmäßige und dokumentierte Überprüfung der vergebenen Zugangsberechtigungen auf Aktualität
8. Angemessene Maßnahmen zur Sicherung der Netzwerk-Infrastruktur (bspw. Netzwerk-Port-Security nach IEEE 802.1X, Intrusion Detection Systeme, Nutzung
9. von 2-Faktor-Authentisierung bei Fernzugängen, Trennung von Netzen, Content-Filter, verschlüsselte Netzwerkprotokolle usw.)
10. Schriftliche Regelungen für Mitarbeiter für den Umgang mit den obigen Sicherungsmaßnahmen und der sicheren Verwendung von Passwörtern.
11. Sicherstellung einer unverzüglichen Installation von kritischen/ oder wichtigen Sicherheits-Updates/Patches
    a) in Client-Betriebssysteme,
    b) in Server-Betriebssysteme, die über öffentliche Netze erreichbar sind (bspw. Webserver),

c) in Anwendungsprogramme (inkl. Browser, Plugins, PDF-Reader usw.) und

d) in Sicherheits-Infrastruktur (Virenscanner, Firewalls, IDS-Systeme, Content-Filter, Router usw.) binnen 48h nach Veröffentlichung durch den Hersteller

a. sowie

e) in Server-Betriebssysteme interner Server binnen 1 Woche nach Veröffentlichung durch den Hersteller

5.3 Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Der Auftragnehmer hat folgende Maßnahmen zur Zugriffskontrolle zu treffen, sofern er selbst die Zugriffsberechtigungen zu Auftragsdaten verantwortet:

1. Beschränkung der Zugriffsberechtigungen zu Auftragsdaten auf das absolut benötigte Mindestmaß.
2. Wirksame Kontrolle der Zugriffsberechtigungen durch ein adäquates Rechte- und Rollenkonzept.
3. Dokumentierte und Nachvollziehbare Prozesse zur Erlangung, Veränderung und Rücknahme von Zugriffsberechtigungen.
4. Regelmäßige und dokumentierte Überprüfung der vergebenen Zugriffsberechtigungen auf Aktualität
5. Angemessene Maßnahmen zum Schutz von Endgeräten, Servern und anderen Infrastruktur-Elementen vor unbefugtem Zugriff (bspw. mehrstufiges Virenschutz-Konzept, Content-Filter, Application Firewall, Intrusion Detection Systeme, Desktop-Firewalls, System-Hardening, Content-Verschlüsselung).
6. Datenträger-Verschlüsselung mit - nach aktuellem Stand der Technik - als sicher einzustufenden Algorithmen zum Schutz von mobilen Geräten (Notebooks, Tablet-PCs, Smartphones usw.) und Datenträgern (Externe Festplatten, USB-Sticks, Speicherkarten, usw.)
7. Protokollierung von Zugriffen, auch durch Administratoren.
8. Technische Sicherungsmaßnahmen für Ex- und Import-Schnittstellen (Hardware- wie Applikationsbezogen).

Der Auftragnehmer hat folgende Mitwirkungspflichten bei der Zugriffskontrolle, sofern er nicht selbst die Zugriffsberechtigungen zu Auftragsdaten verwaltet:

1. Dokumentierte und Nachvollziehbare Prozesse zur Beantragung, Veränderung und Rücknahme von Zugriffsberechtigungen in seinem Verantwortungsbereich
2. Regelmäßige und dokumentierte Überprüfung der vergebenen Zugriffsberechtigungen auf Aktualität soweit möglich
3. Unverzügliche Meldung an den Auftraggeber, wenn vorhandene Zugriffsberechtigungen nicht mehr benötigt werden.

5.4 Weitergabekontrolle

Der Auftraggeber stellt die zu verarbeitenden Daten in einem im Vertrag/Auftrag definierten Übermittlungsverfahren zur Verfügung. Die Ergebnisse der Verarbeitung werden ebenfalls in einem definierten Übermittlungsverfahren wieder an den Auftraggeber übermittelt. Die Art der Übermittlung sowie die Maßnahmen zur Sicherheit der Übermittlung (Übermittlungskontrolle) sind anforderungsgerecht festzulegen; hierbei ist insbesondere die Verwendung einer dem Stand der Technik entsprechender Verschlüsselungstechnik vorzusehen.

Es ist zu 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.
Der Auftragnehmer hat folgende Maßnahmen zur Weitergabekontrolle zu treffen, sofern Auftragsdaten durch den Auftragnehmer empfangen, übertragen oder transportiert werden:

1. Angemessene Maßnahmen zur Sicherung der Netzwerk-Infrastruktur (bspw. Netzwerk-Port-Security nach IEEE 802.1X, Intrusion Detection Systeme, Nutzung von 2-Faktor-Authentisierung bei Fernzugängen, Trennung von Netzen, Content-Filter, verschlüsselte Netzwerkprotokolle usw.)
2. Datenträger-Verschlüsselung mit - nach aktuellem Stand der Technik - als sicher einzustufenden Algorithmen zum Schutz von mobilen Geräten (Notebooks, Tablet-PCs, Smartphones usw.) und Datenträgern (Externe Festplatten, USB-Sticks, Speicherkarten, usw.)

3. Verwendung verschlüsselter Übertragungsprotokolle (bspw. SSL-basierte Protokolle).
4. Prüfmechanismen zur Identifizierung der Gegenstelle bei Übertragungen.
5. Prüfsummen-Abgleich bei empfangenen Daten
6. Schriftliche Regelungen für Mitarbeiter für den Umgang und die Sicherheit bei mobilen Geräten und Datenträgern.

5.5 Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Auftragnehmer trifft folgende Maßnahmen zur Eingabekontrolle auf seinen Systemen, die der Verarbeitung von Auftragsdaten dienen oder den Zugang zu solchen Systemen ermöglichen oder vermitteln:

1. Erstellung und revisionssichere Speicherung von Verarbeitungsprotokollen.
2. Sicherung von Log-Dateien gegen Manipulation
3. Protokollierung und Auswertung von fehlerhaften Anmeldeversuchen
4. Sicherstellung, dass keine Gruppen-Accounts (auch Administratoren oder root) genutzt werden

5.6 Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Auftragnehmer hat folgende Maßnahmen zur Auftragskontrolle zu treffen:

Prozesse und Dokumentationen zur

1. Auswahl von (Unter)Auftragnehmern unter datenschutzrechtlichen und -technischen Gesichtspunkten
2. Sicherstellung der gesetzlich vorgeschriebenen Erstkontrolle von (Unter-)Auftragnehmern im Sinne des § 11 Abs. 2 Satz 4 BDSG sowie der regelmäßigen Nachkontrollen
3. Sicherstellung der frühzeitigen Unterrichtung des betrieblichen Datenschutzbeauftragten bei Einführung neuer oder Veränderung bestehender Verfahren zur Verarbeitung personenbezogener Daten

4. Verpflichtung aller mit der Verarbeitung personenbezogener Daten beauftragte Personen auf das Datengeheimnis gemäß § 5 BDSG
5. regelmäßige Überprüfung der Ordnungsmäßigkeit der Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden
6. Sicherstellung des Vertrautmachen der mit der Datenverarbeitung betrauten Personen mit den relevanten datenschutzrechtlichen und Auftraggeber spezifischen Regelungen
7. Aufrechterhaltung der Fachkunde des betrieblichen Datenschutzbeauftragten
8. Sicherstellung der unverzüglichen Benachrichtigung des Auftraggebers im Falle einer unrechtmäßigen Kenntniserlangung personenbezogener oder anderweitig geschützter Informationen
9. Gewährleistung der unverzüglichen Berichtigung, Sperrung und Löschung von Auftragsdaten auf Weisung des Auftraggebers

5.7 Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Der Auftragnehmer hat folgende Maßnahmen zur Verfügbarkeitskontrolle umzusetzen, sofern die Verarbeitung im Auftrag für die Aufrechterhaltung produktiver Dienste erforderlich ist:

1. Betrieb und regelmäßige Wartung von Brand-Meldeanlagen in Serverräumen, Rechenzentren und wichtigen Infrastrukturräumen.
2. Erstellung täglicher Backups
3. Sicherstellung der Backup-Lagerung in einem separaten Brandabschnitt
4. Regelmäßige Überprüfung der Backups auf Integrität
5. Prozesse und Dokumentationen zur Wiederherstellung von Systemen und Daten

5.8 Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der Auftragnehmer hat folgende Maßnahmen zur Trennung von Auftragsdaten zu treffen, sofern diese in seinem Verantwortungsbereich liegen:

1. Logische und/oder physische Trennung von Test-, Entwicklungs- und Produktionssystemen
2. Mandantentrennung innerhalb der Verarbeitungssysteme und an Schnittstellen
3. Sicherstellung der ständigen Identifizierbarkeit der Auftragsdaten

5.9 Löschung von Daten

Personenbezogene Daten sind zu löschen, wenn sie für Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Löschen ist die Unkenntlichmachung gespeicherter personenbezogener Daten.

Der Auftragnehmer hat folgende Maßnahmen zur Sicherstellung der Löschung von Daten zu treffen, sofern diese in seinem Verantwortungsbereich liegen:

1. Sicherstellung der ständigen Löschbarkeit der Auftragsdaten auf Anforderung des Auftraggebers
2. Prozesse, Tools und Dokumentationen für sicheres Löschen in der Art, dass eine Wiederherstellung der Daten nach heutigem Stand der Technik nicht möglich ist (bspw. durch Überschreiben)
3. Vorgaben für Mitarbeiter, wie wann welche Daten zu löschen sind.