



Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

**Vereinbarung zum Datenschutz und zur Datensicherheit  
in Auftragsverhältnissen gem. Art. 28 DSGVO  
(Auftragsdatenverarbeitung)**

zwischen dem Auftraggeber:

┌

┐

└

┘

(Praxisstempel)

(nachstehend „AG“ genannt)

und

nemecs GmbH  
Tuchmacherstr. 12a  
84524 Neuötting

(nachstehend „nemecs GmbH“ genannt)

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 1 von 12



## **Präambel**

AG hat nemecs GmbH vertraglich zur Erbringung definierter Leistungen beauftragt. Darüber liegen gesonderte Leistungsverträge vor. Bei diesen Leistungen kann nemecs GmbH auch Zugriff auf von AG gespeicherte oder von AG sonst wie nemecs GmbH zur Verfügung gestellte personenbezogene Daten haben, so dass es sich bei der Leistung von nemecs GmbH um Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO handeln kann. Zum Schutz der personenbezogenen Daten treffen die Vertragspartner die nachfolgenden Vereinbarungen zum Datenschutz.

### **§ 1 Datenschutz, Auftragsdatenverarbeitung**

- 1.1 nemecs GmbH beachtet das jeweils geltende Datenschutzrecht und trifft alle notwendigen organisatorischen Maßnahmen, um die Einhaltung des Datenschutzrechts zu gewährleisten.
- 1.2 nemecs GmbH wird nur solche Mitarbeiter einsetzen, die nemecs GmbH vorab auf das Datengeheimnis sowie, falls einschlägig, auf das Fernmeldegeheimnis gem. § 88 TKG und/oder das Sozialgeheimnis gem. § 35 SGB I verpflichtet hat. nemecs GmbH hat die Mitarbeiter über einschlägige Strafbestimmungen, insbesondere § 203 StGB, belehrt.

### **§ 2 Definitionen und Festlegungen**

- 2.1 Gegenstand und Dauer des Auftrags ergeben sich aus dem in der Präambel genannten Vertrag. Für den Fall, dass der Auftraggeber zur Betreuung seiner Praxissoftware regionale Servicepartner von nemecs GmbH oder andere Fremdunternehmen mit der Arbeit an seinen Daten beauftragt, schließt der Auftraggeber einen eigenen Vertrag mit diesen Unternehmen ab. Die vorliegende Vereinbarung bezieht sich ausschließlich auf Leistungen von nemecs GmbH.
- 2.2 Soweit nemecs GmbH Zugriff auf personenbezogene Daten hat, die AG speichert oder AG sonst wie nemecs GmbH zur Verfügung stellt und die nemecs GmbH zur Erbringung der von nemecs GmbH geschuldeten Leistungen verarbeitet oder nutzt (diese Daten werden im Folgenden die „Nutzerdaten“ genannt), erfolgt dies im Auftrag und auf Weisung von AG gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).
- 2.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 2.4 Die Nutzerdaten sind in Anlage 1 genannt.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 2 von 12



### § 3 Weisungsgebundenheit; Erhebung, Nutzung und Verarbeitung der Daten durch nemecs GmbH

- 3.1 nemecs GmbH wird die Nutzerdaten nur im Rahmen der dokumentierten Weisungen von AG erheben, verarbeiten oder nutzen. AG wird mündliche Weisungen unverzüglich schriftlich bestätigen, E-Mail genügt. Nemecs GmbH wird die Nutzerdaten nur in dem Maße nutzen und verarbeiten, wie es für die Erfüllung der von nemecs GmbH nachdem in der Präambel genannten Vertrag geschuldeten Leistungen erforderlich ist.
- 3.2 nemecs GmbH wird alle technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die für nemecs GmbH anwendbaren Vorschriften der DSGVO zu erfüllen, insb. die in Art. 32 DSGVO genannten Anforderungen.

Die konkreten Maßnahmen ergeben sich aus dem Dokument „Technische und Organisatorische Maßnahmen“, das dieser Vereinbarung als Anlage 2 beigefügt ist.

### § 4 Pflichten von nemecs GmbH, Rechte von AG

- 4.1 nemecs GmbH wird AG auf schriftliches Verlangen von AG bei der Wahrung der Rechte der Betroffenen, insb. im Hinblick auf die Benachrichtigung, Auskunftserteilung sowie die Berichtigung, Sperrung oder Löschung der Nutzerdaten im Rahmen der Möglichkeiten von nemecs GmbH unterstützen, insbesondere wird nemecs GmbH
- angesichts der Art der Verarbeitung AG nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht von AG zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen, wenn AG nemecs GmbH diese Anträge übermittelt und unter Zitat des entsprechenden Gesetzestexts nachweist, dass diese Anträge berechtigt sind;
  - AG unter Berücksichtigung der Art der Verarbeitung und von nemecs GmbH zur Verfügung stehenden Informationen unterstützen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten von AG (Sicherheit der Verarbeitung; ggf. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde; ggf. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgenabschätzung mit ggf. vorheriger Konsultation der Datenschutzbehörde), soweit AG gegenüber nemecs GmbH nachweist, dass AG im konkreten Einzelfall, für den AG Unterstützung verlangt, derartige Pflichten hat.
- 4.2 nemecs GmbH wird alle Nutzerdaten vertraulich behandeln und sicher verwahren. nemecs GmbH darf die Nutzerdaten nicht an Dritte weitergeben, außer AG hat zuvor ausdrücklich zugestimmt. nemecs GmbH gewährleistet, dass nemecs GmbH die Pflichten aus Art. 28 DSGVO erfüllt. Insbesondere gewährleistet nemecs GmbH, dass der Datenschutzbeauftragte von nemecs GmbH, und die für nemecs GmbH im Bereich Datenschutzrecht zuständigen Aufsichtsbehörden ihre gesetzlichen Aufsichts- und Kontrollrechte wahrnehmen können.
- 4.3 nemecs GmbH ist berechtigt, für die Datenverarbeitung gemäß dieser Zusatzvereinbarung Unterauftragnehmer einzusetzen. nemecs GmbH wird AG immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch AG die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (siehe Anlage 3).

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 3 von 12



**Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc**

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

Soweit nemecs GmbH von diesem Recht Gebrauch macht, hat nemecs GmbH sicherzustellen, dass alle in dieser Vereinbarung und in Art. 28 DSGVO genannten Pflichten von nemecs GmbH auch von den betreffenden Unterauftragnehmern eingehalten werden, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

- 4.4 AG hat das Recht, im Benehmen mit nemecs GmbH Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig, jedoch mindestens drei (3) Wochen vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Für die Ermöglichung von Kontrollen durch AG kann nemecs GmbH einen Vergütungsanspruch geltend machen.
- 4.5 nemecs GmbH teilt AG auf Wunsch die Kontaktdaten des Datenschutzbeauftragten von nemecs GmbH mit.
- 4.6 nemecs GmbH wird AG auf Anforderung von AG alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten von nemecs GmbH zur Verfügung stellen, wenn AG konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht von nemecs GmbH gem. Art 28 DSGVO AG Informationen benötigt.
- 4.7 Wenn nemecs GmbH erfährt, dass im Verantwortungsbereich von nemecs GmbH gegen geltendes Datenschutzrecht oder gegen Regelungen aus dieser Zusatzvereinbarung verstoßen worden ist, wird nemecs GmbH AG unverzüglich darauf hinweisen.
- 4.8 AG darf nemecs GmbH Weisungen nur im Rahmen der vertraglichen Pflichten von nemecs GmbH erteilen.

**§ 5 Hinweispflicht, Pflichten bei Vertragsbeendigung**

- 5.1 nemecs GmbH wird AG unverzüglich darauf hinweisen, wenn nemecs GmbH der Ansicht ist, dass eine Weisung von AG gegen geltendes Datenschutzrecht verstößt.
- 5.2 Spätestens einen (1) Monat nach Beendigung des Vertrags wird nemecs GmbH von AG übergebene Datenträger, die Nutzerdaten enthalten, an AG zurückgeben und die bei nemecs GmbH gespeicherten Nutzerdaten nach Wahl von AG entweder löschen oder zurückgeben. Dies gilt nicht, soweit nemecs GmbH aufgrund Unionsrecht oder dem Recht der Mitgliedstaaten der EU zur Speicherung der personenbezogenen Daten verpflichtet ist. Im Falle einer solchen längeren gesetzlichen Aufbewahrungs- bzw. Speicherungspflicht wird nemecs GmbH die betreffenden Datenträger zurückgeben und die Nutzerdaten löschen, sobald das Gesetz dies zulässt.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 4 von 12



Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

## § 6 Schlussbestimmungen

- 6.1 Diese Zusatzvereinbarung bedarf der Schriftform, die elektronische Form ist ausgeschlossen. Änderungen bedürfen der Schriftform, die elektronische Form wahrt die Schriftform.
- 6.2 Sollten Bestimmungen dieser Zusatzvereinbarung rechtsunwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die rechtsunwirksamen Bestimmungen sind von den Vertragspartnern unverzüglich durch solche Bestimmungen zu ersetzen, die dem wirtschaftlich gewollten Zweck der Vertragspartner entsprechen. Das gilt entsprechend für Lücken im jeweiligen Vertrag.
- 6.3 Es gilt deutsches Recht. Gerichtsstand ist der Sitz der nemecs GmbH.

---

Ort, Datum

---

Unterschrift Auftraggeber

---

Stempel Auftraggeber

---

Vor- und Nachname in Druckbuchstaben

---


Ort, Datum

---

Unterschrift Auftragnehmer

Geschäftsführung nemecs GmbH

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 5 von 12

	<p align="center"><b>Datenschutzvereinbarung_zur_ Auftragsdatenverarbeitung.doc</b></p>	<p align="center"><b>nemecs GmbH</b> Netzwerke u. medizinische Computersysteme Tuchmacherstr.12a 84524 Neuötting</p>
---	---	--

**Anlage 1 Nutzerdaten**

**nemecs GmbH erhält Zugriff auf die nachfolgend genannten Nutzerdaten:**

- Kategorie betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
- Auftraggeber
- Patienten des Auftraggebers
- Mitarbeiter des Auftraggebers
- Dienstleister des Auftraggebers

**Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 3, 4, 13, 14 und 15 DSGVO) :**

- allgemeine Personendaten (Name, Geburtsdaten, Anschrift, Telefonnummer, Familienstand,
- Staatsangehörigkeit, E-Mail-Adresse, Krankenkassen; Beruf, Arbeitgeberdaten)
- Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonst. Versicherungsnr., Arztnummer)
- Bankdaten
- Administrative Daten (Betriebsstättenbezogene Daten)
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur)
- Medizinische Dokumentationsdaten
- Onlinedaten (IP-Adresse,)
- Software Lizenzdaten, Versionsdaten
- Hard- und Softwareinformationen

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 6 von 12



Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

## Anlage 2 Technische und organisatorische Maßnahmen

### Generelle Beschreibung

Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien.

Datenverarbeitung ist in Arbeits- und Prozessbeschreibungen schriftlich geregelt.

Fremdfirmen haben keinen Zugriff auf Datenverarbeitung.

Vertretungsregelung für IT-Verantwortlichen bei Urlaub oder Krankheit.

Keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO.

Schriftliche Bestellung eines Datenschutzbeauftragten.

Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis sowie ggf. § 88 TKG und ggf. § 35 SGB I, Belehrung über den § 203 StGB.

Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen.

Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art. 30 Abs. 5 DSGVO besteht.

Namentliche Nennung der Ansprechpartner (IT/DV-Verantwortlicher und externer Datenschutzbeauftragter) zur Klärung fachlicher, technischer und organisatorischer Fragen.

Pseudonymisierung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

In den folgenden Abschnitten sind einige technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO konkret beschrieben:


### 1. Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

### Maßnahmen von nemecs GmbH im Einzelnen:

Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster mit einbruchhemmenden Jalousien ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Schlüsseln zu betreten. Zusätzlich werden außerhalb der Bürozeiten einbruch- und feuerhemmende Sicherheitstüren verschlossen. Ausgabe und Rückgabe von Schlüsseln ist geregelt, mit Schlüsselkarte bzw. durch Systemdokumentation. Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern von nemecs GmbH im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten. nemecs GmbH verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 7 von 12

	<p align="center"><b>Datenschutzvereinbarung_zur_ Auftragsdatenverarbeitung.doc</b></p>	<p align="center"><b>nemecs GmbH</b> Netzwerke u. medizinische Computersysteme Tuchmacherstr.12a 84524 Neuötting</p>
---	---	--

Der Zutritt zu den Servern ist durch einen abschließbaren Severschrank abgesichert .  
Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren)  
beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind,  
erhalten keinen Zutritt zu den Serverräumen.

**2. Datenträgerkontrolle**

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von  
Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.

**Maßnahmen von nemecs GmbH im Einzelnen:**

Externer Zugriff von nemecs GmbH -Mitarbeitern auf nemecs GmbH -Server ist nur via VPN und Au-  
thentifizierung am nemecs GmbH -LAN möglich.nemecs GmbH -WLAN wird mit WPA2 betrieben.  
Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.Akten unter Verschluss. Zugang nur für be-  
rechtigte Personen.Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine  
Firewall verhindert ungewollte Zugriffe von außen.  
Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten  
wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst  
nur innerhalb der zentralen Server von nemecs GmbH).  
Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die  
nemecs GmbH zurück.

**3. Speicherkontrolle**

Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezoge-  
nen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten per-  
sonenbezogenen Daten verhindert wird.

**Maßnahmen von nemecs GmbH im Einzelnen:**

Zugriffe auf die Server von nemecs GmbH erfolgen durch Authentifizierung (Benutzername/Passwort)  
mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechti-  
gung in der Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art:  
28 DSGVO (Auftragsdatenverarbeitung) geregelt.  
Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenban-  
ken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.  
Bei Zugriff auf Daten beim Auftraggeber ist durch die von nemecs GmbH eingesetzten Fernwartungs-  
software sichergestellt, dass berechtigte Mitarbeiter von nemecs GmbH ausschließlich auf die ihrer  
Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendo-  
kumentation protokolliert werden.

Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.  
Die Datenfernübertragungssysteme von nemecs GmbH sind mit Datenverschlüsselung versehen und  
werden auf dem jeweils aktuellen technischen Stand gehalten.  
Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftragge-  
berbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 8 von 12





**Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc**

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

Wenn nemecs GmbH die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN 32757-1 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.

s.im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

#### **4. Benutzerkontrolle**

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

#### **Maßnahmen von nemecs GmbH im Einzelnen:**

s. Datenträgerkontrolle und Zugriffskontrolle.

#### **5. Zugriffskontrolle**

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

#### **Maßnahmen von nemecs GmbH im Einzelnen:**

Vorhandensein eines Berechtigungskonzepts.

Datenträgerverwaltung, Datensicherung, Verschlüsselung

Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.

Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

Verbot der Nutzung privater Datenträger.

Zugriff auf Notebooks, PC und Server von nemecs GmbH nur mit Username und Passwort möglich.

Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.

Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung im geschlossenen Raum. Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.

Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten,

Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung geregelt.

#### **6. Übertragungskontrolle**

Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

#### **Maßnahmen von nemecs GmbH im Einzelnen:**


Regelungen zur Datenübertragung sind vorhanden.

Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert.

Die nemecs GmbH bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.

Die Speicherung von Daten aus dem Auftraggeberbereich erfolgt nur während der Arbeiten zur Mängelbeseitigung oder zur Unterstützung des Einsatzes der von nemecs GmbH gelieferten Systeme bzw. von Systemen, für die nemecs GmbH Serviceleistungen erbringt. Daten aus dem Bereich des

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 9 von 12

	<p align="center"><b>Datenschutzvereinbarung_zur_ Auftragsdatenverarbeitung.doc</b></p>	<p align="center"><b>nemecs GmbH</b> Netzwerke u. medizinische Computersysteme Tuchmacherstr.12a 84524 Neuötting</p>
---	---	--

Auftraggebers werden an einen Dritten nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht. Der Auftraggeber kann nemecs GmbH die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server von nemecs GmbH übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

**7. Eingabekontrolle**

Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.

**Maßnahmen von nemecs GmbH im Einzelnen:**

Regelungen zur Dateneingabe sind vorhanden. Erstellung und Änderung von Daten wird protokolliert. Es ist nicht vorgesehen, dass nemecs GmbH personenbezogene Daten aus dem Bereich des Auftraggebers in die Software eingibt. Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an nemecs GmbH übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt, es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat. Keine Möglichkeit für Mitarbeiter von nemecs GmbH Daten in den operativen Systemen vom Auftraggeber einzugeben, zu ändern oder zu entfernen.

**8. Transportkontrolle**

Die Transportkontrolle umfasst 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.

**Maßnahmen von nemecs GmbH im Einzelnen:**

Firewall. Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung. Statistiken mit personenbezogenen Inhalten werden nur im Auftrag von Auftraggeber und nur an berechnigte Personen bei Auftraggeber übermittelt.

**9. Wiederherstellbarkeit**

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störfungsfall wiederhergestellt werden können.

**Maßnahmen von nemecs GmbH im Einzelnen:**

Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.  
Datenträgerverwaltung, Datensicherung, Aufbewahrung in einem feuerfestem Tresor.  
Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.  
Dokumentation von Datenträgerwechslern und Aufbewahrungsorten.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 10 von 12



## 10. Zuverlässigkeit

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

### Maßnahmen von nemecs GmbH im Einzelnen:

s. Verfügbarkeitskontrolle.

## 11. Datenintegrität

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

### Maßnahmen von nemecs GmbH im Einzelnen:

s. Verfügbarkeitskontrolle.

## 12. Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

### Maßnahmen von nemecs GmbH im Einzelnen:

Alle nemecs GmbH -Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten. Alle vom Auftraggeber bereit gestellten Daten verbleiben ausschließlich in der Verfügungsmacht von nemecs GmbH. Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung vom Auftraggeber. Dienstleister von nemecs GmbH unterliegen Überprüfungen. Die nemecs GmbH führt Arbeiten, bei denen sie Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an die nemecs GmbH einen Fehler oder ein Problem meldet. Die Mitarbeiter von nemecs GmbH sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen. Alle Mitarbeiter von nemecs GmbH, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

## 13. Verfügbarkeitskontrolle

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

### Maßnahmen von nemecs GmbH im Einzelnen:

- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen verifiziert.
- Rauchverbot im Serverraum. Serverraum mit unterbrechungsfreier Stromversorgung,
- Überspannungsschutz. Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 11 von 12



**Datenschutzvereinbarung\_zur\_  
Auftragsdatenverarbeitung.doc**

**nemecs GmbH**  
Netzwerke u. medizinische  
Computersysteme  
Tuchmacherstr.12a  
84524 Neuötting

- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Gespiegelte Server-Festplatten.
- Virenschutzprogramme auf allen Computersystemen.
- Nemecs GmbH setzt eine Firewall und aktuelle Virens Scanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virens Scanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf schadhafte Software überprüft.
- E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind angehalten, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System von nemecs GmbH zu überspielen.

#### **14. Trennbarkeit**

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

#### **Maßnahmen von nemecs GmbH im Einzelnen:**

Es ist nicht vorgesehen, dass nemecs GmbH personenbezogene Daten aus dem Bereich des Auftraggebers verarbeitet.

Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

#### **Anlage 3 Unterauftragnehmer**

Es werden keine Unterauftragnehmer tätig.

Erstellt von: GF,JS Geändert von: JS	Freigegeben von:GF	Version: 2 / vom: 15.05.2018
Erstellt am: 2018 Geändert am: 15.05.2018	Freigegeben am: 15.05.2018	Seite 12 von 12