Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Artikel 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO)

Auftragsverarbeitungsvertrag zur Nutzung der Immobilienverwaltungssoftware „NautilusX"

Vertragsparteien

zwischen dem Nutzer (nachfolgend Auftraggeber)

und

Dominik Josef Hofrichter / ATLAS Internet als Betreiber von NautilusX, Seeleinsbühlstraße 15, 94031 Nürnberg (nachfolgend Auftragsverarbeiter / Auftragnehmer)

– Verantwortlicher und Auftragsverarbeiter nachfolgend einzeln auch „**Partei**" und gemeinsam „**Parteien**" genannt –

Präambel

Der Auftragnehmer stellt dem Auftraggeber die webbasierte Software „NautilusX" zur Verwaltung von Immobilien, Mietverhältnissen, Mietinteressenten, Dokumenten und weiteren immobilienwirtschaftlichen Vorgängen zur Verfügung (nachfolgend „**Hauptvertrag**" bzw. „**Leistungsvertrag**"). Im Rahmen der Erbringung dieser Leistungen erhält der Auftragnehmer Zugang zu personenbezogenen Daten, für die der Auftraggeber datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist, und verarbeitet diese ausschließlich in dessen Auftrag.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien, die sich aus der Auftragsverarbeitung nach Art. 28 DSGVO ergeben. Er findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer oder von ihm eingesetzte Beschäftigte oder Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeiten. Der vorliegende Vertrag geht bei Widersprüchen zu datenschutzrechtlichen Regelungen des Hauptvertrages vor.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

(1) Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1** zu diesem Vertrag.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers, soweit er nicht ausnahmsweise durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). 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.

(3) Die Verarbeitung findet ausschließlich innerhalb des Gebiets der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung der Verarbeitung oder eines Teils davon in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) Die Laufzeit dieses Vertrages (Dauer der Verarbeitung) richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Vertrages keine darüber hinausgehenden Verpflichtungen ergeben. Dieser Vertrag kann durch jede Partei jederzeit ohne Einhaltung einer Frist gekündigt werden, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftraggeber ist im Verhältnis der Parteien für die Einhaltung der datenschutzrechtlichen Vorschriften, insbesondere für die Rechtmäßigkeit der Datenverarbeitung und die Wahrung der Rechte der betroffenen Personen, allein verantwortlich (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch für die Rechtmäßigkeit der Übermittlung der personenbezogenen Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der erteilten Weisungen.

(2) Weisungen des Auftraggebers werden zunächst durch die im Hauptvertrag und in diesem Vertrag getroffenen Festlegungen bestimmt und können vom Auftraggeber danach in schriftlicher oder in einem dokumentierten elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer verarbeitet die personenbezogenen Daten nicht zu eigenen Zwecken oder zu Zwecken Dritter. Kopien oder Duplikate der Daten werden ohne Wissen und Weisung des Auftraggebers nicht erstellt; ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer darf die Daten nur im Rahmen der dokumentierten Weisungen des Auftraggebers verarbeiten. Der Auftraggeber behält sich im Rahmen der in diesem Vertrag getroffenen Leistungsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen (Art. 28 Abs. 3 Satz 2 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer ist nicht verpflichtet, eine offensichtlich rechtswidrige Weisung auszuführen.

(4) Die zur Erteilung von Weisungen berechtigten Personen des Auftraggebers und die weisungsempfangsberechtigten Personen des Auftragnehmers sind in **Anlage 4** benannt. Bei einem Wechsel oder einer längerfristigen Verhinderung der genannten Personen sind dem Vertragspartner unverzüglich die Nachfolger bzw. Vertreter in Textform mitzuteilen.

§ 4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, die gesetzlichen Bestimmungen zum Datenschutz einzuhalten und die aus diesem Vertrag folgenden Pflichten zu erfüllen. Er trifft insbesondere folgende Maßnahmen:

(1) **Bestellung eines Datenschutzbeauftragten.** Der Auftragnehmer hat, soweit gesetzlich erforderlich (Art. 37 DSGVO, § 38 BDSG), einen Datenschutzbeauftragten bestellt. Dessen jeweils aktuelle Kontaktdaten werden dem Auftraggeber auf Anfrage mitgeteilt. Da keine gesetzliche Pflicht für den Betreiber von NautilusX besteht, ist Hr. Dominik Josef Hofrichter entsprechende Kontaktperson für datenschutzrechtliche Sachverhalte.

(2) **Vertraulichkeit.** Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO). Die Verpflichtung wirkt auch nach Beendigung der Tätigkeit fort. Der Auftragnehmer weist die von ihm eingesetzten Personen vor Aufnahme ihrer Tätigkeit in geeigneter Weise in die für sie maßgeblichen Bestimmungen des Datenschutzes ein.

(3) **Technische und organisatorische Maßnahmen.** Der Auftragnehmer trifft und gewährleistet für die Dauer dieses Vertrages die zur angemessenen Sicherheit der Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Diese sind in **Anlage 2** dokumentiert. Der Auftragnehmer ist berechtigt, die getroffenen Maßnahmen fortzuentwickeln und an den Stand der Technik anzupassen; dabei darf das vereinbarte Schutzniveau nicht unterschritten werden. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen.

(4) **Unterstützung des Auftraggebers.** Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und mit geeigneten technischen und organisatorischen Maßnahmen a) bei der Erfüllung der Rechte betroffener Personen nach Kapitel III der DSGVO (Art. 28 Abs. 3 lit. e DSGVO; vgl. § 7), b) bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, namentlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Benachrichtigung betroffener Personen sowie der Durchführung von Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f DSGVO; vgl. §§ 8 und 9).

(5) **Nachweis- und Kontrollpflichten.** Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen nach Maßgabe von § 11 (Art. 28 Abs. 3 lit. h DSGVO).

(6) **Berichtigung, Löschung und Rückgabe.** Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der Daten nur nach dokumentierter Weisung des Auftraggebers ein. Nach Abschluss der Verarbeitung verfährt der Auftragnehmer gemäß § 14.

(7) **Führung eines Verzeichnisses.** Der Auftragnehmer führt, soweit einschlägig, ein Verzeichnis zu allen Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung gemäß Art. 30 Abs. 2 DSGVO.

(8) **Ort der Verarbeitung.** Die Verarbeitung und Speicherung der personenbezogenen Daten erfolgt ausschließlich an den in **Anlage 3** genannten Orten innerhalb der EU/des EWR.

§ 5 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen getroffen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer überprüft, bewertet und evaluiert die Wirksamkeit der Maßnahmen regelmäßig (Art. 32 Abs. 1 lit. d DSGVO). Ihm ist gestattet, alternative angemessene Maßnahmen umzusetzen; das Sicherheitsniveau der festgelegten Maßnahmen darf dabei nicht unterschritten werden.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

(2) Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter.

§ 7 Wahrung von Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten dabei, den Anträgen betroffener Personen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, Datenübertragbarkeit, Widerspruch sowie den Informationspflichten nachzukommen (Art. 12 bis 23 DSGVO).

(2) Wendet sich eine betroffene Person mit einem Ersuchen zur Berichtigung, Löschung, Auskunft oder Einschränkung der Verarbeitung unmittelbar an den Auftragnehmer, so wird dieser das Ersuchen unverzüglich an den Auftraggeber weiterleiten und die betroffene Person nicht selbst beauskunften, es sei denn, er ist hierzu ausdrücklich durch den Auftraggeber angewiesen worden.

(3) Der Auftragnehmer stellt hierzu, soweit technisch möglich, geeignete Funktionen der Software bereit (z. B. Export einzelner Datensätze, Löschung von Datensätzen und zugehörigen Dateien, Bereinigung des Papierkorbs). Für einen etwaigen darüber hinausgehenden Aufwand kann eine gesonderte Vergütung nach Aufwand vereinbart werden, sofern die Unterstützung nicht auf einem Umstand beruht, den der Auftragnehmer zu vertreten hat.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, in der Regel innerhalb von 24 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten, die im Auftrag verarbeitet werden, bekannt geworden ist (Art. 33 Abs. 2 DSGVO). Die Frist des Art. 33 Abs. 1 DSGVO (Meldung an die Aufsichtsbehörde binnen 72 Stunden) trifft ausschließlich den Auftraggeber.

(2) Die Meldung an den Auftraggeber enthält mindestens folgende Angaben, soweit verfügbar: a) eine Beschreibung der Art der Verletzung einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der betroffenen Datensätze; b) den Namen und die Kontaktdaten der zuständigen Ansprechperson; c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung; d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und stimmt sich hierüber mit dem Auftraggeber ab.

(4) Meldungen an die zuständige Aufsichtsbehörde oder an betroffene Personen nach Art. 33 und 34 DSGVO nimmt der Auftraggeber vor. Der Auftragnehmer unterstützt ihn hierbei im erforderlichen Umfang.

§ 9 Datenschutz-Folgenabschätzung

Sofern aufgrund der Art der Verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO oder eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO erforderlich ist, unterstützt der Auftragnehmer den Auftraggeber hierbei im Rahmen seiner Möglichkeiten, insbesondere durch Bereitstellung der erforderlichen Informationen über die eingesetzten Verfahren und die getroffenen technischen und organisatorischen Maßnahmen.

§ 10 Einsatz von Unterauftragsverarbeitern

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und werden vom Auftraggeber genehmigt.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung gelten solche Dienstleistungen, die einen unmittelbaren Bezug zur Erbringung der Hauptleistung aufweisen (insbesondere Hosting, Rechenzentrums- und Serverdienstleistungen sowie Backup-Dienste). Nicht hierunter fallen Nebenleistungen, die der Auftragnehmer bei Dritten als Hilfsleistung in Anspruch nimmt, etwa Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, auch bei solchen Nebenleistungen angemessene Vorkehrungen zur Gewährleistung des Datenschutzes und der Datensicherheit zu treffen.

(3) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern rechtzeitig vor der Änderung, spätestens jedoch [z. B. vier] Wochen im Voraus, in Textform. Der Auftraggeber kann der Änderung innerhalb von [z. B. zwei] Wochen nach Zugang der Information aus wichtigem, datenschutzrechtlich begründetem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Änderung als genehmigt. Widerspricht der Auftraggeber, ist der Auftragnehmer berechtigt, die betroffene Leistung ohne Einsatz des Unterauftragsverarbeiters zu erbringen; ist dies mit zumutbarem Aufwand nicht möglich, steht beiden Parteien ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu.

(4) Der Auftragnehmer hat mit dem Unterauftragsverarbeiter einen Vertrag zu schließen, der den Anforderungen des Art. 28 Abs. 4 DSGVO genügt und dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

(5) Die Weitergabe von im Auftrag verarbeiteten Daten an einen Unterauftragsverarbeiter ist erst zulässig, wenn dieser die Verpflichtungen aus diesem Vertrag übernommen hat.

§ 11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessenem Umfang von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(2) Der Auftragnehmer weist die Einhaltung der Pflichten nach Art. 28 DSGVO und der in diesem Vertrag vereinbarten technischen und organisatorischen Maßnahmen auf Anforderung des Auftraggebers durch geeignete Mittel nach. Als geeignete Nachweise kommen insbesondere in Betracht: a) die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO); b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren (Art. 42 DSGVO); c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren); d) eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit.

(3) Sofern die Nachweise nach Absatz 2 im Einzelfall nicht ausreichen, ist der Auftraggeber berechtigt, nach rechtzeitiger vorheriger Ankündigung mit angemessener Vorlaufzeit (in der Regel mindestens [z. B. zwei] Wochen) und während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs, Überprüfungen selbst oder durch einen zur Verschwiegenheit verpflichteten, nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehenden Prüfer durchführen zu lassen. Kontrollen dürfen den Betrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen; sie finden grundsätzlich nicht häufiger als einmal jährlich statt, es sei denn, es besteht ein besonderer Anlass (etwa eine Datenschutzverletzung).

(4) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

(5) Der für die Unterstützung bei der Durchführung einer Vor-Ort-Kontrolle entstehende Aufwand kann, sofern er ein zumutbares Maß überschreitet und nicht auf einem vom Auftragnehmer zu vertretenden Umstand beruht, nach Aufwand gesondert vergütet werden. Dies ist zuvor zwischen den Parteien abzustimmen.

§ 12 Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer teilt dem Auftraggeber unverzüglich mit: a) erhebliche Störungen bei der Auftragserfüllung; b) Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder gegen die Festlegungen dieses Vertrages; c) Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde nach Art. 58 DSGVO, soweit sie sich auf die Auftragsverarbeitung beziehen, sowie den Umstand, dass eine Aufsichtsbehörde gegen den Auftragnehmer nach Art. 83 oder Art. 84 DSGVO ermittelt; d) Anfragen von Strafverfolgungs-, Sicherheits- oder anderen Behörden, die auf die Herausgabe der im Auftrag verarbeiteten Daten gerichtet sind, es sei denn, eine solche Mitteilung ist ihm gesetzlich untersagt.

§ 13 Weisungsberechtigte Personen

Die zur Erteilung und zum Empfang von Weisungen berechtigten Personen ergeben sich aus **Anlage 4**.

§ 14 Löschung und Rückgabe von Daten nach Beendigung des Auftrags

(1) Nach Abschluss der Verarbeitungstätigkeiten hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche personenbezogenen Daten entweder zu löschen oder zurückzugeben, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht (Art. 28 Abs. 3 lit. g DSGVO). Sobald der Auftraggeber sein Nutzerkonto gelöscht hat, werden automatisch sämtliche zugehörigen Daten und Informationen gelöscht - eine Rückgabe der personenbezogenen Daten ist daher nicht möglich.

(2) Die Löschung erfolgt datenschutzgerecht und umfasst auch etwaige Sicherungskopien sowie in Papierform vorhandene Unterlagen. Die vollständige und datenschutzgerechte Vernichtung bzw. Löschung ist dem Auftraggeber auf Anforderung schriftlich zu bestätigen (Löschprotokoll).

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 15 Haftung

(1) Für den Ersatz von Schäden, die einer betroffenen Person aufgrund einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses entstehen, gilt Art. 82 DSGVO im Verhältnis der Parteien und gegenüber der betroffenen Person.

(2) Im Innenverhältnis tragen die Parteien die Verantwortung für Schäden nach Maßgabe des jeweiligen Verursachungs- und Verschuldensanteils. Die Regelungen des Hauptvertrages zur Haftung bleiben im Übrigen unberührt.

§ 16 Vertraulichkeit

Beide Parteien verpflichten sich, alle im Zusammenhang mit der Vertragsdurchführung erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie von personenbezogenen Daten vertraulich zu behandeln und ausschließlich zur Durchführung dieses Vertrages zu verwenden. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.

§ 17 Vergütung

Die Nutzung der Software NautilusX ist kostenfrei.

§ 18 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Gültigkeit der übrigen Bestimmungen hiervon nicht berührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung am nächsten kommt. Entsprechendes gilt für etwaige Regelungslücken.

(2) Änderungen und Ergänzungen dieses Vertrages und seiner Anlagen bedürfen der Schriftform bzw. eines dokumentierten elektronischen Formats (Textform). Dies gilt auch für die Änderung dieser Formklausel. Vorrang haben stets die individuellen vertraglichen Vereinbarungen.

(3) Bei Widersprüchen zwischen den Regelungen dieses Vertrages und den Regelungen des Hauptvertrages gehen hinsichtlich des Datenschutzes die Regelungen dieses Vertrages vor. Bei Widersprüchen zwischen diesem Vertrag und seinen Anlagen geht dieser Vertrag vor, sofern die Anlage nicht ausdrücklich und eindeutig eine vorrangige Regelung trifft.

(4) Es gilt das Recht der Bundesrepublik Deutschland unter Einbeziehung der unmittelbar geltenden Vorschriften der DSGVO.

(5) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist, soweit gesetzlich zulässig, Nürnberg.

Anlage 1 – Beschreibung der Auftragsverarbeitung

1. Gegenstand und Art der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb der Software „NautilusX" zur digitalen Verwaltung von Immobilienbeständen und der damit verbundenen Miet- und Vertragsverhältnisse. Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Speichern, Organisieren, Ordnen, Anpassen, Auslesen, Abfragen, Verwenden, Löschen und Vernichten personenbezogener Daten mittels der bereitgestellten Software sowie das Hosting und die Speicherung der zugehörigen Dokumente und Dateien.

2. Zweck der Verarbeitung

Zweck der Verarbeitung ist die Ermöglichung der immobilienwirtschaftlichen Verwaltungstätigkeit des Auftraggebers, insbesondere die Verwaltung von Objekten, Mietverhältnissen und Mietinteressenten, die Durchführung von Vermietungs- und Auswahlprozessen, die Verwaltung von Finanzierungsanfragen, die Dokumentenverwaltung, die Terminverwaltung, die Führung eines Adressbuchs sowie die Abwicklung wiederkehrender Verwaltungsvorgänge (z. B. Abmahnungen, Kautionsabrechnungen, Nebenkostenabrechnungen).

3. Kategorien betroffener Personen

Von der Verarbeitung sind folgende Kategorien betroffener Personen erfasst:

- Mieterinnen und Mieter (Privat- und Gewerbemieter) einschließlich Mitbewohnerinnen und Mitbewohnern;
- Mietinteressentinnen und Mietinteressenten (Privat und Gewerblich);
- Ansprechpartnerinnen und Ansprechpartner von Unternehmen (bei Gewerbemietern und -interessenten);
- Kontakte des Adressbuchs (z. B. Dienstleister, Handwerker, Hausverwaltungen, Makler, Eigentümer, Bankkontakte, sonstige Kontaktpersonen);
- Antragstellerinnen und Antragsteller bzw. beteiligte Personen von Finanzierungsanfragen.

4. Art der personenbezogenen Daten

Verarbeitet werden insbesondere folgende Datenarten, soweit sie vom Auftraggeber in die Software eingegeben werden:

- **Stammdaten:** Name(n), Anschrift, Kontaktdaten (Telefon, Mobilfunk, E-Mail);
- **Vertrags- und Objektdaten:** zugeordnete Immobilie, Beginn und Art des Mietverhältnisses, Kaltmiete, Nebenkosten, Kautionsdaten;

- **Bonitäts- und Wirtschaftsdaten (bei Privatpersonen):** monatlicher Nettoverdienst, Angaben zum Arbeitsverhältnis, Ergebnis der SCHUFA-/Bonitätsauskunft, Gehaltsnachweise, Mieterselbstauskunft;
- **weitere Angaben zur Person (bei Privatpersonen):** Angaben zu Kindern, Haustieren und Raucherstatus im Rahmen der Mietinteressentenauswahl;
- **Unternehmensbezogene Daten (bei Gewerbemietern/-interessenten):** Rechtsform, Branche, Anzahl der Mitarbeitenden, Angaben zur finanziellen Situation, gewünschte Nutzung und Mietdauer;
- **Kontaktdaten des Adressbuchs:** Anrede, Vor- und Nachname bzw. Unternehmensname und Rechtsform, Kontaktart, Anschrift, E-Mail, Telefon, Bemerkungen;
- **Dokumente und Dateien:** vom Auftraggeber hochgeladene Unterlagen (z. B. Verträge, Nachweise, Schriftverkehr), die personenbezogene Daten enthalten können;
- **Freitext- und Bemerkungsfelder**, die weitere personenbezogene Angaben enthalten können.

Hinweis: Die Software ist nicht auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ausgelegt. Der Auftraggeber stellt sicher, dass solche Daten nur eingegeben werden, soweit hierfür eine Rechtsgrundlage besteht und die zusätzlichen Anforderungen des Art. 9 DSGVO erfüllt sind. Der Auftraggeber ist für die Beachtung der jeweils einschlägigen Erhebungs- und Speichergrenzen (etwa bei Bonitäts- und Selbstauskunftsdaten im Bewerbungs- bzw. Auswahlprozess) allein verantwortlich.

5. Dauer der Verarbeitung

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages. Nach dessen Beendigung erfolgt die Löschung der Daten gemäß § 14 dieses Vertrages.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragnehmer trifft die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen. Maßnahmen, die von der konkreten Betriebs- und Hosting-Umgebung abhängen, sind entsprechend zu konkretisieren und durch den Auftragnehmer bzw. den in Anlage 3 genannten Hosting-Dienstleister sicherzustellen.

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

1.1 Zutrittskontrolle (Schutz vor unbefugtem physischen Zutritt zu Datenverarbeitungsanlagen) Die physische Sicherheit der Server erfolgt über das

eingesetzte Rechenzentrum bzw. den Hosting-Dienstleister (siehe Anlage 3). Zu den dortigen Maßnahmen zählen üblicherweise: gesichertes Rechenzentrum mit Zutrittskontrolle, Videoüberwachung, Alarmanlagen, Vereinzelungsanlagen sowie Protokollierung der Zutritte.

1.2 Zugangskontrolle (Schutz vor unbefugter Systemnutzung)

- Zugang zur Anwendung ausschließlich über eine persönliche, benutzerbezogene Anmeldung mit Benutzername und Passwort;
- Speicherung von Passwörtern ausschließlich als Hashwert unter Verwendung eines individuellen Zufallswertes (Salt); keine Speicherung von Klartextpasswörtern;
- verschlüsselte Übertragung sämtlicher Daten zwischen Endgerät und Server über Transportverschlüsselung (TLS/HTTPS); [durch den Betreiber sicherzustellen];
- Sitzungsverwaltung mit automatischer Beendigung inaktiver Sitzungen bzw. serverseitiger Zugangsprüfung bei jedem Datenzugriff;
- Schutz der administrativen Zugänge zum Server und zur Datenbank durch gesonderte, restriktiv vergebene Zugangsdaten.

1.3 Zugriffskontrolle (Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)

- strikte mandantenbezogene Trennung der Daten: Die Inhaltsdaten jedes Nutzerkontos werden in einem eigenen, dem jeweiligen Konto zugeordneten Speicherbereich abgelegt; ein Zugriff auf Daten anderer Konten ist ausgeschlossen;
- serverseitige Prüfung der Zugehörigkeit jedes Datensatzes und jeder hinterlegten Datei zum jeweils angemeldeten Nutzerkonto vor jedem Zugriff;
- Ablage der Nutzerdaten und der hochgeladenen Dateien in Verzeichnissen, die gegen einen direkten Zugriff über das Internet abgesichert sind (Zugriffssperre auf Verzeichnisebene sowie Deaktivierung der Skriptausführung in Datenverzeichnissen);
- Vergabe von Zugriffsrechten nach dem Prinzip der geringstmöglichen Berechtigung (Need-to-know).

1.4 Trennungskontrolle (getrennte Verarbeitung von Daten unterschiedlicher Zwecke)

- logische Mandantentrennung durch getrennte, kontobezogene Datenspeicher;
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen [soweit vorhanden].

1.5 Pseudonymisierung / Verschlüsselung

- Passwörter werden ausschließlich pseudonymisiert (gehasht und gesalzen) gespeichert;
- Transportverschlüsselung der Datenübertragung; [Verschlüsselung ruhender Daten auf Speicherebene, soweit durch die Hosting-Umgebung unterstützt].

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

2.1 Weitergabekontrolle (Schutz bei Übertragung und Transport)

- verschlüsselte Übertragung sämtlicher Daten über TLS/HTTPS;
- keine Weitergabe von Daten an Dritte außerhalb der in Anlage 3 genannten Unterauftragsverarbeiter.

2.2 Eingabekontrolle (Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen)

- Erfassung von Erstellungszeitpunkten zu Datensätzen;
- Löschungen erfolgen zunächst über einen wiederherstellbaren Papierkorb und werden erst durch dessen Bereinigung endgültig; [ergänzende Protokollierung sicherheitsrelevanter Ereignisse nach Maßgabe der Betriebsumgebung].

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

3.1 Verfügbarkeitskontrolle

- regelmäßige Datensicherung (Backup) der Nutzerdaten und Dateien; [Sicherungsintervall und Aufbewahrung durch den Betreiber festzulegen];
- Möglichkeit des Datenexports und der Datenwiederherstellung über eine integrierte Sicherungs- und Rückspielfunktion;
- Schutz vor konkurrierenden Schreibzugriffen durch Sperrmechanismen (Dateisperren) zur Wahrung der Datenkonsistenz;
- Einsatz von Schutzmaßnahmen gegen Schadsoftware und unbefugte Zugriffe auf Serverebene (z. B. Firewall, aktuelle Sicherheitsupdates); [durch den Betreiber sicherzustellen].

3.2 Rasche Wiederherstellbarkeit

- Wiederherstellung der Daten aus Sicherungskopien innerhalb einer angemessenen Frist im Falle eines physischen oder technischen Zwischenfalls.

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

- regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen;
- Einspielen sicherheitsrelevanter Aktualisierungen der eingesetzten Software- und Serverkomponenten;

- Prozess zur Behandlung von Sicherheitsvorfällen und Datenschutzverletzungen (Incident-Response) einschließlich Meldung an den Auftraggeber gemäß § 8 des Vertrages;
- Auftragskontrolle: Verarbeitung ausschließlich im Rahmen der Weisungen des Auftraggebers;
- Verpflichtung der eingesetzten Personen auf die Vertraulichkeit und Einweisung in die datenschutzrechtlichen Anforderungen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter und Orte der Verarbeitung

Der Auftraggeber genehmigt den Einsatz der folgenden Unterauftragsverarbeiter:

- All-Inkl.com, Hauptstraße 68, Friedersdorf: Dienstleister für Webhosting

Sämtliche Verarbeitungsorte liegen innerhalb der EU/des EWR. Erfolgt der Betrieb ausschließlich auf einer vom Auftragnehmer selbst betriebenen bzw. selbst gehosteten Infrastruktur ohne Einschaltung Dritter, ist dies hier zu vermerken; in diesem Fall werden derzeit keine Unterauftragsverarbeiter eingesetzt.

Anlage 4 – Weisungsberechtigte und weisungsempfangsberechtigte Personen

Datenschutzbeauftragter / für den Datenschutz zuständige Ansprechperson des Auftragnehmers: RA Dominik Josef Hofrichter, Seeleinsbühlstraße 15, 94031 Nürnberg.