Der Rabendoktor
Dr. med.
Steffen Rabe
Kinder- und Jugendarzt

## 1. Vertraulichkeit

### 1.1 Zutrittskontrolle

Die durch die Kinderarztpraxis angemieteten Praxisräume befinden sich in einem Mehrparteienhaus in München/Pasing.

Die Zugänge zum Haus und auch zu den Praxisräumen der Kinderarztpraxis sind Tag und Nacht mit Sicherheitsschlössern verschlossen. Zugang zum Gebäude und den einzelnen Wohnungen/Gewerbe-/Praxisflächen haben nur der Vermieter und die Mieter der entsprechenden Flächen; Besucher/Kunden/Patienten erhalten erst auf Anforderung durch die Klingelanlage Zutritt.

Für das Gebäude und die Praxisräume wurde eine definierte Anzahl von Schlüsseln durch den Vermieter ausgegeben, deren Anzahl beim Vermieter und deren Ausgabe an Mitarbeiterinnen für die Praxisräume durch Herrn Dr. Rabe schriftlich dokumentiert ist. Jeder Empfänger muss den Erhalt eines Schlüssels durch Unterschrift bestätigen und haftet für diesen Schlüssel. Bedingung für den Erhalt eines Schlüssels ist ein vertraglich fixiertes Beschäftigungsverhältnis und eine Verschwiegenheitsverpflichtung, die durch Unterschrift bestätigt wurde. Dies gilt auch für das Reinigungspersonal. Eine (auch nur vorübergehende) Weitergabe des Schlüssels an Dritte ist in der unterschriebenen Verschwiegenheitsverpflichtung ausdrücklich untersagt.

Patienten erhalten erst nach Klingeln und nachfolgender Türöffnung Zutritt zu dem Gebäude und dann den Praxisräumen. Die Eingangstür ist vom Empfang aus einsehbar.

Patienten dürfen sich nicht ohne Begleitung in den Praxisräumen frei bewegen.

Für den Zutritt in die und die Nutzung der Räume durch Ärztinnen, Mitarbeiterinnen und Patientinnen der Praxis für Achtsame Frauenheilkunde gelten nach Zusicherung der verantwortlichen ärztlichen Kolleginnen analoge Regelungen.

### 1.2 Zugangskontrolle

Die elektronische Datenerfassung und -verarbeitung erfolgt in der Kinderarztpraxis ausschließlich an zwei voneinander getrennten Computersystemen – einem am Empfang und einem zweiten im Behandlungsraum Dr. Rabes. Beide Systeme arbeiten als Standalone-Systeme und sind nicht miteinander vernetzt. Um Zugang zu diesen Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen – diese wird unmittelbar mit der Datenerfassung und -verarbeitung befassten Angestellten und nur diesen von Herrn Dr. Rabe in Form eines Benutzernamens und eines Passworts erteilt.

Passwörter haben eine Mindestlänge von 8 Zeichen und bestehen aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Passwörter werden grundsätzlich verschlüsselt gespeichert. Entsprechend den aktuellen Empfehlungen einschlägiger Fachveröffentlichungen werden diese Passwörter nicht regelmäßig geändert, sondern nur, wenn Hinweise darauf bestehen, dass sie kompromittiert wurden.

Es ist den Mitarbeitern der Kinderarztpraxis ausdrücklich untersagt, die Zugangsdaten zu den Computersystemen mit Dritten zu teilen – dies wird in der ausgefüllten Verschwiegenheitserklärung per Unterschrift bestätigt.



Alle Mitarbeiter sind angewiesen, den Zugang zu ihrem Computer zu sperren, wenn sie diesen verlassen. Darüber hinaus ist ein automatischer Bildschirmschutz eingerichtet, der bei fehlender Eingabe aktiviert wird und sich nur mit dem entsprechenden Passwort des Accounts entsperren lässt.

Fehlerhafte Anmeldeversuche werden protokolliert, bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Alle verwendeten Computer sind durch eine Firewall geschützt, eine Virenschutzsoftware ist installiert, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Der an der Anmeldung verwendete Computer wird ausschließlich für die Online-Terminvergabe über die Server der Firma Samedi genutzt – diese erfolgt ausnahmslos über verschlüsselte Verbindungen. Eine darüber hinaus gehende Nutzung des Internets ist an diesem Computer nicht möglich, dies wird durch entsprechende technische Maßnahmen, die den Nutzerzugang entsprechend einschränken, gewährleistet.

### 1.3 Zugriffskontrolle

Berechtigungen für die Computersysteme in der Kinderarztpraxis werden ausschließlich von Herrn Dr. Rabe selber als einzigem Administrator eingerichtet und betreut.

Auf den in Herrn Dr. Rabes Behandlungszimmer befindlichen Computer hat er allein Zugriff.

Berechtigungen zur Datenverarbeitung werden grundsätzlich nach dem Need-to-know-Prinzip vergeben – somit erhalten die Mitarbeiterinnen der Anmeldung keinen Zugriff auf die in der Praxis verwendete Abrechnungssoftware; diese ist ausschließlich auf dem im Behandlungszimmer Herrn Dr. Rabes befindlichen Computer installiert.

Ebenso wenig kann der Computer an der Praxisanmeldung auf elektronisch übertragene Labordaten zugreifen – auch dies ist nur vom Computer Dr. Rabes möglich.

Innerhalb der jeweiligen Computer-Benutzerkonten ist der Zugang zu Programmen, die personenbezogene Patientendaten verarbeiten (Terminbuchungsprogramm, Abrechnungsprogramm, Datenübertragungsprogramm für Labordaten) jeweils nochmals durch entsprechende Passwörter (s.o.) geschützt.

Die Vernichtung von datenschutzrelevanten Unterlagen oder Datenträgern erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 32757 bzw. 66399 gewährleistet. Innerhalb der Praxis werden kleinere Mengen entsprechender Unterlagen ausschließlich mit einem Schredder vernichtet, der den diesbezüglichen gesetzlichen Anforderungen genügt („*cross cut*“, Sicherheitsstufe ≥ 3).

Alle Computersysteme werden entweder automatisiert, und/oder durch Herrn Dr. Rabe als einzigen Administrator regelmäßig mit entsprechenden Sicherheitsupdates aktualisiert.

Mitarbeiterinnen der Kinderarztpraxis haben keine Möglichkeit, Software auf dem Computer im Anmeldebereich zu installieren oder externe Datenträger zu verbinden – dies kann nur Herr Dr. Rabe selber.

Der Zugriff auf elektronische, personenbezogene Daten mit anderen als den erwähnten Geräten ist nicht möglich.

Der Rabendoktor
Dr. med.
Steffen Rabe
Kinder- und Jugendarzt

Die Erhebung personenbezogener Patientendaten in der Praxis selbst erfolgt ausschließlich schriftlich, nicht im Gespräch an der Anmeldung.

Der Anmeldebereich ist so gestaltet, dass der Bildschirm des verwendeten Computers oder an der Anmeldung bearbeitete Unterlagen für Patienten nicht einsehbar sind.

Der Wartebereich für Patienten ist räumlich und durch eine Schiebetür vom Anmeldebereich getrennt, so dass Telefonate von Unbefugten nicht mitgehört werden können. Die Mitarbeiterinnen sind angewiesen, darauf zu achten, dass diese Schiebetür in der Regel geschlossen ist.

Die Behandlung der Patienten erfolgt ausnahmslos in von den Wartebereichen getrennten, durch Türen verschlossenen Räumen, so dass Gesprächsinhalte von Unbefugten nicht mitgehört werden können.

Die Aufbewahrung und Archivierung personenbezogener Patientendaten erfolgt ausnahmslos in Bereichen, die Patienten entweder nicht zugänglich sind oder in denen sie sich zu keinem Zeitpunkt ohne Aufsicht durch Praxispersonal oder Herrn Dr. Rabe selbst aufhalten.

### 1.4 Trennung

Patientendaten werden elektronisch ausschließlich mit Datenbanksystemen verwaltet (Programm Medys der Firma Medys für die Abrechnung, Programm Samedi der Firma Samedi für die Terminbuchung, Programm Amelis der Firma Amedes für Labordaten), die eine Trennung der Daten verschiedener Patienten gewährleisten.

Außerhalb dieser Programme findet keine elektronische Verarbeitung von Patientendaten statt.

### 1.5 Pseudonymisierung und Verschlüsselung

Administrative oder Remote-Zugriffe auf Computersysteme der Kinderarztpraxis erfolgen grundsätzlich über verschlüsselte Verbindungen.

Auch die elektronische Übertragung von Labordaten der Firma Amedes erfolgt über eine verschlüsselte Verbindung.

Auf dem Computer im Anmeldebereich werden grundsätzlich keine Patientendaten gespeichert (die Terminverwaltung erfolgt über die Server der Firma Samedi, auf die ausschließlich über verschlüsselte Verbindungen zugegriffen wird).

Auf dem Computer im Behandlungszimmer Herrn Dr. Rabes werden die Daten auf verschlüsselten Datenträgern gespeichert.

Die Patienten werden konsequent (persönlich an der Anmeldung, in Merkblättern, auf der Internetseite) darauf hingewiesen, keine personenbezogenen medizinischen Daten in unverschlüsselten Emails zu übertragen.

Dr. Rabe bietet eine S/MIME-verschlüsselte Email-Kommunikation für Patienten an, eine Anleitung hierzu ist auf der Internetseite veröffentlicht.

Darüber hinaus haben Patienten die Möglichkeit, Unterlagen über eine SSL-verschlüsselte Verbindung auf den Server der Praxis-Website hochzuladen.

Der Rabendoktor
Dr. med.
Steffen Rabe
Kinder- und Jugendarzt

## 2. Integrität

### 2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten in der Kinderarztpraxis wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, ausschließlich mit ihren eigenen Accounts zu arbeiten. Zugangsdaten zu Benutzerkonten dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

Löschungen personenbezogener Daten werden ausschließlich von Herrn Dr. Rabe selber vorgenommen (z.B. nach Ablauf der gesetzlichen Aufbewahrungsfrist oder auf Wunsch von Patienten, soweit dies gesetzlich zulässig ist).

### 2.2 Weitergabekontrolle

Eine Weitergabe personenbezogener Daten erfolgt nur in dem Umfang, wie dies im Rahmen der gesetzlichen Regelungen zulässig, im Rahmen des Behandlungsvertrages erforderlich und/oder mit dem Patienten ausdrücklich abgestimmt ist.

Soweit möglich werden elektronische Daten an Empfänger verschlüsselt übertragen oder es erfolgt die Datenweitergabe per Fax.

Ein verschlüsselter elektronischer Austausch personenbezogener Daten findet statt mit

- der Firma Samedi zur online-Terminbuchung
- der Firma Amedes zur Übertragung der Ergebnisse von Laboruntersuchungen
- der Firma Arco zur Übertragung der Abrechnungsdaten.

Der Datenaustausch mit den Firmen Amedes und Arco findet ausschließlich über den Computer Herrn Dr. Rabes, der mit der Firma Samedi von beiden Praxis-Computern aus statt.

Patienten oder andere Betroffene (z.B. Mitbehandler) werden konsequent und ausdrücklich telefonisch an der Anmeldung, aber auch auf der Internetseite der Praxis darauf hingewiesen, keine personenbezogenen Daten in unverschlüsselter Form elektronisch zu übertragen (z.B. per Email). Herr Dr. Rabe bietet mit der S/MIME-Verschlüsselung der praxiseigenen Email-Accounts die Möglichkeit, verschlüsselt per Email zu kommunizieren. Die notwendigen Schlüssel werden Patienten und Anderen auf Wunsch in einer ersten, inhaltsfreien Email zur Verfügung gestellt. Eine Anleitung dazu ist auf der Internetseite veröffentlicht.

Die Nutzung privater Datenträger ist den Mitarbeitern der Kinderarztpraxis untersagt.

Die Mitarbeiterinnen der Kinderarztpraxis werden zu Datenschutzthemen geschult und zu einem vertraulichen Umgang mit personenbezogenen Daten schriftlich verpflichtet.

Auskunftsanfragen von Patienten oder berechtigten Stellen zu personenbezogenen Daten werden ausschließlich von Herrn Dr. Rabe selber auf ihre Legitimität hin überprüft und gegebenenfalls beantwortet – diese Anfragen werden von den Mitarbeiterinnen daher unverzüglich an ihn weitergeleitet.

Der Rabendoktor
Dr. med.
Steffen Rabe
Kinder- und Jugendarzt

## 3. Verfügbarkeit und Belastbarkeit

Die Daten auf dem Computer Herrn Dr. Rabes werden mehrmals täglich inkrementell und mindestens wöchentlich „voll" gesichert. Die Sicherungsmedien sind verschlüsselt und an werden an einem physisch getrennten Ort aufbewahrt.

Die Funktionsfähigkeit dieser Backups wird durch Wieder-Einspielen regelmäßig getestet. Die Ergebnisse dieser Tests werden protokolliert.

Die Computer sind an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen, der Computer an der Anmeldung ist darüber hinaus als Laptop vorübergehend auch netzunabhängig zu betreiben.

Bei Ausfall des Anmeldecomputers ist dessen Funktion nahtlos durch den Computer Herrn Dr. Rabes zu übernehmen, bei Ausfall dieses Computers ist durch die Möglichkeit eines Einspielens der entsprechenden Backups auf das tragbare Computersystem Herrn Dr. Rabes (MacBookPro - auf dem normalerweise keine Patientendaten gespeichert sind) eine zeitnahe Wiederverfügbarkeit der Daten gewährleistet.

Der Rabendoktor
Dr. med.
Steffen Rabe
Kinder- und Jugendarzt

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

### 4.1 Datenschutzmanagement

Die hier formulierten TOMs sind die Datenschutzleitlinie und Grundlage des Datenschutzmanagements der Kinderarztpraxis Der Rabendoktor.

Diese Richtlinien werden von Herrn Dr. Rabe regelmäßig auf ihre Wirksamkeit evaluiert und angepasst.

Durch regelmäßige diesbezügliche Unterweisung der Mitarbeiterinnen ist sichergestellt, dass Datenschutzvorfälle als solche erkannt und Herrn Dr. Rabe unverzüglich gemeldet werden.

Sofern die Daten von Patienten betroffen sind werden diese, sofern dies durch die entsprechenden gesetzlichen Regelungen vorgesehen ist, über Art und Umfang des Vorfalls informiert.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO binnen 72 Stunden nach Kenntnis von dem Vorfall eine Meldung an das Bayerische LDA als zuständige Aufsichtsbehörde erfolgen.

### Auftragskontrolle

Die Erfassung, Speicherung und Verarbeitung von Patientendaten erfolgt ausschließlich innerhalb der Europäischen Union.

Bei Einbindung externer Dienstleister wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Vertrag zur Auftragsverarbeitung abgeschlossen. Dessen Einhaltung seitens der Auftragnehmer wird auch während des Vertragsverhältnisses regelmäßig kontrolliert.

### Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

In der Kinderarztpraxis wird schon bei der Auswahl der eingesetzten Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit im Zusammenhang mit der Erfassung, der Speicherung und Verarbeitung der Patientendaten Rechnung getragen wird („Datenminimierung“). So werden z.B. bei der elektronischen Terminvergabe nur die für diese notwendigen Kontaktdaten abgefragt, alle weiteren Daten werden erst im Zusammenhang mit dem Abschluss des Behandlungsvertrages erhoben.

Der Grundsatz, für jeden Arbeitsschritt nur die für diesen unbedingt notwendigen Daten zu erheben und zu speichern, ist ausdrücklicher Grundsatz in der Kinderarztpraxis.