AUFTRAGSVERARBEITUNG gemäß Art. 28 DS-GVO

Stand: 02.05.2018

zwischen dem Verantwortlichen

_____ (Unternehmen)

_____ (ggf. Ansprechpartner)

_____ (Straße / Haus-Nr.)

_____ (PLZ / Ort / Land)

im Folgenden „Auftraggeber“

und dem Auftragsverarbeiter

Prof4Net GmbH

Gerlachstr. 47-49

14480 Potsdam

im Folgenden „Auftragnehmer“

Der Auftragnehmer verpflichtet sich als Anbieter gegenüber dem Auftraggeber nach Maßgabe der folgenden Bestimmungen:

1. Gegenstand dieser Vereinbarung und Laufzeit

1.1. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Bereitstellung der vertraglichen Leistungen durch den Auftragnehmer ergeben. Die Regelungen dieser Vereinbarung gelten, soweit durch den Auftragnehmer Leistungen gemäß der bereits bestehenden oder künftig abzuschließenden Verträge zwischen dem Auftraggeber und dem Auftragnehmer (im Folgenden die „Leistungsvereinbarung“) erbracht werden, und dabei ein Zugriff auf personenbezogene Daten des Auftraggebers (im Folgenden „Daten“) nicht ausgeschlossen werden kann. Nicht-personenbezogene Daten des Auftraggebers sind nicht Gegenstand dieser Vereinbarung.

1.2. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Leistungsvereinbarung.

2. Art und Zweck der vorgesehenen Verarbeitung von Daten

2.1. Neben der Pflicht zu regelmäßigen Datensicherungen trägt der Auftraggeber auch Sorge dafür, dass der Auftragnehmer bei der Erbringung der Leistungen möglichst wenig mit Daten des

Auftraggebers in Berührung kommt. Allerdings kann bei der Erbringung der Leistungen nicht vollständig ausgeschlossen werden, dass der Auftragnehmer Daten des Auftraggebers zur Kenntnis nehmen kann, insbesondere im Rahmen und zum Zwecke der

a) Softwareinstallation und Updates auf dem Kundenserver
b) Fehlerbehebung und Behebung von Störungen
c) Tests bei Anpassung von Programmen
d) Tests bei Erstellung von neuen Programmen und Änderungen von Programmen
e) Unterstützung des Auftraggebers
f) Fehleranalyse auf Basis von Logfiles oder Reproduktion von Fehlern
g) Unterstützung der Leistungsanpassung/ Nutzungsoptimierung Produkt und Service

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Datenverarbeitungen in anderen Ländern dürfen nur erfolgen, sofern der Auftraggeber zuvor schriftlich zugestimmt hat und zusätzlich die Voraussetzungen der Art.44 bis 47 DS-GVO erfüllt sind oder eine Ausnahme nach Art.49 DS-GVO vorliegt. Vereinzelt werden Leistungen (z.B. Tool zur Onlineschulung, Chatportal etc.) von Firmen aus dem Drittland bezogen. Diese sind im Punkt 6 “Unterauftragnehmer” dargelegt und erfüllen die besonderen Voraussetzungen der Art. 44 ff. DS-GVO. Jede weitere Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2.2. Bei folgenden Arten von Daten des Auftraggebers kommt in Zusammenhang mit den in Punkt 2.1 beschriebenen Leistungen eine Kenntnisnahme-Möglichkeit des Auftragnehmers in Betracht:

a) Daten von Kunden des Auftraggebers

Datenkategorien:
- Personenstammdaten (Kunden, Interessenten, Ansprechpartner)
- Kommunikationsdaten (z.B. E-Mail, Telefon)
- Kundenhistorie (z.B. Anfragen, Leads, Reklamationen, Termine, Notizen)
- Rechnungs-, Angebots- und Auftragshistorien
- Fahrzeugdaten

b) Daten von Benutzern (Mitarbeitern) von CATCH des Auftraggebers, die im Rahmen der Protokollierung der Nutzung dieser Software entstehen. Diese Daten sind in den Logfiles enthalten, welche der Auftraggeber, zu den in 2.1 genannten Zwecken dem Auftragnehmer zur Verfügung stellt.

Datenkategorien:

- Benutzer-ID
- Zeitpunkt der An- und Abmeldung bei der Software
- Daten die zu Mitarbeitern gepflegt werden (z.B. Name, Vorname, E-Mail, Durchwahl)

2.3. Der Kreis der in datenschutzrechtlicher Hinsicht Betroffenen sind Kunden des Auftraggebers und Mitarbeiter des Auftraggebers.

2.4 Der Auftragnehmer nimmt die in 2.2 genannten Daten des Auftraggebers ausschließlich zur Erbringung der Leistungen und nach den in dieser Vereinbarung festgelegten Weisungen des Auftraggebers zur Kenntnis. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, ihm ggf. überlassenen Daten des Auftraggebers ohne Zustimmung des Auftraggebers an Dritte weiterzugeben, soweit nicht die Leistungsvereinbarung mit dem Auftraggeber etwas anderes vorsieht (zu "Unterauftragnehmern" siehe Punkt 6.).

2.5. Der Auftragnehmer verpflichtet sich der RiLi 2000/31/EG, insbesondere den Artikeln (12) bis (15), freier Dienstleistungsverkehr, als Grundlage für das reibungslose Funktionieren des Binnenmarktes. Darauf bezieht sich der Artikel 2 (4) DS-GVO explizit.

3. Pflichten des Auftragnehmers

3.1 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.

3.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

3.3 Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

3.4 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.

3.5 Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags 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 Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

3.6 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.

3.7 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.

3.8 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.

3.9 Der Auftragnehmer stellt eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. 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.

3.10 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 dieses Vertrags erfolgen.

3.11 Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

4. Technische und organisatorische Maßnahmen

4.1 Die im Anhang 1 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.

4.2 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.

4.3 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

4.4 Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4.5 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.

4.6 Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt,

ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

5. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

5.1 Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

5.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6. Unterauftragnehmer

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, welche sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, welche der Auftragnehmer z.B. als Telekommunikations- und Informationsleistungen, Post-/Transportdienstleistungen, im Zahlungsverkehr (Banken, Kreditkarteninstitute), Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2. Der Auftragnehmer ist berechtigt, Unterauftragnehmer einzusetzen. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).Wenn und soweit diesen Unterauftragnehmern personenbezogene Daten des Auftraggebers zugänglich werden, setzt der Auftragnehmer diese Unterauftragnehmer erst nach vorheriger Zustimmung des Auftraggebers ein. Der Auftraggeber wird seine Zustimmung erteilen, wenn nicht schwerwiegende datenschutzrechtliche Gründe entgegenstehen. Die Zustimmung gilt als erteilt, wenn der oder die Betroffene nicht innerhalb der Frist widerspricht. Können sich Auftraggeber und Auftragnehmer nach Ausübung des 4-wöchigen Widerspruchsrechts nicht auf eine einvernehmliche Lösung einigen, kann jede Seite den Hauptvertrag innerhalb von 4 Wochen nach Scheitern der Verhandlungen kündigen (Sonderkündigungsrecht).

6.3. Wenn und soweit den Unterauftragnehmern des Auftragnehmers personenbezogene Daten des Auftraggebers zugänglich sind bzw. werden, verpflichtet der Auftragnehmer den jeweiligen Unterauftragnehmer zu geeigneten technischen und organisatorischen Maßnahmen. Die Weiterleitung von personenbezogenen Daten des Auftraggebers durch den

Auftragnehmer an den Unterauftragnehmer erfolgt erst, nachdem der Unterauftragnehmer entsprechend verpflichtet wurde.

6.4. Erbringt der Unterauftragnehmer die vereinbarten Leistungen außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6.5. Der Auftraggeber hat bereits seine Zustimmung erteilt für die Unterstützung des Auftragnehmers durch folgende Unterauftragnehmer:

Für nicht zur Hauptleistung gehörende (optionale) Nebenleistungen:

Firma	**Anschrift**	**Leistung**	**Datenschutzmaßnahme**
domainfactory	Oskar-Messter-Str. 33 85737 Ismaning	Rechenzentrumsleistungen	AVV
Alfahosting GmbH	Ankerstraße 3b 06108 Halle/Saale	Rechenzentrumsleistungen	AVV
pcvisit Software AG	Manfred-von-Ardenne-Ring 20 01099 Dresden	Fernwartung / Support	AVV

7. Rechte und Pflichten des Auftraggebers

7.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

7.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

7.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

7.4 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.

7.5 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 alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber hat vor der Aufnahme der Datenverarbeitung den Auftragnehmer auch anhand der Geeignetheit der technischen und organisatorischen Maßnahmen des Auftragnehmers sorgfältig ausgewählt.

8.2 Der Auftragnehmer kann dem Auftraggeber die Einhaltung und Umsetzung seines internen Sicherheitskonzepts z.B. durch qualifizierte Selbstauskünfte und ggf. Testate von Sachverständigen auf schriftliche Anforderung des Auftraggebers nachweisen.

8.3 Bei begründetem Verdacht eines schwerwiegenden Verstoßes des Auftragnehmers gegen die Anlage 1 ist der Auftraggeber berechtigt, durch seinen betrieblichen Datenschutzbeauftragten eine angekündigte Vor-Ort-Kontrolle zu den üblichen Bürozeiten vorzunehmen. Die Ankündigung durch den Auftraggeber hat schriftlich zu erfolgen und die Verdachtsgründe zu nennen. Der Auftragnehmer ist verpflichtet, bei der Vor-Ort-Kontrolle gemeinsam mit dem betrieblichen Datenschutzbeauftragten des Auftraggebers eine Begehung der Räumlichkeiten durchzuführen. Der dem Auftragnehmer durch die Vor-Ort-Kontrolle entstehende Mehraufwand ist vom Auftraggeber zu vergüten, es sei denn die Vor-Ort-Kontrolle ergibt, dass sich der Verdacht einer schwerwiegenden Verletzung des Auftragnehmers gegen die Anlage 1 nachweislich bestätigt. Der Auftraggeber ist insoweit nachweispflichtig.

8.4 Der Auftraggeber ist berechtigt, alle Zugriffe, die für die Erbringung der Leistungen erfolgen, in seinem System zu verfolgen und zu protokollieren (Einzelheiten siehe Anlage 1). Der Auftragnehmer verpflichtet sich, eine auftraggeberseitige Protokollierung nicht abzuschalten oder technisch zu unterbinden.

8.5. Auch bei seinen Kontrollen berücksichtigt der Auftraggeber seine Pflichten hinsichtlich Geheimhaltung zum Schutz des Auftragnehmers. Insbesondere ist der Auftraggeber verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen des Auftragnehmers und auftragnehmereigenem Know-How - auch soweit technische und organisatorische Sicherheitsmaßnahmen betroffenen sind - vertraulich zu behandeln.

8.6 Der Auftragnehmer verpflichtet sich, im Falle einer Kontrolle durch die für den Auftraggeber zuständige Datenschutzbehörde der prüfenden Datenschutzaufsichtsbehörde (nachfolgend „Behörde“) im gesetzlich erforderlichen Umfang Zugang zu den Arbeitsräumen zu gewähren und/oder Auskünfte zu erteilen. Er benachrichtigt den Auftraggeber, möglichst bevor eine solche angekündigte behördliche Kontrolle stattfindet. Ist die behördliche Kontrolle durch den Auftraggeber veranlasst, etwa weil bei der Behörde eine Datenschutzbeschwerde über den Auftraggeber eingegangen ist, und entsteht dem Auftragnehmer durch die behördliche Kontrolle oder durch sonstige aufsichtsrechtliche Maßnahmen Mehraufwand, so ist dieser dem Auftragnehmer zu vergüten.

9. Mitteilungspflichten

9.1 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.

9.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontr7ollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4 Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1 Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2 Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 2.

10.3 Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4 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.

10.5 Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

11.1 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.

11.2 Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3 Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

11.4 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Sonstiges

12.1 Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages 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.

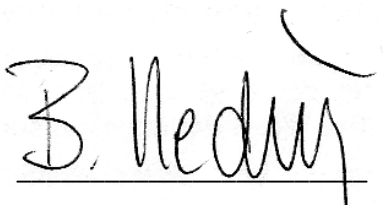
12.2 Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

12.3 Für Nebenabreden ist die Schriftform erforderlich.

12.4 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

12.5 Der Gerichtsstand ist Potsdam.

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

_____	Potsdam, 22.05.2018_____
Ort, Datum	Ort, Datum
	
_____	
Auftraggeber	Auftragnehmer *Björn Keding* *Geschäftsführer der Prof4net GmbH*

Anlage 1 – technische und organisatorische Maßnahmen

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.

13. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

13.1 Im Rahmen der Verarbeitung von personenbezogenen Daten kommen verschiedene Verschlüsselungsmechanismen (bspw. SSL/SSH-Verschlüsselung bei Übertragung; externer Zugriff per VPN) zum Einsatz.

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

14.1 Zutrittskontrolle Unternehmensräumlichkeiten

- Alle Mitarbeiter wurden dokumentiert geschult, informiert und sensibilisiert. Die Schulungen werden regelmäßig durchgeführt.
- Es wird ein dem Schutzbedarf der Daten angemessenes Schließsystem verwendet.
- Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
- Eine Dokumentation der Schlüsselvergabe wird geführt und laufend aktualisiert.
- Das Gebäude ist verschlossen und kann nur manuell durch die Mitarbeiter geöffnet werden.

14.2 Zutritts- und Zugangsregelungen

- Der Zutritt zu den Räumlichkeiten bzw. der Zugang zu den IT-Diensten ist gegen Unbefugte zu schützen und zu kontrollieren. Hierbei sind verschiedene Rollen festzulegen.
- Für jeden Mitarbeiter sind Berechtigungen für den Zutritt zu Räumlichkeiten, den Zugang zu IT-Diensten und den Zugriff auf Informationen festzulegen. Alle Rechte sind restriktiv zu vergeben und zu dokumentieren. Hierbei sind die zwingenden dienstlichen Erfordernisse zugrunde zu legen.
- Die Authentisierung der Zugangsberechtigung ist durch Passwörter sicherzustellen. Es sind Passwortregeln zu erstellen. Diese werden allen Betroffenen durch Sicherheitshinweise für Benutzer mitgeteilt.
- Der Zugang der Administratoren ist speziell zu sichern. Die Passwörter der Administratoren sind sicher zu verwahren. Den Stellvertretern ist eine eigene Administratoren-Kennung zuzuteilen.
- Bereiche, in denen hoch vertrauliche Informationen verarbeitet werden, sind besonders zu sichern. Nur berechtigte, namentlich benannte Personen haben Zutritt zu diesen Bereichen.
- IT-Systeme im Eingangs- und Empfangsbereich sind so zu sichern, dass Unbefugte keinen unbeobachteten Zugriff nehmen und Informationen nicht eingesehen werden können.

14.3 Verschlüsselung

- Vertrauliche und andere sicherheitsrelevante Daten sind verschlüsselt zu speichern. Sofern im Klartext gespeichert wird, ist beim Netzzugriff die Übertragung zu verschlüsseln.
- Zur Verschlüsselung ist IT-Benutzern auf Antrag ein Programm zur Verfügung zu stellen. Berechtigten IT-Benutzern sind ein öffentlicher und ein geheimer Schlüssel zur Verfügung zu stellen.

14.4 Richtlinien zum Umgang mit mobilen Datenträgern

- Sämtliche mobilen Datenträge (USB-Sticks) sind zu verschlüsseln.
- Dazu sind Container auf dem USB-Sticks anzulegen, die bei Bedarf gemountet werden.
- Dateien dürfen nur im verschlüsselten Container auf den mobilen Datenträgern gespeichert werden.
- Es dürfen keine privaten mobilen Datenträger für das Abspeichern von Firmeninformationen genutzt werden

14.5 Datensicherung/ Archivierung

- Es sind regelmäßig Datensicherungen durchzuführen. Die IT-Benutzer sind dabei zu unterstützen.
- Informationen sind einheitlich und dokumentiert aufzubewahren, so dass sie problemlos wieder aufgefunden werden können.
- Die Sicherungskopie findet zentral und automatisiert auf einem verschlüsselten NAS statt. Dies passiert inkrementell jeden Tag.
- Zusätzlich wird einmal pro Monat ein Image des jeweiligen PCs durchgeführt.
- Die Daten werden auf einem Nas gesichert, dabei sind die Daten auf dem NAS verschlüsselt.
- Die Backups werden einmal pro Monat geprüft und ein Image wird testweise zurückgespielt.
- Zusätzlich wird einmal pro Monat ein verschlüsseltes Backup auf einem externen Datenträger gemacht. Dieser Datenträger wird vom IT-Sicherheitsbeauftragten an einem sicheren Ort außerhalb des Unternehmens aufbewahrt.
- Sicherungskopien sind in gesicherten Behältnissen in einem anderen Brandabschnitt aufzubewahren. Die Datenträger sind eindeutig zu kennzeichnen.

14.6 Notfallvorsorge

- Alle Probleme, die IT-Dienste betreffen, müssen dem IT-Sicherheitsbeauftragten und den Administratoren gemeldet werden. Es sind Verhaltensregeln und Handlungsanweisungen für relevante Schadensereignisse zu definieren und den Mitarbeitern mitzuteilen.
- Sämtliche Sicherheitsprobleme sind dem direkten Vorgesetzten sofort persönlich/telefonisch oder per E-Mail zu melden.
- Der Vorgesetzte hat diese Sicherheitsprobleme zu bewerten und an den IT-Sicherheitsbeauftragen und an die Geschäftsführung weiterzugeben.

14.7 Patch-Management

- Beim Patch-Management schaut der IT-Sicherheitsbeauftragte einmal pro Quartal sämtliche PCs durch und kontrollierte diese mit der Anlage „Patch-Management“.
- Die Prüfung einmal pro Quartal erfolgt vor Ort und es werden vom IT-Sicherheitsbeauftragen Termine mit jedem Mitarbeiter zur Kontrolle vereinbart.

- Dabei werden sämtliche PCs auf Aktualität des Betriebssystems, Office, Virenscanner und Webbrowser kontrolliert. Die PCs aktualisieren sich automatisch, werden aber zusätzlich kontrolliert.

14.8 Clear Desk / Clear-Screen Policy

- Sobald ein Arbeitsplatz für längere Zeit nicht besetzt ist, tritt folgende Regelung in Kraft: Alle sensiblen und vertraulichen Dokumente müssen vom Schreibtisch entfernt und in eine Schublade oder einen Rollcontainer verstaut werden. Dies gilt auch für Speichermedien wie USB-Sticks oder CDs und DVDs.
- Jeglicher Papiermüll, der sensible oder vertrauliche Informationen enthält, muss in den dafür bereitgestellten Datenmüllbehälter entsorgt werden. Unter gar keinen Umständen sollten solche Daten in den üblichen Müll gelangen.
- Am Ende des Arbeitstages werden die Computerarbeitsplätze gesichert. Dazu gehört, dass sämtliche Laptops, Tablets und Massenspeichergeräte in Schubladen oder Rollcontainer deponiert und verschlossen werden. Die jeweiligen Schlüssel sollten nicht an der Schublade oder dem Rollcontainer vergessen werden. Gleiches gilt für Drucker und Faxgeräte: Hinterlassen Sie keine ausgedruckten Daten mit vertraulichen Informationen dort.
- Ähnliches gilt auch für die Computer:
    - Beim Verlassen des Arbeitsplatzes muss jeder Benutzer sich am PC abmelden.
    - Wenn nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann der Computer stattdessen gesperrt werden (z.B. „Windows-Taste +

15 Integrität (Art. 32 Abs. 1 DSGVO)

15.1 Weitergabekontrolle

- Ein physischer Versand von Datenträgern ist nicht vorgesehen.
- Verbot des Einsatzes privater Datenträger.
- Nicht mehr benötigte Datenträger werden durch Dienstleister zerstört.
- Alle zum Transport oder für die Übertragung vorgesehenen sensitiven Daten werden verschlüsselt.
- Der Schutz personenbezogener Daten beim physischen Transport bzw. bei der elektronischen Übermittlung wird durch folgende Maßnahmen sichergestellt:
    - Verschlüsselung von Datenträgern
    - ausschließliche Nutzung von durch die IT freigegeben Systeme
    - SFTP-Server
    - VPN

- Folgende Sicherheitsmaßnahmen existieren:
    - Hardware- und Software-Firewall
    - Programme, die das Eindringen von Viren verhindern bzw. das Eindringen erkennen
    - Erkennung und Markierung von SPAM
    - Nur freigegebene Dienste dürfen genutzt werden
    - Für mobile Arbeitsplätze und Heimarbeitsplätze existieren VPN-Zugänge zum Unternehmensnetzwerk

15.2 Eingabekontrolle

- Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden
- sind, kann nachträglich überprüft und festgestellt werden durch:
    - Benutzerprofile
    - Benutzeridentifikation
    - Protokollierung eingegebener Daten (Verarbeitungsprotokoll)
    - Protokollierung der Eingabe, Änderung und Löschung von Daten

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

Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch:

- Einsatz von RAID-Festplattensystemen
- Einsatz von USV inkl. Überspannungsschutz
- In den Unternehmensräumlichkeiten: Betrieb einer Alarmanlage inkl. Weiterleitung an Leitstelle, Feuerwehr, Wachdienst
- Mehrfache Datenbank- und Systembackups.
- Alle wichtigen DV-Systeme werden vom Backup-System abgedeckt.
- Konzept zur Rekonstruktion der Datenbestände (Backup/Restore-Konzept).
- Virenschutzprogramme/Anti-Malwareprogramme sind vorhanden und aktuell.
- Notfallpläne sind vorhanden und werden regelmäßig geprobt.

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

16.1 Datenschutz-Management

Die Prof4Net GmbH hat eine IT-Sicherheitsrichtlinie definiert, die durch den Datenschutzbeauftragten geprüft und permanent weitergepflegt wird. Die IT-Sicherheitsrichtlinie beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.

16.2 Incident-Response-Management

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/ Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

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

Grundsätzlich werden nur Daten erhoben und verarbeitet, welche für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden. Die Software kann vom Kunden selbst angepasst und verwaltet werden. Eine Löschung/ Berichtigung der Daten im System seitens des Kunden ist möglich.

16.4 Auftragskontrolle

- Die Mitarbeiter sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen unterzeichnet.
- Sollte der Auftragnehmer bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DS-GVO i.V.m. Art 32 Abs. 1 DS-GVO.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitung zur Verfügung, welche entsprechende Regelungen zur Kontrolle enthält:
  - Sorgfältige Auswahl des Auftragnehmers,
  - Eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen
  - Klare und eindeutige Erteilung von Weisungen (schriftliche Form), sowie Festlegung der zur Erteilung und zum Empfang von Weisungen berechtigten Personen,
  - Kontrolle der bei dem Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen,
  - Regelung des Einsatzes von Unterauftragnehmern,
  - soweit erforderlich, Bestellung eines Datenschutzbeauftragten bei dem Auftragnehmer

17 Sicherheitsmaßnahmen speziell bei Fernwartung

- Sofern der Auftragnehmer für Wartungsmaßnahmen auf das System des Auftraggebers zugreifen muss, ist dieser Vorgang mit dem Auftraggeber vorab abzustimmen.
- Der Auftraggeber ergreift technische Maßnahmen, um die Zugriffe des Auftragnehmers auf sein System fortlaufend zu überwachen und zu protokollieren. Der Auftraggeber stellt durch Protokollierung der Fernwartungszugriffe sicher, dass alle Fernwartungszugriffe nach der Durchführung nachvollzogen werden können. Der Auftraggeber bewahrt die Dokumentation drei Jahre auf.
- Der Auftraggeber ist berechtigt, den Fernwartungsvorgang von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen. Sofern der Fernwartungsvorgang unterbrochen wird, wird der Auftragnehmer insbesondere von seinen Verpflichtungen bezüglich Reaktionszeit, Herstellungszeiten etc. entbunden.
- Der Auftragnehmer darf personenbezogene Daten im Wege einer Dateiübertragung oder Downloads für Zwecke der Fehleranalyse und -behebung nur dann von den Datenverarbeitungssystemen des Auftraggebers abziehen und auf sein eigenes kopieren, wenn er dafür zuvor die Zustimmung des Auftraggebers eingeholt hat.
- Personenbezogene Daten, die der Auftragnehmer beim Fernzugriff erhalten hat, wird der Auftragnehmer unverzüglich löschen oder dem Auftraggeber zurückgeben, wenn diese Daten für die Durchführung der Leistungen des Auftragnehmers nach dem Wartungsvertrag nicht mehr erforderlich sind. Etwaige dem Auftragnehmer übergebene Papierausdrucke mit personenbezogenen Daten muss der Auftragnehmer nach Abschluss der Wartungs-/Pflegearbeiten gemäß dem Wartungsvertrag unverzüglich zurückgeben oder mit Zustimmung des Auftraggebers datenschutzgerecht vernichten.

- Dies gilt nicht für Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Fernwartung benötigt werden.

18 Sicherheitsmaßnahmen speziell bei Supportanfragen

- Namen von Mitarbeitern des Auftraggebers sowie personenbezogene Fehlermeldungen, Bedienungsfehler/ -probleme oder sonstige personenbezogene Störungen werden vom Auftragnehmer nur erhoben, verarbeitet und genutzt, soweit dies zur Bearbeitung von telefonischen oder Email-Support-Anfragen gemäß der Leistungsvereinbarung erforderlich ist.
- Der Auftraggeber stellt sicher, dass Daten aus Log-Files von Datensicherungen oder sonstige personenbezogene Dateien nur insoweit an den Auftragnehmer weitergeleitet werden, soweit dies zur ordnungsgemäßen Erbringung der Support-Leistungen notwendig ist.

Anlage 2 – Bestimmung der Kontaktpersonen

Bezüglich der Weisungsbefugnis wird folgendes vereinbart:

a) weisungsberechtigte Personen des Auftraggebers sind:

Name/Vorname	**Funktion**	**E-Mailadresse**

b) Weisungsempfänger beim Auftragnehmer sind die Geschäftsführer, die Teamleiter und der Datenschutzbeauftragte. Die jeweils aktuellen Kontaktmöglichkeiten sind auf der Website des Auftragnehmers leicht zugänglich hinterlegt.