Auftragsverarbeitung gemäß Art. 28 DSGVO
Vereinbarung

zwischen dem/der

_____
– Verantwortlicher - nachstehend Auftraggeber genannt –

und

Jan Hardt, Hochwinkel 18, 51069 Köln - Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1) Gegenstand und Dauer des Auftrags

(1) Gegenstand

Die Vereinbarung bezieht sich auf die Wartung - und Supporttätigkeiten über die Fernwartung und den Service vor Ort.

Die Fernwartung bezieht sich in der Regel auf Netzwerkadministration sowie Support und Anfragen vom Auftraggeber und dessen Mitarbeiter. Mit Start der Fernwartungssoftware Teamviewer oder ähnlicher Programme gestattet der Auftraggeber dem Auftragnehmer die Einsicht auf seinen PC und auch die Fernsteuerung des PCs mit der Möglichkeit der Datenveränderung.

(2) Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) gilt bis auf Widerruf und beginnt mit dem Datum der Unterschrift.

2) Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Art und der Zweck des Vertrages umfassen Hilfeleistungen, Unterstützung bei Problemen, die Analyse von Fehlern und Ablaufstörungen, die Suche nach technischen Fehlerursachen, Lösungsvorschlage und deren Umsetzung,Wartung und Supporttätigkeiten. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung von Daten in ein Drittland ist ausgeschlossen. Der Ort von dem aus die Fernwartung stattfindet ist davon nicht betroffen.

(2) Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung sind personenbezogene Daten, die sowohl Kundendaten (Personenstammdaten oder ähnliches) als auch Patientendaten umfasst.

(3) Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst Patientendaten i. S. d. § 3 Abs. 11 BDSG.

3) Pflichten des Auftraggebers
Der Auftraggeber hat seine Datenbestände und EDV-Anlagen durch geeignete organisatorische und technische Vorkehrungen wie z.B. Virenscanner, Firewalls und Passwortschutz ausreichend zu schützen.
Der Auftraggeber trägt selbst die Verantwortung für eine aktuelle Datensicherung in angemessener Form.
Diese Sicherung muss auch eine zeitnahe und wirtschaftlich vernünftige Wiederherstellung der Daten garantieren.
Der Auftraggeber hat sicherzustellen, dass die Verarbeitung und Nutzung von personenbezogenen Daten auf seinen EDV-Anlagen unter Beachtung der jeweiligen Datenschutzvorschriften, insbesondere des Bundesdatenschutzgesetzes erfolgt und auch den für den Auftraggeber gegebenenfalls besonders geltenden Datenschutzvorschriften Rechnung trägt.

4) Technisch-organisatorische Maßnahmen
Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.
Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als „Anlage 1“ zu diesem Vertrag beigefügt gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbe-sondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO.
Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

5) Berichtigung, Einschränkung und Löschung von Daten
Nach Aufforderung des Auftragsgebers und nach vorheriger Bestätigung des Auftragsgebers nimmt der Auftragsnehmer Änderungen an dem Datenbestand des Auftragsgebers vor. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren.

6) Datengeheimnis / Qualitätssicherung und sonstige Pflichten des Auftragnehmers
Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
a) Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend

der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
b) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

7) Unterauftragsverhältnisse
a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, 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.
b) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Mitarbeit von Gerhard Gengenbacher, Hochwinkel 18, 51069 Köln ist hiermit dokumentiert und genehmigt.
c) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
d) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Davon ausgenommen sind Fernwartungen, sofern bei diesen nur der Bildschirm abgegriffen wird und keinerlei Daten auf Datenträgern außerhalb der EU gespeichert werden.
e) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

8) Kontrollrechte des Auftraggebers
Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.
Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, ITSicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

9) Mitteilung bei Verstößen des Auftragnehmers
(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.
a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsgebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10)Weisungsbefugnis des Auftraggebers
(1) Mündliche Weisungen werden beim Auftragsnehmer in der Kunden- bzw. Rechnungsverwaltung dokumentiert
(2) Der Auftragnehmer hat den Auftraggeber zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11)Löschung und Rückgabe von personenbezogenen Daten
(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger

Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12) Geheimhaltung
Der Auftragnehmer ist verpflichtet, über alle vertraulichen Informationen vom Auftraggeber Stillschweigen gegenüber jedermann zu bewahren, diese Vertraulichen Informationen weder in mündlicher, schriftlicher noch anderer Form an Dritte weiterzugeben oder zugänglich zu machen und die Kenntnisse nicht zum Nachteil des Auftraggebers zu verwenden.
Der Auftragnehmer wird alle nötigen Sicherheits- und Vorsichtmaßnahmen ergreifen, um sicherzustellen, dass mit sämtlichen seiner gesetzlichen Vertreter, leitenden Angestellten, Angestellten und Beratern, an die die Auftragnehmer die Vertraulichen Informationen weitergeben möchten, eine Geheimhaltungsvereinbarung abgeschlossen worden ist, die mindestens ebenso weitreichende Schutzbestimmungen enthält wie die vorliegende Geheimhaltungsvereinbarung.
Die Verpflichtungen zur Geheimhaltung einschließlich der bei einem Verstoß vereinbarten Rechtsfolgen gelten zeitlich unbeschränkt und insbesondere auch über die Dauer des jeweiligen Vertragsverhältnisses und der vorliegenden Geheimhaltungsvereinbarung hinaus.
Für den Fall, dass der Auftragnehmer rechtlich verpflichtet ist, vertrauliche Informationen gegenüber Dritten oder Behörden zu offenbaren, ist der Auftragnehmer zu einer solchen Offenbarung berechtigt. Der Auftragnehmer wird dem Auftraggeber in dem Fall der gesetzlichen Verpflichtung unverzüglich (nachdem der Auftragnehmer selbst Kenntnis von dieser Verpflichtung erlangt hat) unterrichten.

13) Gewährleistung /Haftung
Jan Hardt haftet für Vorsatz und grobe Fahrlässigkeit. Für leichte Fahrlässigkeit haftet er nur bei Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht), deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf.
Jan Hardt schuldet die branchenübliche Sorgfalt. Bei der Feststellung, ob Jan Hardt ein Verschulden trifft, ist zu berücksichtigen, dass Software technisch nicht fehlerfrei erstellt werden kann.
Die Haftung ist im Falle leichter Fahrlässigkeit summenmäßig beschränkt auf die Höhe des vorhersehbaren Schadens, mit dessen Entstehung typischerweise gerechnet werden muss, maximal ist diese Haftung jedoch beschränkt auf 250 EUR pro Schadensfall und insgesamt auf 1000 EUR.
Für den Verlust von Daten und/oder Programmen haftet Jan Hardt insoweit nicht, als der Schaden darauf beruht, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.
Die vorstehenden Regelungen gelten auch zugunsten der Erfüllungsgehilfen von der Jan Hardt.

13)Salvatorische Klausel
Sollten sich einzelne Bestimmungen dieses Vertrages als ungültig, unwirksam oder unerfüllbar erweisen, so soll dadurch die Gültigkeit, Wirksamkeit und Erfüllbarkeit der übrigen Teile des Vertrages nicht beeinträchtigt werden.

Köln den 10.4.2018

Ort und Datum

Unterschrift Auftragnehmer

_____

Ort und Datum

_____

Unterschrift Auftraggeber

Anlage: Technisch-organisatorische Maßnahmen

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

• Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

- Privathaushalt, bewohnt.
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal

• Zugangskontrolle Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

• Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

• Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit;

- Logische Mandantentrennung (softwareseitig)

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

• Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Verschlüsselung

• Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme ein-gegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

• Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (on-line/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

- Schutzsteckdosenleisten
- Feuerlöschgeräte
- Erstellen von Backups
- Teilweise Aufbewahrung von Datensicherung an einem sicheren Ort
- Serverräume nicht unter sanitären Anlagen