

Zeitlich befristete Vereinbarung über die Auftragsverarbeitung
personenbezogener Daten nach EU-Datenschutz-Grundverordnung (AV-
Vertrag)

zwischen dem Interessenten

(Firma, Straße, PLZ & Ort)

und der

Software24.com GmbH, Eichbichlstraße 1, 83071 Stephanskirchen

Als Interessent für Win-CASA der Software24.com GmbH haben Sie eine Online-Präsentation gebucht. Diese erfolgt über eine Fernwartungsverbindung. Der Mitarbeiter des Support-Teams erhält damit Einsicht in eventuell bereits erfasste personenbezogene Daten (Mieter, Eigentümer, Kontakte, Lieferanten).

Art und Ablauf der Verarbeitung: Der Mitarbeiter schaltet sich auf Ihren Arbeitsplatz und erläutert Ihnen die Funktionen von Win-CASA. Die Daten werden nur zur Veranschaulichung betrachtet.

In speziellen Fällen werden zur Veranschaulichung kurzzeitig Daten geändert, jedoch nicht verarbeitet. Die Dauer der Verarbeitung der Daten ist auf die einzelne Präsentation beschränkt. Der Kreis der Personen, die durch die Auftragsverarbeitung mit den personenbezogenen Daten im Rahmen der Präsentation des Problems in Kontakt kommen, ist auf den Supportmitarbeiter und Interessenten begrenzt. Im Ausnahmefall zieht der Supportmitarbeiter den Leiter der Supportabteilung hinzu. Zu den technischen und organisatorischen Maßnahmen gehört, dass der Rechner des Supportmitarbeiters kennwortgeschützt ist und eine intakte Firewall aktiv ist.


Nach Beendigung der Präsentation wird vom Supportmitarbeiter am Arbeitsplatz unverzüglich die Fernwartung beendet. Dadurch erlischt die Einsicht auf die Daten des Kunden komplett.

Ort, Datum

Stephanskirchen, 23. April 2018

Ort, Datum

Unterschrift Auftraggeber (Kunde)



Unterschrift Auftragnehmer

(Software24.com GmbH vertreten
durch den Geschäftsführer Uwe Fernengel)

Bitte beachten Sie, dass diese Vereinbarung nur gültig ist, wenn alle Angaben im Kopf des Dokumentes ausgefüllt sind. Eine Unterschrift allein ist unzureichend.

Zeitlich befristete Vereinbarung über die Auftragsverarbeitung personenbezogener Daten nach EU-Datenschutz-Grundverordnung

zwischen dem Win-CASA Kunden der Software24.com GmbH - nachstehend **Auftraggeber** genannt - und der **Software24.com GmbH, Eichbichlstr. 1, 83071 Stephanskirchen** - nachstehend **Auftragnehmer** genannt.

1. Einleitung, Geltungsbereich, Definitionen

- (1) Diese Vereinbarung regelt die Rechte und Pflichten von **Auftraggeber** und **Auftragnehmer** im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag sowie für die Fernwartung. Auftraggeber und Auftragnehmer werden im Folgenden „Parteien“ genannt,
- (2) Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeiten.
- (3) In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1. Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

1. Präsentation der Softwarefunktionen gemäß Auftraggeberwunsch.

Die Verarbeitung geschieht einmalig und endet unverzüglich nach Beendigung der Präsentation.

Die Vereinbarung ist unabhängig von einem eventuellen zusätzlichen Support- & Software-Vertrag nach Erwerb der Software.

2.2. Dauer

Die Verarbeitung beginnt am Tag der Präsentation und endet nach dieser unweigerlich. Eine Präsentation endet spätestens nach 45 Minuten.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1. Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Anpassung oder Veränderung, Darstellung der Funktionsweise der Software.

Die Verarbeitung dient folgendem Zweck: Präsentation gemäß Auftraggeberwunsch.

3.2. Art der Daten

Es werden folgende Daten verarbeitet:

Die vom Auftraggeber erfassten Daten in der Win-CASA Datenbank. Dazu gehören personenbezogene Daten von Mietern, Eigentümern und Kontakten, Lieferanten sowie Buchhaltungsdaten. Dazu zählen Name, Anschrift, E-Mail-Adressen und Bankdaten.

Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen,

teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- (7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Datenschutzbeauftragter ist Herr Rico Hummel, r.hummel@software24.com, Eichbichlstraße 1, 83071 Stephanskirchen. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.
- (11) Kann der Auftragnehmer den Auftraggeber aufgrund von fehlenden Informationen nicht eindeutig zuordnen (z.B. keine Signatur in der E-Mail) wird die Datensicherung nicht eingelesen und verarbeitet. Der Auftraggeber wird benachrichtigt, die Informationen nachzuliefern. Erfolgt diese nicht, wird die E-Mail gelöscht.

4. Technische und organisatorische Maßnahmen

- (1) Die im Anhang 1 und Anhang 2 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete

Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren. Der Auftragnehmer verpflichtet sich bei technischen Maßnahmen im wirtschaftlich vertretbaren Maße den Stand der Technik einzuhalten.
- (3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- (6) Die Verarbeitung von Daten in Privatwohnungen ist ausgeschlossen. Sie erfolgt ausschließlich in den Räumlichkeiten des Auftragnehmers.
- (7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

5. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieser Vereinbarung hinaus Folge leisten. Sollte der Auftragnehmer bei einer Weisung des Auftraggebers datenschutzrechtliche Bedenken haben, wird der Auftragnehmer den Auftraggeber unverzüglich darauf hinweisen.

6. Unterauftragsverhältnisse mit Subunternehmern

- (1) Die folgenden Regelungen gelten nicht für die in der Anlage 3 aufgeführten Subunternehmer, in deren Einsatz der Auftraggeber hiermit einwilligt.
- (2) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung gestattet. Weitere Subunternehmer als in Anlage 3 aufgelistet sind nicht erforderlich.
- (3) Der Auftragnehmer hat vertraglich sichergestellt, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und Subunternehmers deutlich voneinander abgegrenzt werden.
- (4) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.

7. Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
- (5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als einmal im Kalenderjahr statt. Die Aufwandsentschädigung für Kontrollen wird dem Auftraggeber pro begonnene Stunde mit 200,00 Euro brutto berechnet.

8. Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9. Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 2.
- (3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10. Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt Schutzklasse 2.
- (2) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vereinbarungsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vereinbarungsende übergeben.

11. Vergütung

Die Online-Präsentation ist kostenfrei und begrenzt auf 20 Minuten.

12. Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- (2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
- (3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vereinbarungsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
- (4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13. Sonderkündigungsrecht

- (1) Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen

Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vereinbarungswidrig verweigert.

- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
- (4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieser Vereinbarung in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

14. Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vereinbarungsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung der Vereinbarung vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 – Auftragsverarbeitung: Technische und organisatorische Maßnahmen

Software24.com GmbH
Vertreten durch Herrn Uwe Fernengel (GF)
Eichbichlstraße 1
83071 Stephanskirchen

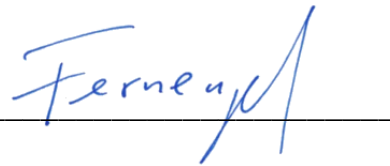
Stand 23.01.2020

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Der Auftragnehmer bestätigt für die folgenden Angaben die Richtigkeit.

Stephanskirchen, 23.01.2020

Ort, Datum, Unterschrift des Auftragnehmers



Beschreibung Fernwartung

Gegenstand dieser Vereinbarung ist die Durchführung von Fernwartungsarbeiten durch die Firma Software24.com GmbH (Auftragnehmer) auf dem EDV-System des Kunden (Auftraggeber), die zur Wartung oder Problembeseitigung für das von dem Kunden erworbene Softwareprodukt Win-CASA der Firma Software24.com GmbH erforderlich sind.

Der Auftraggeber verpflichtet sich, für die Fernwartungssitzungen nur das von dem Auftragnehmer eingesetzte Kommunikationsprogramm zu verwenden. Eine Fernwartung erfolgt jedoch nur auf ausdrückliche Weisung des Kunden. Die Fernwartungsleistungen werden von Montag bis Donnerstag in der Zeit von 9.00 – 12.00 und 14.00 bis 17.00 Uhr, am Freitag von 9.00 bis 12.00 Uhr durchgeführt. Außerhalb der Geschäftszeiten des Auftragnehmers werden keine Fernwartungsleistungen erbracht.

Der Aufbau der Fernwartungsverbindung findet nur in Abstimmung mit dem Kunden statt. Die Datenübertragung erfolgt verschlüsselt. Nach Beendigung der Fernwartungsarbeiten wird die Verbindung unverzüglich beendet. Der Kunde räumt der Firma Software24.com GmbH die notwendigen Rechte zur Fernwartung über die eingesetzte Fernwartungslösung ein. Der Kunde hat das Recht und die Möglichkeit, die Fernwartungssitzung jederzeit zu trennen. Die Firma Software24.com GmbH wird Kundendateien im Wege eines Filetransfers oder Downloads nur für Zwecke der Fehleranalyse und -Beseitigung vom EDV-System des Kunden abziehen und auf ihr eigenes kopieren. Auf den PC des Kunden zu übertragende Dateien werden vorher mit einem aktuellen Virensuchprogramm überprüft. Die Firma Software24.com GmbH wird Daten des Kunden, die während der Fernwartung ausgetauscht wurden, unverzüglich löschen, wenn sie zur Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

Beschreibung Auftragsverarbeitung

Die vom Auftraggeber überlassenen kennwortgeschützte Datenbank in Form einer komprimierten Datensicherung (von Win-CASA unter Datenbank – Datensicherung erstellt) wird i.d.R. vom Auftragnehmer bearbeitet und an den Auftraggeber als komprimierte und kennwortgeschützte neue Datensicherung zurückgesendet. **Nach 14 Tagen wird diese Datensicherung und die dazugehörige Datenbank beim Auftragnehmer gelöscht. Ebenso wird der Anhang der vom Auftraggeber erhaltenen E-Mail (=Datensicherung) beim Auftragnehmer gelöscht.** Evtl. Verzögerungen bei der Verarbeitung werden dem Kunden unverzüglich mitgeteilt. **Während der Fernwartung bzw. während die Datenbank beim Auftragnehmer verarbeitet wird, werden folgende technische und organisatorische Maßnahmen eingehalten:**

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

1. Zutrittskontrolle

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

A.	Serverseitig getroffene Zutrittskontrollmaßnahmen
01.01	Der Server wird durch den Auftragnehmer selbst betrieben und befindet sich innerhalb des Unternehmens vom Auftragnehmer.
01.02	Der Standort des Servers befindet sich am folgenden Ort (Angabe von Stockwerk und Gegebenheit des Raumes (z. B. fensterlos): Kellergeschoss, fensterlos
01.03	Betriebsfremde Personen werden zum Raum des Servers persönlich begleitet.
01.04	Der Raum des Servers hat ein mechanisches Schloss. Die Ausgabe wird protokolliert.
01.05	Die Zutrittsberechtigungen sind personenbezogen und auf ein Minimum vergeben.
01.06	Der Raum des Servers ist videoüberwacht. Die Bilddaten werden gespeichert.
B.	Clientseitig getroffene Zutrittskontrollmaßnahmen
01.07	Die Adresse der Clientarbeitsplätze ist identisch dem Ort der Serverinfrastruktur.
01.08	Das Bürogebäude des Firmensitzes ist vollständig umfriedet.
01.09	Die Ausgabe der Schlüssel wird protokolliert.
01.10	Das Bürogebäude ist videoüberwacht. Die Bilddaten werden nicht gespeichert.

2. Zugangskontrolle

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

02.01	Ein persönlicher Passwort-Benutzername-Zugangsschutz zu den Systemen ist vorhanden.
02.02	Für die Administration der Systeme ist ein eigenständiger ADMIN-Account vorhanden.
02.03	Es existieren verbindliche Vorgaben zum manuellen Sperren des Clients, z. B. beim Verlassen des Arbeitsplatzes.
02.04	Bei Verlust/ Vergessen/ Ausspähen eines Passwortes wird das Passwort umgehend geändert.
02.05	Eine Begrenzung von Anmeldeversuchen ist vorhanden.
02.06	Es existieren passwortgesicherte und verschlüsselte Fernzugänge.
02.07	Die Systeme sind mit einer Firewall abgesichert. Die Firewall wird regelmäßig upgedatet.
02.08	Mobile Endgeräte und weitere Speichermedien sind verschlüsselt.

3. Zugriffskontrolle

Maßnahmen, die 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.

03.01	Es existiert ein differenzierendes Berechtigungskonzept.
03.02	Bedarfsgerechte Rechtevergabe bei Mitarbeitern
03.03	Eine Protokollierung der Zugriffe auf Daten findet statt.
03.04	Es wird kein Testsystem benötigt, somit ist die Trennung von Produktiv- und Testsystemen resultierend.
03.05	Nicht mehr benötigte <u>Datenträger</u> mit personenbezogenen Daten werden durch einen externen Dienstleister datenschutzkonform vernichtet.
03.06	Nicht mehr benötigte <u>Unterlagen</u> mit personenbezogenen Daten werden durch einen externen Dienstleister datenschutzkonform vernichtet.

4. Trennungskontrolle

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

04.01	Je nach Funktion im Unternehmen existieren unterschiedliche Zugriffsrechte.
-------	---

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

05.01	Es werden keine Testsysteme verwendet. Somit resultiert eine Trennung von Produktiv- und Testsystemen.
-------	--

b. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

6. 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.

06.01	Schützenswerte personenbezogene digitale Daten werden bei ihrer Übertragung verschlüsselt bzw. per Passwort geschützt.
06.02	Nutzung eines Virtual Private Network (VPN) für den Zugriff auf Daten

7. 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.

07.01	Zugriffe auf Daten werden protokolliert.	
-------	--	--

c. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

8. Verfügbarkeitskontrolle

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

A.	Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen
08.01	Datensicherungen erfolgen regelmäßig.
08.02	Die Datensicherungen sind verschlüsselt.
08.03	Die Datensicherungen werden extern aufbewahrt (getrennter Brandabschnitt)
08.04	Der Serverraum verfügt über eine feuerfeste/ feuerhemmende Zugangstür
08.05	Der Serverraum ist klimatisiert.
08.06	Der Serverraum verfügt über eine unterbrechungsfreie Stromversorgung.
08.07	Ein dokumentiertes Backup Konzept ist vorhanden.

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

9. Auftragskontrolle

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

09.01	Das Unternehmen hat auf freiwilliger Basis einen Datenschutzbeauftragten (DSB) bestellt.
09.02	Die Mitarbeiter werden regelmäßig im Datenschutzrecht geschult.
09.03	Die Mitarbeiter werden schriftlich auf das Datengeheimnis verpflichtet.
09.04	Dienstleister werden auf deren Qualifikation geachtet.
09.05	Mit Dienstleistern werden schriftliche Verträge geschlossen.
09.06	Mit Dienstleistern wird, sofern notwendig, eine ADV-Vereinbarung geschlossen.
09.07	Prüfung der TOM-Dokumentation (Technische und organisatorische Maßnahmen) des Auftragnehmers
09.08	Regelmäßige Bewertung, Verbesserung und Prüfung der bestehenden TOM-Dokumentation

10. Datenschutz-Management

Zentrale Verwaltung, Nachvollziehbarkeit und Protokollierung des aktuellen Datenschutzniveaus im Unternehmen

10.01	Nutzung eines durch den DSB gepflegten Datenschutzmanagementsystems (<i>zentrale und strukturierte Ablage mit Nachweismöglichkeiten</i>)
-------	--

11. Incident-Response-Management

Umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT/Datenschutz-Bereichen berücksichtigen.

11.01	Es sind Meldewege und Meldeprozesse bekannt.
-------	--

12. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Einstellungen von Soft- und Hardware vor Nutzung und Herausgabe an Benutzer bzw. Kunden.

12.01	Beachtung bei der App-Entwicklung
12.02	Beachtung bei der Softwareprogrammierung

Anlage 2 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:
Leiter der technischen Abteilung (Herr René Hoffmann, Herr Uwe Fernengel), sowie deren mit dieser Aufgabe betrauten weisungsgebundenen Mitarbeiter.

Anlage 3 – Genehmigte Subunternehmer

Folgende Subunternehmer sind mit Unterzeichnung des Vertrages genehmigt:

roNet GmbH Internet-Service-Provider	Äußere Oberaustraße 36, 83026 Rosenheim	Hosting des Portales unter www.meineVerwaltung24.de , dies betrifft ausschließlich Kunden, die eine Portalmitgliedschaft mit der Software24.com GmbH abgeschlossen haben
Deutsche Post AG, Abteilung E-Post	Charles-de-Gaulle-Straße 20, 53113 Bonn	Mailingaktionen und aktuelle Kundeninformationen über die Produkte der Software24.com GmbH werden in unregelmäßigen Abständen per E-Post versendet
AnyDesk Software GmbH	Friedrichstraße 9, 70176 Stuttgart	Fernwartung, für Kunden mit Software- & Support-Vertrag, bei Online-Schulungen und technischer Wartung
Digitmail GmbH Martin Biersack	Oberaustraße 16, 83026 Rosenheim	Mailingaktionen und aktuelle Kundeninformationen über die Produkte der Software24.com GmbH werden in unregelmäßigen Abständen über digitmail GmbH versendet