Vereinbarung zur Auftragsverarbeitung gem. Artt. 28 und 29 EU-DSGVO (AV-Vertrag)

zwischen der

Genaue Firmenbezeichnung, Straße und Ort (ggf. Firmenstempel):

_____

_____

_____

_____

- Verantwortlicher - nachstehend Auftraggeber genannt -

michael martin GmbH & Co. KG

Daimlerstraße 42, 69190 Walldorf

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

- Der Gegenstand des Auftrags ergibt sich aus der Bereitstellung und Lieferung der Branchensoftware mmOrthosoft® in allen Varianten und den damit verbundenen Dienstleistungen, die in den jeweiligen Einzelverträgen geregelt sind. (im Folgenden Leistungsvereinbarung).

1.2 Dauer

- Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung und ist an diese gekoppelt.
- Für Rückfragen und für Dokumentationszwecke werden die Daten entsprechend der gesetzlichen Aufbewahrungsfristen weitere 10 Jahre bevorratet und dann gelöscht.
- Auf Anfrage einzelner Personen, können diese Daten nach Ablauf einer Sperrfrist von 36 Monaten auch vorher gelöscht werden.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung laut Anlage:

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.

3. Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

3.3 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. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 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. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. 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:

- Schriftliche Bestellung, soweit nach DSGVO bzw. BDSG-Neu erforderlich, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
- Dessen Kontaktdaten werden ggf. dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird ggf. dem Auftraggeber unverzüglich mitgeteilt.
- Dessen jeweils aktuelle Kontaktdaten sind ggf. auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.

michael martin GmbH & Co.KG, Daimlerstraße 42, D-69190 Walldorf
Sparkasse Heidelberg (BLZ 672 500 20) Konto-Nr. 57 717 920 IBAN: DE70 6725 0020 0057 7179 20 SWIFT-BIC: SOLADES1HDB
Volksbank Walldorf (BLZ 672 922 00) Konto-Nr. 20 018 909 IBAN: DE44 6729 2200 0020 0189 09 SWIFT-BIC: GENODE61WIE
Geschäftsführer: Dipl.-Ing.(FH) Michael Martin, UST ID: DE200331568, SteuerNr: 32074/05166, HRA 350648 Amtsgericht Mannheim

- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

Die michael martin GmbH & Co. KG verarbeitet (Auftragsverarbeitung) personenbezogene Daten im Auftrag des Auftraggebers. Diese Tätigkeiten umfassen alle Dienstleistungen von der michael martin GmbH & Co. KG und nach den jeweiligen vertraglichen Vereinbarungen mit dem Auftraggeber, die eine Auftragsverarbeitung darstellen. Die jeweils aktuell eingesetzten Auftragsverarbeiter sind über unsere tagesaktuelle F&A Datenbank im Internet unter www.funda.mmorthosoft.de im Kapitel „mmO Info Datenschutz / GoBD / QM“ unter „EU-DSGVO: mmGmbH gegenüber mmO Anwendern“ mit der Bezeichnung „2.1 AV-Vertrag Erweiterung der Unterauftragnehmer“ oder unter der ID 181200 ersichtlich. Sofern weitere Unterauftragnehmer in Anspruch genommen oder bisherige Unterauftragnehmer ersetzt werden, erhalten Sie per E-Mail / Fax eine schriftliche Information.

6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- Der Auftraggeber stimmt der Beauftragung der aktuell eingesetzten Unterauftragnehmer gemäß unserer Auflistung der Unterauftragnehmer in der tagesaktuellen F&A Datenbank im Internet unter www.funda.mmorthosoft.de im Kapitel „mmO Info Datenschutz / GoBD / QM“ unter „EU-DSGVO: mmGmbH gegenüber mmO Anwendern“ mit der Bezeichnung „2.1 AV-Vertrag Erweiterung der Unterauftragnehmer“ (ID 181200) unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 DSGVO zu:

- Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
  - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
  - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
  - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 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.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers sowie des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte und Pflichten des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen 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.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz oder DIN-ISO 27001).
- Durch die Akzeptanz der dem Auftraggeber zur Verfügung gestellten technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Dieser darf die tatsächlich entstanden Kosten nicht überschreiten.

mOrthosoft®
michael martin GmbH & Co.KG, Daimlerstraße 42, D-69190 Walldorf
Sparkasse Heidelberg (BLZ 672 500 20) Konto-Nr. 57 717 920 IBAN: DE70 6725 0020 0057 7179 20 SWIFT-BIC: SOLADES1HDB
Volksbank Walldorf (BLZ 672 922 00) Konto-Nr. 20 018 909 IBAN: DE44 6729 2200 0020 0189 09 SWIFT-BIC: GENODE61WIE
Geschäftsführer: Dipl.-Ing.(FH) Michael Martin, UST ID: DE200331568, SteuerNr: 32074/05166, HRA 350648 Amtsgericht Mannheim
Die bewährte Branchenlösung

7.5 Der Auftraggeber verpflichtet sich seinen Transparenzpflichten gemäß Art. 13 DSGVO nachzukommen und die Möglichkeit des Zugriffs durch den Auftragnehmer auf die Software und die damit verbundenen Daten zu erwähnen.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1 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 vorherige Konsultationen. Hierzu gehören u. 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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutzfolgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Schriftform.

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich 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.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 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.

michael martin GmbH & Co.KG, Daimlerstraße 42, D-69190 Walldorf
Sparkasse Heidelberg (BLZ 672 500 20) Konto-Nr. 57 717 920 IBAN: DE70 6725 0020 0057 7179 20 SWIFT-BIC: SOLADES1HDB
Volksbank Walldorf (BLZ 672 922 00) Konto-Nr. 20 018 909 IBAN: DE44 6729 2200 0020 0189 09 SWIFT-BIC: GENODE61WIE
Geschäftsführer: Dipl.-Ing.(FH) Michael Martin, UST ID: DE200331568, SteuerNr: 32074/05166, HRA 350648 Amtsgericht Mannheim

10.2 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.

10.3 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.

Anlage – Technisch-organisatorische Maßnahmen (auf Anforderung)

Eine Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO ist Bestandteil dieses Auftrages und kann beim Auftragnehmer in aktueller Form angefordert werden. Bei Abschluss dieser Vereinbarung wurden die technischen und organisatorischen Maßnahmen durch den Auftraggeber oder durch eine von ihm bevollmächtigten Personen kontrolliert und für ausreichend befunden. Diese zum Datenschutz getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert.

_____

Ort, Datum und Unterschrift des Inhaber / Geschäftsführer / Prokurist

- Auftraggeber – Firma / Firmenstempel_____

Walldorf, 03.04.2019 _____

Ort, Datum und Unterschrift

- Auftragnehmer - michael martin GmbH & Co. KG

Anlage 1: Leistungsvereinbarung

Grundsätzliches:

Die michael martin GmbH & Co. KG stellt ihren Kunden eine umfassende Branchensoftwarelösung für die Zielgruppe der „Sonstigen Leistungserbringer“ zur Verfügung. Neben der ständigen Weiterentwicklung der Branchensoftwarelösung werden weitere Dienstleistungen passend zur Branchensoftware und zum Branchenumfeld angeboten. Diese Leistungen umfassen folgende Schwerpunkte:

- Seminare & Training zur Branchenlösung
- Hotline zur Branchenlösung
- Helpline zur Branchenlösung
- Helpline zu technischen Themen
- Beschaffung und Installation von Daten, Preislisten und Verträgen
- Beschaffung und Installation von IT Komponenten
- Schnittstellenbetreuung
- Individualprogrammierungen
- Fernwartungsarbeiten
- Programmupdates

Kategorien betroffener Personen:

- A) Kunden / Anwender / Interessenten
- B) Lieferanten / freie Mitarbeiter / Handelsvertreter / sonstige Leistungserbringer / Krankenkassen / Abrechnungszentren
- C) Patientendaten von Kunden (Versicherte bzw. andere Betroffene)

Verarbeitung von personenbezogenen Daten der Mitarbeiter und Ansprechpartner der Kategorien A) & B) in der mmFaktura®:

Bei der Betreuung unserer Kunden mit der Branchensoftware mmOrthosoft®, speichern wir personenbezogenen Daten in unserer eigenen Branchensoftware mmFaktura®, der uns bekannten Mitarbeiter und Ansprechpartner der Kategorien A) & B). Je nach Stellung im Unternehmen werden auch Berechtigungen, Weisungsbefugnisse, etc. gespeichert. Folgende Informationen können von den Ansprechpartnern gespeichert werden:

Anrede	Herr/Frau
Name	Mustermann
Straße	Mustermannstraße 1
Land/Plz/Ort	D 00000 Musterstadt
Funktion	z. B. Abteilungsleiter
Prio. Ansprechpartner	x
Erhält Werbeaktion	x

mmOrthosoft®
michael martin GmbH & Co.KG, Daimlerstraße 42, D-69190 Walldorf
Sparkasse Heidelberg (BLZ 672 500 20) Konto-Nr. 57 717 920 IBAN: DE70 6725 0020 0057 7179 20 SWIFT-BIC: SOLADES1HDB
Volksbank Walldorf (BLZ 672 922 00) Konto-Nr. 20 018 909 IBAN: DE44 6729 2200 0020 0189 09 SWIFT-BIC: GENODE61WIE
Geschäftsführer: Dipl.-Ing.(FH) Michael Martin, UST ID: DE200331568, SteuerNr: 32074/05166, HRA 350648 Amtsgericht Mannheim
Die bewährte Branchenlösung

Geburtsdatum	00.00.0000
WKZ	Werbekennzeichen
Telefon 1	00000/000000
Telefon 2	00000/000000
Telefon 3	00000/000000
Fax	00000/000000
Handy	00000/000000
E-Mail	max.mustermann@muster.de
Skype	
Eintritt	00.00.0000
Austritt	00.00.0000
Erfassungsdatum	00.00.0000
Änderungsdatum	00.00.0000
Teilgenommene Seminare	Musterseminar
Hot & Helplineberechtigung	
Vereinbarung Artt. 28 & 29	als PDF

Verarbeitung von personenbezogenen Patientendaten, der Kategorie C) in mmOrthosoft®:

Bei der Betreuung unserer Kunden mit der Branchensoftware mmOrthosoft® unterstützen wir unsere Kunden / Anwender und haben teilweise dabei die Möglichkeit die Realdaten unserer Kunden / Anwender zu sehen, bzw. gemeinsam mit unseren Kunden/ Anwendern zu verarbeiten. Folgende Informationen können von den Ansprechpartnern verarbeitet werden:

Adressdaten:	
Anrede	Herr/Frau
Name	Mustermann
Vorname	Max
Straße	Mustermannstraße 1
Land/Plz/Ort	D 00000 Musterstadt
Kontaktdaten:	
Telefon 1	00000/000000
Telefon 2	00000/000000
Telefon 3	00000/000000
Fax	00000/000000
Handy	00000/000000
E-Mail	max.mustermann@muster.de
Skype	
Homepage	www.mustermann.de

Personenbezogen:	
Ust. ID	0
Geburtsdatum	00.00.0000
Staatsangehörigkeit	deutsch
Geschlecht	weiblich / männlich
Gesundheitsdaten	Behinderungen/Beeinträchtigungen etc.
Maßdaten	Schuhgröße
Körpergröße	000 cm
Gewicht	000 kg
Verstorben	Ja / Nein
Versichertendaten:	
Versicherten-Nr.	000000000000
Mitgliedsstatus	1000
KVK gültig bis	00.00
Krankenkasse	Musterkasse
Zuzahlungspflichtig	Ja / Nein
BG/Ovst (Orthop. Versorgungsstelle)	Musterkasse
Betreuer / Vormund	Name, Vorname
Fotos / Videos	C:/Pfadangabe
Biometrische Daten	C:/Pfadangabe
Rechnungsdaten:	
Rechnungs-Nr.	000000
Positionen	000
Artikel / Name / Bezeichnung	XXXXXX
Anrede	Herr/Frau
Name	Mustermann
Vorname	Max
Straße	Mustermannstraße 1
Land/Plz/Ort	D 00000 Musterstadt
Steuer-ID:	
Steuer-Nr.	1111/12
Bankverbindung:	
Konto-Inhaber	Mustermann, Max
IBAN	00000000000000000000
BIC	AAADES04
Name der Bank	Musterbank
Bankleitzahl	000 000 00
Konto-Nr.	000 00 00 00
Einzugserm. erteilt	Ja / Nein
Mandatsreferenz	000000000000
Signatur	00.00.0000

Auftraggeber:	
Auftraggeber	Mustermann, Max, 00000 Musterstadt
Abteilung	Musterabteilung
Telefon-Nr.	00000/000000
Gebäude / Zimmer-Nr.	00
Theapeut	Dr. Musterarzt
Abrechnung:	
Zahlungsbed.	00 Tage Netto Muster
Mahnen	Ja / Nein
Sperrung	nur Warnung Muster
Grund	Insolvenz Muster
Debitor / Kreditor	0000 / 0000
Arbeitsunfall:	
Arbeitgeber	Firma Mustermann
Aktenzeichen	000/000
Unfalldatum:	00.00.0000
Pflege:	
Pflegestufe	00
Tour	Mustermann
Mitarbeiter	Max Mustermann
Filiale	Musterfiliale
Preisgruppen:	
Material	000 Sani Muster
Bundes-Prothesenliste	000000
Kundengruppen	0000
Notiz	Musternotiz zum Patient
Belege	Musterbeleg zum Patient

EU-DSGVO # Technische und organisatorische Maßnahmen

Aufstellung für Auftraggeber der michael martin GmbH & Co. KG zu den bei der michael martin GmbH & Co. KG getroffenen technischen und organisatorischen Maßnahmen im Datenschutz.

Diese Auflistung der bei der michael martin GmbH & Co. KG getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 9 BDSG(alt) und der Anlage zu § 9 Satz 1 BDSG(alt), diese Dokumentation ermöglicht eine strukturierte Dokumentation der TOMs, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG-neu) dazu Vorgaben für nicht öffentliche Stellen gibt (§ 64 BDSG-neu findet bei nicht öffentlichen Stellen keine Anwendung). Diese Angaben dokumentieren auch die Forderungen des § 78a SGB X und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihre Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Artt. 28 und 29 DSGVO und 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Artt. 28, 29 DSGVO konformen, Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhanden Sicherheitsniveau nicht unterschritten wird.

Die Daten, die bei der michael martin GmbH & Co. KG im Auftrag (im Rahmen von Softwarewartungsarbeiten) eingesehen werden können, sind als besonders sensibel eingestuft. Es handelt sich um personenbezogene Daten gemäß Art. 4 Nr. 1 und um Sozialdaten gemäß § 67 Abs. 1 SGB X in Verbindung mit besonderen Daten gemäß Art. 4 Nr. 15 DSGVO (Gesundheitsdaten).

Ergänzend sei noch erwähnt, dass es bei der michael martin GmbH & Co. KG IT-Notfallpläne, Datensicherungs- und Berechtigungskonzepte und dokumentierte Prozessabläufe gibt.

Allgemeiner Teil:

1. Name und Anschrift des Unternehmens:
   michael martin GmbH & Co. KG
   Daimlerstr. 42
   69190 Walldorf

2. Ansprechpartner mit Telefon, Fax und E-Mail:
   Herr Markus Schäfer, interner Datenschutzkoordinator
   Tel.: +49 6227 8383223
   Fax: +49 6227 838399
   E-Mail: markus.schaefer@mmorthosoft.de

3. Name des Geschäftsführers:
Dipl.-Ing. (FH) Herr Michael Martin

4. Name und Kontaktdaten der Datenschutzbeauftragten:
Herr Joachim Kramer

Kramer & Partner
Dipl.-Ing (FH) Sylvia Kramer & Joachim Kramer GbR
Büro für Datenschutz und Datensicherheit
Elsternweg 24
42555 Velbert
Tel.: 02052 / 92897 -66
Fax: 02052 / 92897 -67
E-Mail: j.kramer@datenschutz-kramer.de

5. Datenschutzbeauftragter:

5.1. Bestellung:
- *externer Datenschutzbeauftragter gem. § 4 f Abs. 2 BDSG(alt) bzw. Art. 37 DSGVO und § 38 BDSG-Neu*
- *schriftliche Bestellung vom 28.02.2018 liegt vor*

5.2. Qualifikation:
- *Datenschutz-Auditor (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV Akademie Rheinland Nr. 19553*
- *über 20 Jahre Erfahrung im IT-Bereich*
- *regelmäßige Fortbildungen*
- *Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO*
- *GDD Mitglied*
- *Firma Kramer & Partner besitzt über 30 Jahre Erfahrung im Datenschutz*

6. Mitarbeiter der michael martin GmbH & Co. KG:
- *alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB, der Vertraulichkeit nach DSGVO, BDSG-Neu und auf das Sozialgeheimnis nach § 35 SGB I verpflichtet worden*
- *die Verpflichtung erfolgte auf einem extra Formular*
- *die der Verpflichtung zugrunde liegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt*
- *die Verpflichtung wird bei Einstellung durch die Personalabteilung vorgenommen*
- *Betriebsvereinbarung über die private Nutzung von E-Mail, Internet und Umgang mit Firmenhardware*
- *alle Mitarbeiter werden in regelmäßigen Abständen durch den bDSB bzw. durch den internen Datenschutzkoordinator geschult*

7. Verfahrensverzeichnisse/Verzeichnis der Verarbeitungstätigkeiten:
- *das „Verzeichnis der Verarbeitungstätigkeiten“ liegt vor*

Technische und organisatorische Maßnahmen:

8. In unserem Haus ist die räumliche **Zutrittskontrolle** folgendermaßen sichergestellt:
   - *Closed-Shop-Betrieb*
   - *eigenes Bürogebäude*
   - *Zutritt in die Geschäftsräume nur über Schlüssel möglich*
   - *Besucher müssen klingeln*
   - *Alarmanlage mit Bewegungsmeldern*
   - *Schlüsselliste und Schlüsselquittungen*
   - *Serverraum zusätzlich mit Zahlencodeschloss verschlossen*
   - *Besucher haben nur in Begleitung von Mitarbeitern Zutritt*

9. Um das unbefugte Eindringen in unsere Systeme und Datenverarbeitungssysteme zu verhindern, verwenden wir folgende **Zugangskontrollen:**
   - *Benutzername und Kennwort*
   - *automatische Sperrung (Pausenschaltung)*
   - *Sperrung des Accounts bei wiederholter Falschanmeldung*
   - *datenschutzgerechte Passwortrichtlinien gem. BSI werden vom Domaincontroller vorgegeben*
   - *Passwortgültigkeit 90 Tage*
   - *Active Directory mit Zugangsprotokoll*
   - *Server mit zusätzlichen Administrator Passwörtern*

10. Wie wird der Zugriff (**Zugriffskontrolle**) auf verschiedene Daten bzw. Systeme geregelt:
    - *durch differenzierte Berechtigungen, gesteuert durch die Anmeldung*
    - *Berechtigungskonzept vorhanden*
    - *extra Administrationspasswörter für die Server mit abgestuften Administrationsrechten*

11. Wir kontrollieren die Weitergabe (**Weitergabekontrolle**) personenbezogener Daten bei Übermittlung bzw. Übertragung oder bei Transport mit folgenden Maßnahmen:
    - *für Fernwartungsarbeiten bei Auftragnehmern wird TeamViewer mit telefonisch übermittelter Sitzungsnummer oder eine VPN-Verbindung eingesetzt*
    - *Weitergabe von Datenträgern nur verschlüsselt (ZIP oder Veracrypt)*

12. Wir gewähren die Nachvollziehbarkeit bzw. Dokumentation der Wartungsarbeiten bzw. Systemzugriffe mit folgenden Maßnahmen (**Eingabekontrolle**). Dadurch kann nachvollzogen werden, wer auf ein System bzw. Daten zugegriffen hat und wann:
    - *durch Protokolle am Domain-Controller*
    - *durch Server Protokolle*
    - *in den Programmen werden bei Erfassung bzw. Änderung von Daten die Mitarbeiterkürzel mit protokolliert*

Orthosoft®
michael martin GmbH & Co.KG, Daimlerstraße 42, D-69190 Walldorf
Sparkasse Heidelberg (BLZ 672 500 20) Konto-Nr. 57 717 920 IBAN: DE70 6725 0020 0057 7179 20 SWIFT-BIC: SOLADES1HDB
Volksbank Walldorf (BLZ 672 922 00) Konto-Nr. 20 018 909 IBAN: DE44 6729 2200 0020 0189 09 SWIFT-BIC: GENODE61WIE
Geschäftsführer: Dipl.-Ing.(FH) Michael Martin, UST ID: DE200331568, SteuerNr: 32074/05166, HRA 350648 Amtsgericht Mannheim
Die bewährte Branchenlösung

13. Die Aufträge (**Auftragskontrolle**) unserer Kunden kontrollieren wir anhand folgender Möglichkeiten:
- *bei Supportanfragen wird ein Ticket erstellt*
- *im Rahmen der mit den Kunden abgeschlossenen AV-Vereinbarungen*

14. Folgende Sicherheitsmaßnahmen (**Verfügbarkeitskontrolle**) haben wir gegen zufällige oder mutwillige Zerstörung und gegen Verlust bzw. Sabotage von Daten ergriffen:
- *alle Server sind mit Raid-Systemen ausgestattet, die die Daten permanent spiegeln*
- *die Raidsysteme der Server melden Plattenausfälle sofort, sodass die Störung, ohne den Betriebsablauf der Kunden zu stören, behoben werden kann*
- *alle Server sind an USVs angeschlossen*
- *automatisiertes Backupverfahren mit Protokollen*
- *Datensicherungskonzept*
- *Virenscanner mit automatischem Update*
- *Datensicherungen in einem anderen Brandabschnitt*
- *separate verschlüsselte Datensicherung bei einem deutschen Cloudanbieter*

15. Um Daten, die zu unterschiedlichen Zwecken erhoben wurden oder um die Daten von Mandanten voneinander zu trennen (**Trennungskontrolle**), haben wir folgende Maßnahmen ergriffen:
- *physikalische Server sind in VM-Server unterteilt*
- *durch interne Mandantenfähigkeit und Authentifizierung der Auftraggeber*
- *verschiedene Systeme sind auch auf unterschiedlichen Servern installiert*

16. Nicht mehr benötigte Daten in Papierform bzw. nicht mehr gebrauchte oder defekte Datenträger, werden bei uns wie folgt entsorgt:
- *Daten in Papierform werden gem. DIN 66399 P3 und P4 datenschutzgerecht in eigenen Schreddern vernichtet*
- *elektronische und optische werden mechanisch selbst zerstört*

Zu erwähnen ist noch, dass es sich bei der michael martin GmbH & Co. KG um ein Softwarehaus handelt. Die Fernwartungen werden selbst mit eigenem Personal durchgeführt.

Velbert, 30.05.2018 J. Kramer

Ort, Datum Joachim Kramer, betrieblicher Datenschutzbeauftragter

Walldorf, 30.05.2018

Ort, Datum Michael Martin, geschäftsführender Inhaber