kvt
Kassenärztliche
Vereinigung Thüringen

Datenschutz

2. Auflage

Handbuch für die Mitglieder der KVT

INHALTSVERZEICHNIS

I Datenschutz in der vertragsärztlichen Praxis

1 Vorwort

Mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 hat die Einhaltung des Datenschutzes sowie der Datensicherheit einen neuen gesetzlichen Rahmen und gesellschaftlichen Stellenwert erfahren. Trotz bereits bestehender gesetzlicher Vorgaben, haben sich auch für die Arztpraxen einige Neuerungen ergeben. Für den niedergelassen Arzt bilden primär die Regelungen aus der DS-GVO sowie die des Bundesdatenschutzgesetzes (BDSG) den rechtlichen Rahmen. Zusätzlich sind spezielle datenschutzrechtliche Vorgaben aus bereichsspezifischen Gesetzen zu beachten, welche die allgemeinen Bestimmungen ergänzen oder auch konkretisieren.

Im Hinblick auf die immer weiter voranschreitende Digitalisierung des Gesundheitswesen werden eine Vielzahl von Patientendaten automatisiert verarbeitet. Mit dem verpflichtenden Anschluss an die Telematikinfrastruktur ergeben sich zudem neue Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeiten sowie neue Möglichkeiten der Datenverarbeitung.

Mit diesem Praxis-Handbuch wollen wir Ihnen einen kompakten Überblick über die wesentlichen Anforderungen zur Einhaltung des Datenschutzes und der Datensicherheit in einer Arztpraxis an die Hand geben. Zu Beginn sollen die Grundlagen der Datenverarbeitung und hier im speziellen die Voraussetzungen für die Übermittlung von Patientendaten erläutert werden. Dem schließen sich Ausführungen zu den Maßnahmen an, welche in der Arztpraxis insbesondere durch die Regelungen der Datenschutz-Grundverordnung umzusetzen sind. Um Ihnen die Umsetzung zu erleichtern, finden Sie in diesem Handbuch einige Muster zur Implementierung in Ihrem Datenschutzmanagement.

Ass. jur. Christin Kirschmann
Datenschutzbeauftragte

Sven Auerswald
Hauptgeschäftsführer

2 Grundlagen der Datenverarbeitung

2.1 Rechtsgrundlagen für die Verarbeitung der Gesundheitsdaten

2.1.1 Wann ist die Verarbeitung von Gesundheitsdaten erlaubt?

Im Grundsatz geht das Gesetz davon aus, dass die Verarbeitung sensibler Gesundheitsdaten nicht erlaubt ist. Von diesem strikten Verbot der Verarbeitung bestehen jedoch Ausnahmen, nämlich immer dann, wenn eine Einwilligung der betroffenen Person vorliegt oder eine gesetzliche Grundlage dies erlaubt (sog. Verbot mit Erlaubnisvorbehalt).

2.1.2 Auf welche gesetzlichen Grundlagen kann ich die Verarbeitung von Patientendaten stützen?

Die zentralen Vorschriften für die Verarbeitung von Gesundheitsdaten in der Arztpraxis bilden Art. 9 DS-GVO sowie § 22 BDSG.

Ärzte dürfen hiernach insbesondere Gesundheitsdaten bei der Gesundheitsvorsorge, der ärztlichen Behandlung, zur Erfüllung spezieller Pflichten aus dem Sozialrecht sowie im öffentlichen Gesundheitsinteresse, zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten, aus Gründen eines erheblichen öffentlichen Interesses oder zur Wahrung von Rechtsansprüchen verarbeiten.

Daneben finden sich zahlreiche bereichsspezifische Vorschriften, wonach die Verarbeitung von Gesundheitsdaten zulässig ist.

2.1.3 Welche Anforderung sind bei der Verarbeitung von Gesundheitsdaten zu erfüllen?

Die Arztpraxis muss angemessene und spezifische Maßnahmen zur Wahrung der Rechte der Patienten im Zusammenhang mit der Verarbeitung ihrer Daten umsetzen. Hierzu können insbesondere die folgenden Maßnahmen ergriffen werden:

- die Umsetzung technischer und organisatorischer Maßnahmen für die Datensicherheit
- Sensibilisierung der Mitarbeiter

- Pseudonymisierung sowie Verschlüsselung personenbezogener Daten
- Benennung eines Datenschutzbeauftragten
- Beschränkung der Zugriffsrechte auf Patientendaten
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten

2.2 Einwilligung in die Verarbeitung von Gesundheitsdaten

2.2.1 Wann wird eine Einwilligungserklärung des Patienten für die Verarbeitung seiner personenbezogenen Daten benötigt?

Im Rahmen der ärztlichen Behandlung kann die Datenverarbeitung der Gesundheitsdaten in der Regel auf eine gesetzliche Grundlage gestützt werden. In bestimmen Ausnahmefällen liegt jedoch keine gesetzliche Befugnis oder Pflicht vor, sodass die Rechtmäßigkeit der Verarbeitung von einer Einwilligung des Patienten abhängig ist. In bestimmten Fällen schreibt das Gesetz ausdrücklich die Einholung einer Einwilligung vor.

2.2.2 Wann ist eine Einwilligung des Patienten zur Datenübermittlung insbesondere erforderlich?

- freiwillige Anwendungen der elektronischen Gesundheitskarte
- Übermittlung an privatärztliche Verrechnungsstellen oder private Versicherungsgesellschaften
- Übermittlung an den Arbeitgeber oder Agentur für Arbeit
- bei einer Praxisveräußerung
- im Rahmen der besonderen bzw. integrierten Versorgung
- für strukturierte Behandlungsprogramme
- Online Terminbuchungs- oder Terminerinnerungsservice

2.2.3 Wann wird keine Einwilligungserklärung des Patienten für die Übermittlung seiner personenbezogenen Daten benötigt?

- Übermittlungen an den Betreuer, sofern er für die Gesundheitsfürsorge zuständig ist
- bei Bestehen gesetzlicher Mitteilungspflichten, z. B. gegenüber:
  - Unfallversicherungsträger
  - Krankenkassen
  - Gesundheitsämter auf der Grundlage des Infektionsschutzgesetzes
  - Jugendämter bei Kindeswohlgefährdung
  - Kassenärztliche Vereinigung
  - Medizinischer Dienst
- Übermittlung an das Labor

2.2.4 Ist das vorherige Einholen einer an sich erforderlichen Einwilligungserklärung notwendig, wenn der Patient beispielsweise bewusstlos ist?

Kann der Patient seine Einwilligung nicht mehr erklären, beispielsweise weil er bewusstlos ist oder an einer schweren Erkrankung leidet, und bedarf es zu seiner weiteren Behandlung und zur Aufrechterhaltung seines Lebens der Weitergabe seiner personenbezogenen Daten - z. B. an einen anderen weiterbehandelnden Arzt - ist in der Regel eine sogenannte mutmaßliche Einwilligung gegeben. In diesen Fällen kann davon ausgegangen werden, dass der Patient im Fall seiner Befragung mit der Offenbarung seiner Daten einverstanden wäre.

2.2.5 Was ist bei der Einwilligungserklärung besonders zu beachten?

Die Einwilligung des Patienten muss in jedem Falle freiwillig erfolgen.

Hinsichtlich der Form der Einwilligungserklärung bestehen grundsätzlich keine gesetzlichen Vorgaben, sodass diese mündlich, elektronisch oder auch schriftlich erfolgen kann. Aus Beweisgründen sollte die Einwilligungserklärung in schriftlicher Form erfolgen.

Die Einwilligung muss in verständlicher, klarer und einfacher Sprache erfolgen. Der Patient muss den Zweck und den Umfang kennen, zu dem er den Arzt berechtigt, seine personenbezogenen Informationen weiterzugeben (z. B. für die Weiterbehandlung bei einem anderen Arzt).

Die Einwilligungserklärung muss einen Hinweis darauf enthalten, dass der Patient seine Einwilligung jederzeit widerrufen kann.

Beachte: Eine pauschale Einwilligung in alle denkbaren Varianten der Datenverarbeitung, deren Reichweite der Patient nicht erkennen kann, sind unzulässig. Aus der Einwilligung muss sich für den konkreten Einzelfall ergeben, wer in welchem Umfang die personenbezogene Daten verarbeitet und aus welchem Grund (Zweck der Verarbeitung). Die Angaben sollten so präzise wie möglich erfolgen. Im Zusammenhang mit der Übermittlung von Patientendaten muss klar sein, wer der genaue Empfänger sein soll.

2.2.6 Gibt es ein Muster?

Ein Muster haben wir Ihnen unter Punkt II. 1 zur Verfügung gestellt.

3 Der Datenschutzbeauftragte

3.1 Warum muss bzw. sollte ein Datenschutzbeauftragter bestellt werden?

Der Zweck den der Gesetzgeber mit der Benennung eines Datenschutzbeauftragten verfolgt ist der, dass dem Verantwortlichen bei der Überwachung und Umsetzung der internen Vorgaben zur Einhaltung des Datenschutzes, eine weitere Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts verfügt, zur Seite steht.

3.2 Wann muss ein Datenschutzbeauftragter bestellt werden?

3.2.1 Benennung nach Schwellenwert: Zwanzig-Personen-Regel

Ein Datenschutzbeauftragter ist zwingend zu bestellen, wenn mindestens zwanzig Personen regelmäßig Daten automatisiert (z. B. am Computer) verarbeiten. Abzustellen ist dabei auf die in der Praxis tätigen Personen. Es ist unerheblich, ob die Personen in Voll- oder Teilzeit oder als Auszubildende beschäftigt sind. Nicht mitgezählt werden der Praxisinhaber als Verantwortlicher selber oder Externe.

3.2.2 Benennung nach Risikobewertung

In Ausnahmefällen kann eine Bestellpflicht auch unabhängig von der Anzahl der in der Praxis tätigen Personen bestehen. Dies ist beispielsweise der Fall, wenn eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt oder aufgrund eines hohen Risikos bei der Datenverarbeitung eine Datenschutz-Folgenabschätzung (siehe Punkt 5) durchzuführen ist.

Ab wann des Kriterium „umfangreich“ erfüllt ist, muss im konkreten Einzelfall betrachtet werden. In Arztpraxen in denen nicht mehr als zwanzig Personen beschäftigt sind, dürfte die Art, der Umfang, die Umstände oder die Zwecke der Verarbeitung nicht zu einer zusätzlichen Risikoerhöhung führen.

3.3 Wer kann zum Datenschutzbeauftragten bestellt werden?

Mit der Aufgabe des Datenschutzbeauftragten kann sowohl ein fachlich qualifizierter Mitarbeiter, welcher nicht der Praxisinhaber selber sein darf, oder ein externer Datenschützer betraut werden. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde (TLfDI) mitzuteilen. Dies umfasst die Adresse, ggf. Telefonnummer und die E-Mail-Adresse des Datenschutzbeauftragten . Eine Mitteilung des Namens ist nicht erforderlich.

Die Person des Datenschutzbeauftragten muss die nötige Fachkunde und Zuverlässigkeit haben. Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten. Er sollte aus diesen Gründen über die entsprechenden datenschutzrechtlichen und technischen Kenntnisse verfügen. Die notwendigen Fachkenntnisse können über Schulungen erworben werden.

3.4 Welche Aufgaben hat der Datenschutzbeauftragte?

Der Datenschutzbeauftragte hat die Aufgabe, die Einhaltung des Datenschutzes und der Datensicherheit in der Praxis zu überwachen und geeignete Maßnahmen festzulegen. Er unterrichtet und berät das Praxisteam über ihre Pflichten nach dem Datenschutzrecht. Er kann mit der Durchführung von Schulungen und der Sensibilisierung von Mitarbeitern betraut werden. Darüber hinaus ist er Ansprechpartner für die Aufsichtsbehörde sowie von der Datenverarbeitung Betroffene.

4 Das Verzeichnis von Verarbeitungstätigkeiten

4.1 Ist die Arztpraxis zur Erstellung des Verzeichnisses von Verarbeitungstätigkeiten verpflichtet?

Jeder datenschutzrechtlich Verantwortliche einer Arztpraxis, z. B. dessen Inhaber, ist zur Führung eines solchen Verzeichnisses verpflichtet. Es dient vorrangig der Datenschutzorganisation in der Arztpraxis. Das Verzeichnis ist der Aufsichtsbehörde jedoch nur auf Anfrage zu übersenden.

4.2 Was ist unter einer Verarbeitungstätigkeit zu verstehen?

Eine Verarbeitungstätigkeit stellt jeder hinreichend abstrakte Geschäftsprozess dar, dem ein eigener Zweck zugrunde liegt. Mehrere Einzelverarbeitungsschritte, welche zu einem gemeinsamen Zweck erfolgen, können zu einer Verarbeitungstätigkeit zusammengefasst werden.

4.3 Was beinhaltet das Verarbeitungsverzeichnis und wie wird es erstellt?

In dem Verzeichnis von Verarbeitungstätigkeiten werden Tätigkeiten bzw. Vorgänge erfasst, mit denen in der Praxis personenbezogene Daten verarbeitet werden. Das betrifft Daten, die die Praxis selbst erhebt, solche die gespeichert, verändert, verwendet, übermittelt oder vernichtet werden. Hierbei kann es sich beispielsweise um folgende Tätigkeiten handeln:

<u>Patientenbezogene Verarbeitungstätigkeiten, zum Beispiel:</u>

- Anlegen einer elektronischen Patientenakte
- Anlegen einer Patientenakte (Papierform)
- Verarbeitung von Patientendaten zur Abrechnung über die KVT bzw. PVS
- Betrieb der Website mit Möglichkeit der Online-Terminbuchung
- Terminvergabe
- Auslesen von Kontaktdaten aus der Telefonanlage
- Führen eines Impfbuches oder Laborbuches
- Labor
- Erstellen ärztlicher Gutachten
- Videosprechstunde
- Ausstellung von Verordnungen

- Ausstellung von Überweisungen
- Einsatz von Videokameras
- Terminvergabe
- Tele-Rucksack
- Verarbeitung von Patientendaten durch 24-Stunden-Blutdruckmessgerät/ Langzeit-EKG/
- Lungenfunktionstest/Ruhe-EKG/Ultraschallgerät
- Datensicherung (z. B. Back-Up-Verfahren)
- Datenvernichtung

Personalbezogene Verarbeitungstätigkeiten:

- Lohnabrechnung
- Personalverwaltung
- Führen von Personalakten
- Bewerbermanagement

4.4 Welche Angaben sind zu jeder Verarbeitungstätigkeit erforderlich?

- Namen und Kontaktdaten der Arztpraxis und, soweit vorhanden, die Angaben zur Person des Datenschutzbeauftragten
- Zweck der Verarbeitung (z. B. ärztliche Dokumentation)
- betroffene Personengruppen (z. B. Patienten, Mitarbeiter der Praxis, Angehörige)
- Beschreibung der Datenkategorien (z. B. Name und Adressdaten, Gesundheitsdaten, Personaldaten)
- Kategorien von Empfängern gegenüber denen, die personenbezogenen Daten offengelegt worden sind oder noch werden (z. B. Krankenkassen, Kassenärztliche Vereinigungen, Medizinischer Dienst, Finanzamt)
- Fristen für die Löschung der Daten (z. B. 10 Jahre nach Abschluss der Behandlung)
- allgemeine Beschreibung der technisch und organisatorischen Maßnahmen

Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

4.5 Was passiert, wenn eine Praxis kein Verarbeitungsverzeichnis hat?

Das Verarbeitungsverzeichnis ist auf Verlangen der Aufsichtsbehörde, dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), bereitzustellen. Liegt das Verzeichnis nicht vor, drohen Geldstrafen.

4.6 Wo finde ich Muster für das Verzeichnis von Verarbeitungstätigkeit?

Unter II. 2. haben wir für sie ein Muster erstellt. Daneben finden Sie weitere Muster unter https://www.kbv.de/html/dsgvo-in-der-praxis.php.

5. Die Datenschutz-Folgenabschätzung

5.1 Was ist eine Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung ist eine spezielle Methode zur Beurteilung von Risiken bei Datenverarbeitungsvorgängen mit dem Ziel, diese zu vermeiden oder zu reduzieren. Dabei werden die Eintrittswahrscheinlichkeit und die Schwere hoher Risiken unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Ursachen des Risikos bestimmt und bewertet (Verhältnismäßigkeitsprüfung).

5.2 Wann muss eine Datenschutz-Folgenabschätzung erfolgen?

Eine Datenschutz-Folgenabschätzung muss in der Arztpraxis nicht zwingend bei jeder Datenverarbeitung durchgeführt werden. Erforderlich ist sie jedoch, wenn eine Form der Datenverarbeitung, insbesondere bei der Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, deren Gesundheitsdaten verarbeitet werden sollen. Zu betrachten sind deshalb Datenverarbeitungsvorgänge mit hohem Gefährdungspotenzial für die Rechte und Freiheiten für die von der Verarbeitung betroffenen Personen.

Der Gesetzgeber hat Fälle geregelt, in denen ein solch hohes Risiko regelmäßig vermutet wird:

- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z. B. Videoüberwachung in der Arztpraxis)
- umfangreiche Verarbeitung von Gesundheitsdaten
- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, welche als Grundlage für rechtserhebliche Entscheidungen gegenüber dieser Person dienen oder diese in ähnlich erheblicher Weise beeinträchtigen

Beachten Sie:

Auch wenn in Arztpraxen eine Verarbeitung von zahlreichen Gesundheitsdaten stattfindet, handelt es sich nach Auffassung des Normgebers im Falle von Einzelpraxen nicht um eine umfangreiche Verarbeitung von Gesundheitsdaten, so dass hier keine Datenschutz-Folgenabschätzung nötig sein soll.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben eine sog. „Blacklist“ veröffentlicht, in der die Verarbeitungsvorgänge genannt sind, die eine Datenschutz-Folgenabschätzung zwingend erforderlich machen.

Bei der Folgenabschätzung ist der Datenschutzbeauftragte der Praxis zu beteiligen. Zeigt die Folgenabschätzung ein verbleibendes hohes Risiko, muss der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) konsultiert werden.

Im Zweifelsfalle sollte der TLfDI mit einbezogen werden.

5.3 Was muss eine solche Datenschutz-Folgenabschätzung beinhalten?

Um mit Datenschutz-Folgenabschätzungen zu vergleichbaren Ergebnissen zu gelangen und ein einheitliches Datenschutzniveau zu gewährleisten, sind zumindest inhaltliche Mindestanforderungen nötig. Diese wurden in der DS-GVO nachfolgend festgelegt:

- Beschreibung des Verarbeitungsvorganges und Zweckes der Verarbeitung (ggf. vom Arzt/Psychotherapeuten mit der Verarbeitung verfolgte berechtigte Interessen)
- Bewertung der Notwendigkeit/Verhältnismäßigkeit im Hinblick auf den Zweck der Verarbeitung
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (von der Datenverarbeitung Betroffene)
- geplante Abhilfemaßnahmen, durch die der Schutz der personenbezogenen Daten sichergestellt wird (technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten)

6 Auftragsverarbeitung – Zusammenarbeit mit Dienstleistern

6.1 Was ist Auftragsverarbeitung?

Eine Auftragsverarbeitung liegt vor, wenn personenbezogene Daten (z. B. Gesundheitsdaten) im Auftrag des Verantwortlichen (z. B. Arzt) verarbeitet werden.

6.2 Wann müssen Verträge zur Auftragsverarbeitung geschlossen werden?

Ein Vertrag zur Auftragsverarbeitung muss immer dann geschlossen werden, wenn externe Dienstleister Patienten- oder Mitarbeiterdaten verarbeiten und entsprechend auf diese zugreifen können.

Beispiele für Auftragsverarbeitung:

- Wartung der Praxis-EDV
- Vernichtung von Akten und Datenträgern
- Nutzung von Cloud-Systemen
- Terminvergabe durch Externe (nicht Terminservicestellen der KVen)
- externer IT-Dienstleister
- Archivierungsdienstleistungen

Beispiele die keine Auftragsverarbeitung darstellen:

- reine technische Wartungen der IT-Infrastruktur
- Arbeiten an der Stromzufuhr, Kühlung oder Heizung
- Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörige anderer Berufe, die als „Geheimnisträger“ gelten

6.3 Wird im Rahmen der Zusammenarbeit mit dem Labor ein Vertrag zur Auftragsverarbeitung nötig?

Nein. Der Laborarzt verarbeitet die personenbezogenen Daten nicht auf Weisung des überweisenden Arztes, sondern im eigenen Interesse. Dabei hat der Begriff der Auftragsüberweisung nicht die gleiche Bedeutung wie der datenschutzrechtlich geprägte Begriff der Datenverarbeitung im Auftrag. Mit dem Proben- und Anforderungsscheinversand wird zwischen dem Patienten und dem Labor ein eigenständiges Behandlungsverhältnis begründet. Die Verarbeitung der Patientendaten erfolgt im Rahmen des Behandlungsvertrages im Sinne des Art. 9 Abs. 2 Buchstabe h) Datenschutz-Grundverordnung (DS-GVO).

6.4 Welche Inhalte sollte der Vertrag haben?

- Gegenstand und Dauer der Verarbeitung, Bezeichnung der Leistung, die durchgeführt werden soll und die Dauer der Beauftragung
- Art und Zweck der Verarbeitung, wozu dient die Verarbeitung und welches Ziel soll erreicht werden
- Art der personenbezogenen Daten und Kategorien betroffener Personen, z. B. Zugriff auf Gesundheitsdaten, Patienten
- Rechte und Pflichten des Auftraggebers sowie dessen Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung berechtigten Personen zur Vertraulichkeit
- Benennung der technischen und organisatorischen Maßnahmen, die das Unternehmen zum Schutz personenbezogener Daten durchführt
- Verpflichtung des Auftragnehmers zur Unterstützung des Auftraggebers bei Anfragen und Ansprüchen Betroffener im Zusammenhang mit der Auftragsverarbeitung und bei der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Verpflichtung des Auftragnehmers, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten bereitzustellen

6.5 Woher weiß man, dass der Auftragnehmer den Datenschutz einhält?

Hierzu empfehlen wir Ihnen, sich vom Dienstleister ein geeignetes Zertifikat vorlegen zu lassen, welches dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten beim Auftragnehmer dient (z. B. ISO/IEC 27001).

7 Technische und organisatorische Maßnahmen (TOM) zur Einhaltung des Datenschutzes

7.1 Was sind technische und organisatorische Maßnahmen?

Bei den technischen und organisatorischen Maßnahmen handelt es sich um Vorkehrungen, welche die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten sollen. Sie sollten schriftlich dokumentiert und in regelmäßigen Abständen auf ihre Wirksamkeit überprüft werden.

Technische Maßnahmen beziehen sich hierbei besonders auf die eingesetzte Hard- und Software und die Netzwerkkomponenten. Die organisatorischen Maßnahmen hingegen betreffen insbesondere den Ablauf, die Umstände und die verarbeitenden Personen selbst.

7.2 Welchen Zweck hat die Aufstellung der technischen und organisatorischen Maßnahmen?

Die Arztpraxen sind für den Schutz personenbezogener Daten verantwortlich und müssen daher sicherstellen, dass diese Daten entsprechend ihres jeweiligen Risikos angemessen geschützt werden. Um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten, muss der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen und dokumentieren.

7.3 Welche Maßnahmen müssen im Einzelnen getroffen und dokumentiert werden?

Eine abschließende Auflistung, welche Maßnahmen zu ergreifen sind, enthält das Gesetz an dieser Stelle nicht. Vielmehr sind die zu treffenden Maßnahmen von den besonderen Umständen, der Art der Daten und deren Kosten abhängig. Sie müssen ein dem Risiko angemessenes Schutzniveau gewährleisten. Auch wenn der Schutz zwingend zu gewährleisten ist, dürfen Arztpraxen die Kosten in die Auswahl der Maßnahmen einbeziehen.

Die DS-GVO gibt zudem einige Kriterien vor, welche bei der Auswahl der Maßnahmen berücksichtigt werden müssen. So sollte darauf geachtet werden, dass die getroffenen Maßnahmen dem aktuellen Stand der Technik entsprechen. Da die Entwickelung in diesem Bereich sehr dynamisch verläuft, sollten die ergriffenen Maßnahmen regelmäßig geprüft und bei Bedarf angepasst werden.

Aus der Datenschutz-Grundverordnung ergeben sich zwingend die Einhaltung der folgenden Maßnahmen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Datenbestände,
- der Einsatz von Systemen und Diensten, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten können,
- Sicherheitsmaßnahmen, um Daten bei physischen oder technischen Zwischenfällen wiederherstellen zu können (z. B. Backups),
- die Etablierung von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.
- Nach § 75b Abs. 4 Satz 1 SGB V ist die Richtlinie zur IT-Sicherheit der KBV in der vertragsärztlichen Versorgung verbindlich. Die Umsetzung dieser Vergaben hilft ebenfalls die Patientendaten noch sicherer zu verwalten und Risiken wie Datenverlust oder Betriebsausfall zu minimieren. Die Richtlinie umfasst auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur, die in der vertragsärztlichen Versorgung genutzt werden.

In der Praxis kann es bei der Auswahl der Maßnahmen helfen, sich den eigenen Praxisablauf, die Räumlichkeiten und den Praxisalltag vor Augen zu halten, um insbesondere zu prüfen, ob Patientendaten ausreichend geschützt sind, beispielsweise dadurch, dass Patientenakten nicht „offen herumliegen“, Telefonate zwischen Praxispersonal oder Arzt und Patient nicht mitgehört werden können und ähnliches. Sodann sollte überlegt werden, welche Maßnahmen bzw. Vorkehrungen Sie in den einzelnen Räumen oder an den einzelnen Computern Ihrer Praxis getroffen haben, damit ein Zugriff auf personenbezogene Daten (beispielsweise Patientenunterlagen) durch Unberechtigte (beispielsweise andere Patienten) vermieden wird.

Es ist darauf zu achten, dass Patientendaten, Patientenakten, Auskünfte über oder an Patienten streng vertraulich sind und keinen unberechtigten Personen (z. B. anderen Patienten) zur Kenntnis gelangen dürfen. Auch sollten die Mitarbeiter des Praxisteams zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DS-GVO verpflichtet werden.

7.4 Gibt es ein Muster für die Dokumentation der technischen und organisatorischen Maßnahmen?

Unter II.4 haben wir für Sie ein Muster sowie eine Erarbeitungshilfe zusammengestellt, welche Ihnen bei der Aufstellung der Maßnahmen helfen soll.

8. Verpflichtung der Praxismitarbeiter zum Datenschutz und zur Verschwiegenheit

Der Arzt/Psychotherapeut bzw. Praxisinhaber muss sicherstellen, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf dessen Anweisung verarbeiten. Es ist nicht verbindlich geregelt, wie diese Pflicht konkret umgesetzt werden muss, zu empfehlen ist jedoch die Einholung einer schriftlichen Verpflichtungserklärung.

8.1 Wer muss verpflichtet werden?

Neben den Praxismitarbeitern sind auch Auszubildende, Praktikanten, Leiharbeiter, ehrenamtlich Tätige usw. zu verpflichten.

8.2 Wann muss die Verpflichtung erfolgen?

Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen. Sie sollte daher möglichst (spätestens) am ersten Arbeitstag vorgenommen werden.

8.3 Wie muss eine Verpflichtung erfolgen?

Zuständig für die Verpflichtung ist der Arzt/Psychotherapeut bzw. der Praxisinhaber. Es wird empfohlen, ein Formular zu verwenden, das sowohl vom Arzt/Psychotherapeuten bzw. Praxisinhaber als auch von dem Verpflichteten unterschrieben wird. So kann sicher nachgewiesen werden, dass alle Beschäftigten auf die Beachtung der datenschutzrechtlichen Anforderungen sowie der

Schweigepflicht verpflichtet wurden. Die Verpflichtung selbst kann schriftlich oder in elektronischer Form erfolgen.

Die Beschäftigten müssen darüber informiert werden, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen.

8.4 Reicht es aus, die Beschäftigten einmalig datenschutzrechtlich zu verpflichten?

Die DS-GVO schreibt nicht vor, wie oft Beschäftigte datenschutzrechtlich zu verpflichten sind. Im Hinblick auf die hohe Bedeutung des Schutzes personenbezogener Daten, insbesondere im Gesundheitswesen, empfiehlt es sich, die Beschäftigten immer wieder zu sensibilisieren, beispielsweise im Rahmen von Schulungen, schriftlichen Hinweisen oder auch durch regelmäßiges Unterzeichnen und Besprechen des entsprechenden Formulars.

8.5 Gibt es ein Muster zur Datenschutzverpflichtung?

Ein Muster zur Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen finden Sie unter II.5.

9 Datenschutzerklärung auf der Internetseite

Welche Angaben muss die Datenschutzerklärung auf der Internetseite beinhalten?

Da auf jeder Internetseite personenbezogene Daten verarbeitet werden, benötigt auch jeder Webseitenbetreiber eine entsprechende Datenschutzerklärung. Ob es sich hierbei um die IP-Adresse des Besuchers, Browser-Daten oder Angaben aus einem Kontaktformular handelt, ist dabei unerheblich.

Zu den zwingenden Angaben auf der Praxiswebseite gehört zunächst der Name und die Kontaktdaten des Verantwortlichen. Hierbei handelt es sich in der Regel um den Praxisinhaber. Bei juristischen Personen, wie zum Beispiel einer GmbH, müssen die Daten der gesetzlichen Vertreter angegeben werden.

Auch die Zwecke und die Rechtsgrundlagen der Verarbeitung sowie die Dauer der Datenspeicherung müssen benannt werden. Weiterhin muss die Datenschutzerklärung die betroffenen Personen über ihre Rechte (Auskunft, Löschung, Einschränkung, Widerspruch, Datenübertragung, Beschwerderecht) aufklären. Soweit die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, ist diese zudem über ihr Widerrufsrecht zu informieren. Muss die Praxis aufgrund des BDSG einen Datenschutzbeauftragten bestellen, ist auch dieser im Rahmen der Datenschutzerklärung zu benennen.

Häufig werden auf Internetseiten Elemente von Sozialen Netzwerken eingebaut. Hierbei kann es sich um die Kommentarfunktion oder einen „Gefällt mir“-Button handeln. In solchen Fällen muss die Datenschutzerklärung auch hierüber informieren und über einen Link direkt zu den Datenschutzinformationen des jeweiligen Anbieters führen.

Nutzen Sie auf Ihrer Webseite Kontaktformulare zur Kommunikation mit Ihren Patienten, müssen Sie auch bezüglich dieser Datenverarbeitung ausführlich informieren.

Achten Sie immer darauf, dass Sie Daten nur für die Zwecke nutzen, für welche sie erhoben wurden. Die Nutzung von Daten für einen anderen, als die in der Datenschutzerklärung benannten Zwecke, ist nur in einem sehr engen Rahmen zulässig und sollte daher nie ohne rechtliche Prüfung geschehen.

Fehlende oder fehlerhafte Datenschutzerklärungen können als Verstoß gegen die DS-GVO Bußgelder nach sich ziehen. Daher empfehlen wir, diese durch einen Dienstleister erstellen oder zumindest prüfen zu lassen.

10 Meldungen von Datenschutzverletzungen

10.1 Wann liegt eine Verletzung des Schutzes personenbezogener Daten vor?

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die Sicherheit der Daten unbeabsichtigt oder unrechtmäßig verletzt wird und dies zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung bzw. zum unbefugten Zugang zu personenbezogenen Daten führt.

Beispiele sind der Verlust von Datenträgern, Übermittlung eines Faxes oder Briefes an einen falschen Empfänger oder ein erfolgreicher Angriff auf die Praxissoftware.

10.2 Was ist zu tun, wenn der Schutz personenbezogener Daten verletzt wurde?

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls an die zuständige Aufsichtsbehörde (TlfDI) gemeldet werden.

Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen (in der Regel des Patienten) führt. Ein solches Risiko kann z. B. durch eine geeignete Verschlüsselung personenbezogener Daten ausgeschlossen werden, welche beim Verlust eines Datenträgers die Kenntnisnahme der Daten durch Dritte verhindert.

Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, muss der Verantwortliche (Arzt/Psychotherapeut) auch die betroffene Person (Patient) ohne unangemessene Verzögerung benachrichtigen.

11 Rechte des Patienten

11.1 Patienteninformation über die Datenverarbeitung

11.1.1 Welchen Zweck hat die Patienteninformation?

Die Patienten müssen darüber informiert werden, was mit ihren Daten passiert. Die Information muss Angaben zum Zweck sowie zu den Rechtsgrundlagen der Datenverarbeitung enthalten sowie die Kontaktdaten der Praxis und ggf., soweit vorhanden, des Datenschutzbeauftragten der Praxis.

11.1.2 Muss der Patient die Information unterschreiben?

Nein, eine Unterschrift des Patienten zur Darlegung, dass der Patient über die Datenverarbeitung in der Arztpraxis informiert wurde, ist nicht erforderlich. Der Arzt kommt seiner Rechenschaftspflicht auch dadurch nach, indem er entweder einen Vermerk in der Patientenakte fertigt oder einen konkreten Verfahrensablauf beschreibt, wie in der Arztpraxis der Informationspflicht gegenüber den Patienten nachgekommen wird. Werden die Patienteninformationen beispielsweise im Zugangsbereich der Praxis gut sichtbar in entsprechender Größe ausgehängt, genügt dies um der Informationspflicht nachzukommen.

11.1.3 Darf die Behandlung des Patienten abgelehnt werden, wenn er die Patienteninformation nicht zur Kenntnis nehmen will?

Nein, eine solche Praxis wäre mit der Datenschutz-Grundverordnung nicht vereinbar. Die Informationspflicht des Arztes bezweckt, dass dem Patienten die Gelegenheit gegeben wird, die Information zur Verarbeitung seiner Daten einfach und ohne Umwege zu erhalten. Der Patient muss diese jedoch nicht zur Kenntnis nehmen, wenn er dies nicht möchte.

11.1.4 Gibt es ein Muster für die Information der Patienten?

Sie finden ein Muster auf der Internetseite der KBV unter:

https://www.kbv.de/html/dsgvo-in-der-praxis.php

11.2 Auskunftsanspruch

11.2.1 Hat der Patient ein Recht auf Einsicht in seine Patientenakte?

Mit dem Patientenrechtsgesetz wurde dem Patienten das Recht auf Einsicht in seine Akten ausdrücklich eingeräumt. Nach der Regelung des § 630g Abs. 1 BGB ist dem Patienten unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Das Einsichtsrecht betrifft auch Fremdbefunde und persönliche Notizen des Behandelnden.

Auch Art. 15 DS-GVO begründet einen Auskunftsanspruch des Patienten. Ob dieser jedoch zwingend die Einsicht in die Patientenakte beinhaltet, ist umstritten. Nach derzeitiger Auffassung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit kann dies im Einzelfall zutreffen, wenn die Einsicht beispielsweise erforderlich ist, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen. Grundsätzlich zielt Art. 15 DS-GVO jedoch nicht auf ein Recht der Einsichtnahme in die Patientenakte ab. Vielmehr begründet er ein Recht über die Auskunft, ob überhaupt personenbezogene Daten verarbeitet werden. Werden keine Daten verarbeitet, beinhaltet der Anspruch aus Art. 15 DS-GVO auch das Recht auf eine Negativauskunft. Somit müssen Sie die anfragende Person ebenfalls informieren, wenn Sie keine ihrer Daten verarbeiten. Zudem beinhaltet Art. 15 DS-GVO ein abschließende Aufzählung, welche Informationen eine Auskunft nach Art. 15 DS-GVO beinhalten muss.

11.2.2 Besteht das Recht das Patienten auf Einsichtnahme in seine Patientenakte ausnahmslos?

Das Recht auf Akteneinsicht kann in bestimmten Einzelfällen beschränkt sein. Stehen erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegen, ist eine Verweigerung der Einsichtnahme möglich. Die Verweigerung setzt voraus, dass durch Kenntnisnahme der Aufzeichnungen des Arztes dem Patienten in therapeutischer Hinsicht negative gesundheitliche Konsequenzen drohen können, zum Beispiel durch Selbstverletzungs- oder Suizidgefahr. Rechte Dritter können entgegenstehen, wenn die Behandlungsunterlagen sensible Informationen, zum Beispiel über Eltern oder Ehegatten beinhalten. Zu prüfen ist hierbei jedoch nicht nur ob erheblich therapeutische Gründe oder

sonstige erhebliche Rechte Dritter entgegenstehen, sondern auch in welchem Umfang das Einsichtsrecht hierdurch eingeschränkt werden kann. Gegebenenfalls kommt dennoch eine teilweise Akteneinsicht oder die Einsicht in teilweise geschwärzte Unterlagen in Betracht. Eine Ablehnung ist in jedem Fall gegenüber dem Patienten zu begründen.

11.2.3 Kann ein Recht auf Akteneinsicht auch in die Akten verstorbener Patienten bestehen?

Die ärztliche Schweigepflicht bleibt über den Tod des Patienten hinaus bestehen. Das Recht auf Einsichtnahme in die Patientenakte steht nach dem Tod des Patienten entweder dem Erben zu, wenn dieser vermögensrechtliche Interessen wahrnehmen möchte oder seinen nächsten Angehörigen soweit diese immaterielle Interessen verfolgen. In beiden Fällen ist die Einsichtnahme jedoch ausgeschlossen, soweit dieser der ausdrückliche oder mutmaßliche Wille des verstorbenen Patienten entgegen steht. Ob der mutmaßliche Wille des Verstorbenen der Einsichtnahme entgegensteht, ist hierbei durch den Behandelnden zu beurteilen.

11.3 Recht auf Löschung

In bestimmten Fällen können Patienten die Löschung ihrer Daten verlangen. Grundsätzlich steht diesem Anspruch jedoch die gesetzliche Dokumentations- und Aufbewahrungspflicht entgegen.

12 Fragen aus dem Praxisalltag

12.1 Darf man die Patienten im Wartezimmer mit dem Namen aufrufen?

Ja, dies ist möglich. Bezüglich dieser Fragestellung erfolgte auch eine Rücksprache mit dem TlfDI, der keinen Verstoß gegen geltende Datenschutzbestimmungen sieht, wenn Patienten mit Namen aufgerufen werden.

12.2 Ist die Verwendung eines Faxgerätes zur Übermittlung von personenbezogenen Daten zulässig?

Nein, aufgrund der technischen Veränderungen in den vergangenen Jahren kann das Fax nicht mehr als sicherer Übermittlungsweg betrachtet werden. Da heute kaum noch „reale“ Faxgeräte, sondern meist Fotokopierer mit Fax-Funktion oder Fax-Server, welche eingehende Faxe in E-Mails umleiten, eingesetzt werden, kommt dem heutigen Fax noch lediglich das Sicherheitsniveau einer unverschlüsselten E-Mail zu.

12.3 Was ist bei der Datenübermittlung per E-Mail zu beachten?

Aufgrund der Komplexität und Fehleranfälligkeit bei der zwingend erforderlichen Verschlüsselung, sollten Patientendaten nicht mehr per E-Mail übermittelt werden.

Für die sichere Übersendung sollte der Übermittlungsdienst KIM (Kommunikation im Medizinwesen) genutzt werden. Hier erfolgt neben der Verschlüsselung auch eine eindeutige Identifizierung der Absender und Empfänger.

12.4 Was ist bei der Übermittlung von Daten an Dritte (z. B. MDK, Krankenkassen, Versicherungen) zu beachten?

Bei der Übermittlung der personenbezogenen Daten ist darauf zu achten, dass für diese eine gesetzliche Grundlage existiert. Sofern Unsicherheiten bestehen, ob eine Übermittlung auf der Grundlage eines Gesetzes verpflichtend oder auch erlaubt ist, sollte sich der Arzt/Psychotherapeut von der anfordernden Stelle die Rechtsgrundlage nennen lassen, auf welcher diese ihr Ersuchen stützt. Die Übermittlungspflichten, die bisher galten, bestehen auch mit der Geltung der DS-GVO weiter fort.

Daneben ist es möglich, dass die personenbezogenen Daten auf der Grundlage der Einwilligung des Patienten an die anfordernde Stelle (z. B. Versicherungen) übermittelt werden können. Die Einwilligungserklärung muss in diesen Fällen inhaltlich dahingehend geprüft werden, ob die angeforderten Daten auch von dieser umfasst werden und der angefragte Arzt/Psychotherapeut entsprechend auch von seiner Schweigepflicht befreit wurde.

12.5 Welchen Umfang muss eine Schweigepflichtentbindung haben?

Zunächst muss die Schweigepflichtentbindung klar erkennen lassen, wer wen von der Schweigepflicht entbinden möchte. Auch muss klargestellt werden, für welchen Zweck der Patient den Arzt/Psychotherapeuten von der Schweigepflicht entbindet. Dem Patienten muss also bewusst sein, weshalb er hier auf die Schweigepflicht verzichtet.

Eine Schweigepflichtentbindung ist zudem nur dann wirksam, wenn sie hinreichend bestimmt ist. Eine vorweggenommene generelle Entbindung von der Schweigepflicht ist somit nicht wirksam. Sie muss anlassbezogen eingeholt werden und eindeutig ihren Umfang erkennen lassen.

12.6 Wann müssen die Daten gelöscht werden?

Grundsätzlich dürfen personenbezogene Daten nur solange aufbewahrt werden, bis sie ihren Zweck, zu welchem sie erhoben wurden, erfüllt haben. Darüber hinaus kann die Löschung auch dann erforderlich sein, wenn der Patient die Einwilligung in die Datenverarbeitung widerrufen hat. Es bestehen jedoch gesetzliche Ausnahmen, welche eine längere Aufbewahrung rechtfertigen. Die wichtigste Ausnahme für den Arzt bildet das Bestehen einer vertraglichen oder satzungsgemäßen Aufbewahrungspflicht. Für den Bereich der ärztlichen Dokumentation gilt grundsätzlich eine 10-jährige Aufbewahrungspflicht. Es können sich darüber hinaus längere Aufbewahrungsfristen ergeben (z.B.: 30 Jahre für Aufzeichnungen von Strahlenbehandlungen). Auch unter dem Gesichtspunkt der Rechtsverteidigung vor Ansprüchen von Patienten ist eine Aufbewahrung von personenbezogenen Daten denkbar.

12.7 Wie müssen Patientendaten nach der Aufbewahrungsfrist entsorgt werden?

Bei Patientenakten handelt es sich um personenbezogene Daten besonderer Kategorien, weshalb auch bei der Entsorgung ein besonders hohes Schutzniveau erforderlich ist. Keinesfalls dürfen Patientenakten über den normalen Müll entsorgt werden.

Papierakten sollten daher mindestens mit Aktenvernichtern der Sicherheitsstufe P-4 vernichtet werden. Digitale Datenträger müssen entweder physisch zerstört oder so gelöscht werden, dass deren Inhalt auch mit spezieller Software und Kenntnissen nicht wieder hergestellt werden kann. Daher sollten Sie sich hierfür eines entsprechenden Dienstleisters bedienen. Hierbei ist jedoch darauf zu achten, dass mit diesen Dienstleistern ein entsprechender Auftragsverarbeitungsvertrag geschlossen werden muss, da es sich um eine Datenverarbeitung handelt (siehe Punkt 6). Weitere Informationen hierzu finden Sie auf unserer Internetseite.

12.8 Dürfen personenbezogene Daten und Gesundheitsdaten über WhatsApp an den Patienten oder Dritte übermittelt werden?

Die Nutzung des Messenger Dienstes WhatsApp auf dem Diensthandy des Arztes/Psychotherapeuten stellt einen Verstoß gegen die DS-GVO dar, wenn hierfür nicht das Einverständnis der von der Datenverarbeitung betroffenen Person eingeholt wurde.

Grund hierfür ist, dass das Handy-Adressbuch des Arztes ausgelesen wird und die Daten an einen Server weitergeleitet werden, um diese mit bereits dort gespeicherten Daten abzugleichen. Der Arzt/Psychotherapeut benötigt von jedem in seinem Handy gespeicherten Patienten oder Dritten eine Einwilligung zur Kontaktaufnahme über WhatsApp, sofern eine dienstliche Nutzung des Gerätes erfolgt.

12.9 Dürfen Papierdokumente für die digitale Aktenführung gescannt und anschließend vernichtet werden (ersetzendes Scannen)?

Aufgrund der Digitalisierung im Gesundheitswesen ist es naheliegend, seine Papierdokumente durch Scannen in die digitale Patientenakte importieren zu wollen. Grundsätzlich ist dies auch zulässig, soweit Sicherungs- und Schutzmaßnahmen ergriffen werden, mit denen Veränderungen, Vernichtung oder unrechtmäßige Verwendungen verhindert werden können.

Was passiert jedoch mit den Papierakten, nachdem diese eingescannt wurden? Bevor diese vernichtet werden, sollte man sich über die Folgen Gedanken machen. Die eingescannten elektronischen Unterlagen haben vor Gericht nicht denselben Beweiswert wie die Originalurkunde. Drucken Sie das Dokument wieder aus, erzeugen Sie hierdurch lediglich eine Kopie des Originals, welche nur als widerlegbarer Anscheinsbeweis und nicht als Urkundenbeweis gewertet wird.

Daher liegt die Entscheidung, ob die Unterlagen vernichtet werden sollen, bei Ihnen und sollte Einzelfallbezogen gefällt werden.

Um die höchstmögliche Sicherheit beim ersetzenden Scannen zu erreichen, sollte zudem nach der Vorgaben der TR-RESISCAN (BSI Technische Richtlinie 03138) verfahren werden. Diese finden Sie auf der Webseite des Bundesamtes für Sicherheit und Informationstechnik (BSI).

12.10 Wer ist die zuständige Aufsichtsbehörde für datenschutzrechtliche Angelegenheiten für die in Thüringen niedergelassenen Ärzte und Psychotherapeuten?

Dies ist in Thüringen der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit: Dr. Lutz Hasse, Häßlerstraße 8, in 99096 Erfurt.

Die Postanschrift lautet:

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Postfach 900455
99107 Erfurt

II Muster

Nachfolgend haben wir Ihnen einige Muster angefügt, welche Ihnen bei der Einhaltung der datenschutzrechtlichen Vorgaben helfen sollen.

Unsere Muster wählen eine möglich Art und Weise der Dokumentation und sind nicht zwingend in dieser Form umzusetzen. Bei der Verwendung der Muster ist darauf zu achten, dass diese jeweils an die Gegebenheiten in der eigenen Arztpraxis angepasst werden müssen. Beispiele oder Maßnahmen, die Sie in einigen Mustern finden, sind nicht abschließend aufgeführt, sondern dienen lediglich als Hilfe und Orientierung.

Alle Muster finden Sie zudem auch als Download auf der Internetseite der KVT unter https://www.kvt.de/?id=1607.

1 Einwilligung in die Datenverarbeitung

Patienteneinwilligung in die Datenverarbeitung

Hiermit willige ich _____ _____
Name, Vorname Geburtsdatum

_____
Adresse

ein, dass die mich betreffenden Behandlungsdaten und Befunde von meinem behandelnden Arzt /Psychotherapeuten

Praxisname und Anschrift:_____

(bitte zutreffendes ankreuzen)

☐

an die nachfolgend benannten weiterbehandelnden Ärzte, Psychotherapeuten, Krankenhäuser oder sonstigen medizinischen Leistungserbringer

Name und Adresse des Empfängers:_____

Name und Adresse des Empfängers:_____

Name und Adresse des Empfängers:_____

zum Zwecke der durchzuführenden Dokumentation und weiteren Behandlung übermittelt werden dürfen.

☐

von den nachfolgend benannten Ärzten, Psychotherapeuten, Krankenhäusern oder sonstigen medizinischen Leistungserbringern

Name und Adresse des Empfängers:_____

Name und Adresse des Empfängers:_____

Name und Adresse des Empfängers:_____

zum Zwecke der Dokumentation und der weiteren Behandlung erhoben werden dürfen.

Auf die „Patienteninformation zum Datenschutz“ wurde ich hingewiesen und ich habe diese inhaltlich zur Kenntnis genommen.

Widerruf

Mir ist bekannt, dass ich diese Einwilligungserklärung gegenüber meinem behandelnden Arzt/Psychotherapeuten jederzeit ganz oder teilweise mit Wirkung für die Zukunft widerrufen kann. Bisher durchgeführte, von dieser Einwilligung abgedeckte Datenübermittlungen bleiben rechtmäßig.

_____ _____
Ort, Datum Unterschrift des Patienten (ggf. des gesetzlichen Vertreters)

2 Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO	Vorblatt

Angaben zum Verantwortlichen Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.	
Name	Dr. Max Mustermann
Straße	Straße des Datenschutzes 1
Postleitzahl	12345
Ort	Musterstadt
Telefon	0123/456789
E-Mail-Adresse	praxis@mustermann.de

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen	
Name	-
Straße	-
Postleitzahl	-
Ort	-
Telefon	-
E-Mail-Adresse	-

Angaben zum Vertreter des Verantwortlichen Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.	
Name	-
Straße	-
Postleitzahl	-
Ort	-
Telefon	-
E-Mail-Adresse	-

Angaben zur Person des Datenschutzbeauftragten* (extern mit Anschrift) *sofern gem. Artikel 37 DS-GVO benannt			
Anrede	Frau	Titel	
Name, Vorname	Gewissenhaft, Anna		
Straße	Straße des Datenschutzes		
Postleitzahl	12345		
Ort	Musterstadt		
Telefon	0123/456789		
E-Mail-Adresse	datenschutzpraxis@mustermann.de		

Verarbeitungstätigkeit: Benennung: Anlegen einer Patientenakte		Lfd. Nr.: 1
Datum der Einführung:	Datum der letzten Änderung:	
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	Dr. Max Mustermann 0123/456789 praxis@mustermann.de	
Zwecke der Verarbeitungstätigkeit Art. 30 Abs. 1 S. 2 lit b)	Behandlungsdokumentation	
Optional: Name des eingesetzten Verfahrens		
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	[x] Patienten [ ] … [ ] ... [ ] … [ ] … [ ] [ ] [ ]	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 1 lit. c)	[x] Personenstammdaten [ ] [ ] Besondere Kategorien personenbezogener Daten (Art. 9): [x] Gesundheitsdaten (Anamnesedaten, Diagnosedaten, Befunddaten, Labordaten, Fremdbefunde)	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	[x]	intern (Zugriffsberechtigte) - Mitarbeiter
	[x]	extern Empfängerkategorie - Vor-, Mit- und Nachbehandelnder, Krankenkassen, MDK - Pflegeeinrichtungen, Krankenhäuser - Unfallversicherungsträger, Rentenversicherungsträger - Gerichte, Angehörige, Erben, Versicherungen
	[ ]	Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an einer Drittland oder an einer internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e) Nennung der konkreten Datenempfänger sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	[x]	Datenübermittlung findet nicht statt und ist auch nicht geplant
	[ ]	Datenübermittlung findet wie folgt statt: Drittland oder internationale Organisation (Name) Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	Frühestens 10 Jahre nach Behandlungsende (gesetzliche Aufbewahrungsfrist); ggf. Aufbewahrung bis zu 30 Jahren (Röntgenbehandlung, Strahlenbehandlung, Aufzeichnungen gem. Transplantationsgesetz)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DS-GVO (Art. 30 Abs. 1 S. 2 lit. g) siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8

.....	.....	.....
Verantwortlicher	Datum	Unterschrift

3 Muster Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

Inhaltsverzeichnis

1 Zusammenfassung

…

Ergebnis der Datenschutz-Folgenabschätzung:

…

2 DatenschutzFolgenabschätzung

…

2.1 Systematische Beschreibung der Verarbeitungsvorgänge (Artikel 35 Absatz 7 Buchstabe a DS-GVO)

…

2.1.1 Kategorien von Verarbeitungsvorgängen

Sollte die Datenverarbeitung in unterschiedlichem Umfang erfolgen, sollten hier Kategorien gebildet werden. Hier kann zum Beispiel zwischen Daten unterschieden werden, die ausschließlich gespeichert oder transportiert werden, Daten, deren Weiterverarbeitung ausschließlich die Verschlüsselung oder Authentifizierungen betrifft oder Daten, die umfangreich weiterverarbeitet oder weitergegeben werden.

2.1.2 Systematische Beschreibung

Die systematische Beschreibung hat nach Erwägungsgrund (ErwG) sowie Art 35 Absatz 7 Buchstabe a und Absatz 8 DS-GVO sowie nach den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679, wahrscheinlich ein hohes Risiko mit sich bringt“ der Artikel-29-Datenschutzgruppe (WP 248) zu enthalten:

Kriterium	Beschreibung
Art der Verarbeitung: (ErwG 90 DS-GVO)	*Soweit in 2.1.1 Kategorien nach den Verarbeitungsvorgängen gebildet wurden, kann hier darauf verwiesen werden.*
Umfang der Verarbeitung: (ErwG 90 DS-GVO)	*Neben dem Umfang der jeweiligen Verarbeitungen sollten hier die von der Verarbeitung betroffenen Personen benannt werden.*
Umstände bzw. Kontext der Verarbeitung: (Artikel-29-Datenschutzgruppe, WP 248,21)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Zweck der Verarbeitung: (Art. 35 Absatz 7 Buchstabe a DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*

Empfängerinnen und Empfänger: (Artikel-29-Datenschutz-gruppe, WP 248, 21)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Speicherdauer: (Artikel-29-Datenschutzgruppe, WP 248, 21)	
Funktionelle Beschreibung der Verarbeitung: (Artikel 35 Absatz 7 Buchstabe a DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Beschreibung der Anlagen (Hard- und Software bzw. sonstige Infrastruktur): (Artikel-29-Datenschutz-gruppe, WP 248, 21)	
Eingehaltene, gemäß Artikel 40 DS-GVO genehmigte Verhaltensregeln: (Artikel-29-Datenschutz-gruppe, WP 248, 21)	

2.2 Notwendigkeit und Verhältnismäßigkeit (Artikel 35 Absatz 7 Buchstabe b DS-GVO)

Im Rahmen der Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge müssen nach den ErwGen 90 und 96, nach Artikel 35 Absatz 7 Buchstabe b und d DS-GVO sowie nach den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679, wahrscheinlich ein hohes Risiko mit sich bringt“ der Artikel-29-Datenschutzgruppe (WP 248) Maßnahmen zur Einhaltung der Verordnung bestimmt werden, wobei Folgendes berücksichtigt werden muss:

Maßnahmen im Sinne der Verhältnismäßigkeit und Notwendigkeit der Verarbeitung (Artikel 5 und 6 DS-GVO) sowie Maßnahmen im Sinne der Rechte der Betroffenen (Art. 12 bis 21, 28, 36 und Kapitel V DS-GVO)

Kriterium	Beschreibung
Festgelegter Zweck: (Artikel 5 Absatz 1 Buchstabe b DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Eindeutiger Zweck: (Artikel 5 Absatz 1 Buchstabe b DS-GVO)	
Legitimer Zweck: (Artikel 5 Absatz 1 Buchstabe b DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Rechtmäßigkeit der Verarbeitung: (Artikel-29-Datenschutz-gruppe, WP 248, 21 i. V. m. Artikel 6 DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Angemessenheit und Erheblichkeit der Verarbeitung, Beschränktheit der Verarbeitung auf das notwendige Maß: (Artikel-29-Datenschutz-gruppe, WP 248, 21 i. V. m. Artikel 5 Absatz 1 Buchstabe c DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*

Speicherbegrenzung: (Artikel-29-Datenschutzgruppe, WP 248, 21 i. V. m. Artikel 5 Absatz 1 Buchstabe e DS-GVO)	
Informationspflicht gegenüber Betroffenen: (Artikel-29-Datenschutz-gruppe, WP 248, 21 i. V. m. Artikel 12, 13 und 14 DS-GVO)	*Soweit nötig kann auch hier eine Unterscheidung nach 2.1.1 erfolgen.*
Auskunftsrecht der betroffenen Personen: (Artikel-29-Datenschutz-gruppe, WP 248, 21 i. V. m. Artikel 15 DS-GVO)	
Recht auf Berechtigung und Löschung: (Artikel-29-Datenschutz-gruppe, WP 248, 21 i. V. m. Artikel 16, 17 und 19)	
Recht auf Datenübertragbarkeit: (Artikel 20 DS-GVO)	
Auftragsverarbeiterinnen und Auftragsverarbeiter: (Artikel 28 DS-GVO)	
Schutzmaßnahmen bei der Übermittlung in Drittländer: (Kapitel V DS-GVO)	*Soweit unter 2.1.1 unterschiedliche Kategorien gebildet wurden, sollten diese hier aufgegriffen und unterschieden werden.*
Vorherige Konsultation: (Artikel 36 und EwrG 96 DS-GVO)	

2.3 Risiken für die Rechte und Freiheiten der betroffenen Personen (Artikel 35 Absatz 7 Buchstabe c DS-GVO)

Die Risiken für die Rechte und Freiheiten der betroffenen Personen sind nach ihrer Ursache, Art, Besonderheit, Schwere und Eintrittswahrscheinlichkeit zu bewerten (ErwGe 76, 77, 84 und 90 DS-GVO).

Risikoquellen sind

…

…

…

Die Risikobewertung orientiert sich am Standard-Datenschutzmodell (SDM) der Aufsichtsbehörden für den Datenschutz und den dort definierten Gewährleistungszielen. Die Schadens- und Eintrittswahrscheinlichkeitsstufen sowie die Risikomatrix orientiert sich am DSK-Kurzpapier Nummer 18 „Risiko für Rechte und Freiheiten natürlicher Personen“ i. V. m. der ISO/IEC 29134:2017 zum Privacy Impact Assessment. In der folgenden Tabelle werden die einzelnen Risiken identifiziert, inklusive Schadenshöhe, Schadensereignissen, betroffenen Gewährleistungszielen des Standard-Datenschutzmodells und Eintrittswahrscheinlichkeit. Die Bewertung der Eintrittswahrscheinlichkeit erfolgt unter Berücksichtigung der referenzierten Abhilfemaßnahmen, die detailliert in Abschnitt 2.4 beschrieben sind.

Schaden	Beschreibung der Schadensereignisse	Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)
Physische, materielle oder immaterielle Schäden, finanzielle Verluste, erhebliche wirtschaftliche Nachteile: (ErwG 90 i. V. m. 85 DS-GVO) **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … … …
Verlust der Kontrolle über personenbezogene Daten: (ErwG 90 i. V. m. 85 DS-GVO) **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Transparenz, Intervenierbarkeit	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … …
Diskriminierung, Rufschädigung, erhebliche gesellschaftliche Nachteile: (ErwG 90 i. V. m. 85 DS-GVO) **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … …
Identitätsdiebstahl oder -betrug: (ErwG 90 i. V. m. 85 DS-GVO) **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … …
Verlust der Vertraulichkeit bei Berufsgeheimnissen: (ErwG 90 i. V. m. 85 DS-GVO) **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Datenminimierung, Vertraulichkeit, Integrität	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … …
Beeinträchtigung/Verlust der Verfügbarkeit: **Schadenshöhe:** ***(geringfügig, mittel, groß)***	… Betroffene Gewährleistungsziele (SDM): Verfügbarkeit	EWS: ***(geringfügig, mittel, groß)*** Abhilfemaßnahmen: … … …

2.4 Abhilfemaßnahmen (Artikel 35 Absatz 7 Buchstabe d DS-GVO)

Gemäß Artikel 35 Absatz 7 Buchstabe d DS-GVO sind zur Bewältigung der Risiken Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren umzusetzen, durch die die Risiken für die Rechte der Betroffenen eingedämmt werden und der Schutz personenbezogener Daten sichergestellt wird.

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den ErwGen 28, 78 und 83 DS-GVO genannt:

Kriterium	Beschreibung
Minimierung der Verarbeitung personenbezogener Daten: (ErwG 78 DS-GVO)	
Schnellstmögliche Pseudonymisierung personenbezogener Daten: (ErwG 28 und 78 DS-GVO)	
Transparenz in Bezug auf die Funktion und die Verarbeitung personenbezogener Daten: (ErwG 78 DS-GVO)	
Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen: (ErwG 78 DS-GVO)	
Datensicherheitsmaßnahmen: (ErwG 78 und 83 DS-GVO)	

Datum: Unterschrift:

---------- ----------

4 Muster für die Dokumentation der technischen und organsiatorischen MaßnahmenEinwilligung in die Datenverarbeitung

Verzeichnis
der technischen und organisatorischen Maßnahmen
nach Artikel 32 Datenschutz-Grundverordnung
(im Weiteren: DS-GVO)

Nachfolgend werden die technischen und organisatorischen Maßnahmen (TOM) aufgelistet, die seitens des Verantwortlichen ergriffen worden sind, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

A. Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

1.1.	Alarmanlage	- Eingangsbereich - …
1.3.	Schließsystem	- Sicherheitsschlösser - …
1.4.	räumliche Abgrenzungen	- Technikraum - Arbeitszimmer - …
1.5.	Anwesenheitskontrolle	- Zeiterfassungssystem - Protokollierung - …..

2. Zugangskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten die Nutzung von Datenverarbeitungssystemen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

2.1.	Zugriffs-, Berechtigungs- und Rechtekonzept	- persönlicher und individueller User-Log-In - Passwortrichtlinie - Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechten - …
2.2.	sichere Hard- und Software	- regelmäßige Anpassung an den aktuellen Stand der Technik/aktuelle Versionen der Software - …
2.3.	IT-Sicherheitsmaßnahmen	- Sperren von externen Schnittstellen (z. B. USB) - Bildschirmsperren mit Passwortaktivierung - Abschluss von Auftragsverarbeitungsverträgen - …

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nicht unbefugt verarbeitet werden:

3.1.	Zugriffs-, Berechtigungs- und Rechtekonzept	- Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechten - Verwaltung der Rechte durch Systemadministrator - Verschlüsselung von externen Datenträgern - Zugriffsbeschränkungen durch: o verschließbare Aktenschränke o verschließbare Datentonnen - …
3.2.	Datenvernichtung	- datenschutzkonforme Löschung von Datenträgern vor Wiederverwendung - Einsatz von Dienstleistern zur datenschutzkonformen Vernichtung von Datenträgern - …

B. Integrität

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

1.1.	Übermittlungssicherheit	- Einsatz von VPN-Technologie - Protokollierung von Datentransport - Verschlüsselung von Datenträgern - gesicherter Datentransport (z. B. SSL) - …
1.2.	nutzerbasierte Protokollierung der Verarbeitung	- von regelmäßigen Abruf- und Übermittlungsvorgängen - …

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen verarbeitet wurden:

2.1.	Zugriffs-, Berechtigungs- und Rechtekonzept	- Erteilung von Zugangsberechtigungen durch mehrstufiges Freigabeverfahren - Verwaltung der Rechte durch Systemadministrator - Mehraugenprinzip - …
2.2.	nutzerbasierte Protokollierung der Verarbeitung	- der Eingabe, Änderung und Löschung von Daten

3. Kontrolle der Auftragsverarbeiter

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber hat den Auftragsverarbeiter unter den folgenden Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) auszuwählen und zu beauftragen:

3.1.	Geeignetheits- und Zuverlässigkeitsprüfung	- datenschutzkonforme, insbesondere den Anforderungen des Art. 28 DS-GVO entsprechende Verarbeitung - Verarbeitung nur innerhalb der EU - …
3.2.	Protokollierung	- des Auswahlverfahrens und der Vertragsgestaltung

C. Verfügbarkeit / Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

1.1.	Havarieschutz	- unterbrechungsfreie Stromversorgung - Feuer- und Rauchmeldeanlagen - Rauchverbot im Gebäude - …
1.2.	Backup- und Recovery-System	- Backup- & Recovery-Konzept - Testen der Datenwiederherstellung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort - …

2. Trennungskontrolle

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

2.1.	Zugriffs-, Berechtigungs- und Rechtekonzept	- Erteilung von Zugangsberechtigungen durch mehrstufiges Freigabeverfahren - Verwaltung der Rechte durch Systemadministrator - verschließbare Aktenschränke - …
2.2.	Trennungsprinzip und Zweckzuordnung	- Trennung von Produktiv- und Testsystemen

D. Organisationskontrolle

Maßnahmen, die gewährleisten, dass die vorgenannten technischen und organisatorischen Maßnahmen eingehalten und regelmäßig evaluiert werden.

1.1.	Datenschutzkonzept	- Konzept zur Überwachung und regelmäßigen Evaluierung
1.2.	Fachbeauftragte	- Datenschutzbeauftragter

Erarbeitungshilfe „technischer und organisatorischer Maßnahmen“

Eingang-Zutrittskontrolle

- Wer hat Praxisschlüssel?
- Schließ-/Alarmanlage vorhanden?
- Wer hat wann wie Zutritt/Zugang zur Praxis?

Empfang

- Diskretion in den Praxisräumlichkeiten, beispielsweise durch Trennung des Anmeldebereiches vom Wartebereich.
- Am Anmeldebereich könnte ein Schild aufgestellt werden, dass am Tresen Abstand gehalten werden soll, wenn mehrere Patienten dort warten. Dritte sollen am Empfang oder im Behandlungsraum keine Gespräche mithören können.
- sichere Verwahrung von Patientenakten; Patientenakten dürfen niemals „offen herumliegen“, sondern sind so zu positionieren, dass andere Patienten und sonstige Unbefugte wie beispielsweise Handwerker, EDV-Dienstleister oder Reinigungspersonal diese nicht einsehen können.
- Computer müssen passwortgeschützt sein, es sollte eine automatische Bildschirmsperre aktiviert werden.
- Bei Auskünften am Telefon muss darauf geachtet werden, dass es sich bei dem Anrufer tatsächlich um den Patienten oder einen auskunftsberechtigten Dritten handelt. Das kann z. B. durch gezielte Zusatzfragen oder einen Rückruf sichergestellt werden. Außerdem ist darauf zu achten, dass bei telefonischen Auskünften die umstehenden Patienten keine Rückschlüsse auf die Person des Anrufers und dessen gesundheitliche Daten ziehen können (Wahrung des Patientengeheimnisses, Schweigepflicht).
- Gespräche im Praxisteam über Patienten und deren personenbezogene Daten finden nie im Beisein von Patienten statt, um zu gewährleisten, dass das Patientengeheimnis und die Schweigepflicht gewahrt sind.

Behandlungsräume

- sichere Verwahrung von Patientenakten; Patientenakten dürfen niemals „offen herumliegen“, sondern sind so zu positionieren, dass andere Patienten und sonstige Unbefugte wie beispielsweise Handwerker, EDV-Dienstleister oder Reinigungspersonal diese nicht einsehen können.
- sicherstellen, dass Patient keine Informationen über andere Patienten erhält (keine Telefonate mit einem anderen Patienten während der Behandlung)
- Computer müssen passwortgeschützt sein/Bildschirmschoner

Datensicherheit

- Versendung von Patientendaten über das Internet (z. B. E-Mail, WhatsApp oder ähnliches) nur verschlüsselt
- Erteilung von Zugriffsberechtigungen, um klar zu regeln, wer in der Praxis auf Dateien und Ordner zugreifen kann

- Computer müssen passwortgeschützt sein, es sollte eine automatische Bildschirmsperre aktiviert werden.
- regelmäßiges Ändern des Passwortes
- aktuelle Virenschutzprogramme, Firewalls
- regelmäßige Datensicherung
- Sicherung gegen Diebstahl, Einbruch - Alarmanlage
- Es wird festgelegt, wann und durch wen personenbezogene Daten gelöscht oder vernichtet werden (wenn die Aufbewahrungsfrist abgelaufen ist)/Datenträger, Papier.
- Patientenakten werden nach DIN-Normen vernichtet.
- Datenschutzverpflichtung des Praxispersonals
- Schutzmaßnahmen bei digitaler Datenübertragung
- Maßnahmen, die dazu dienen, personenbezogene Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall möglichst schnell wieder herzustellen

Datenschutzpanne

- Es wird festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (in der Regel an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden, in Thüringen der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit).

5 Muster zur Verpflichtung der Mitarbeiter

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Herr/Frau ….....
(Mitarbeiter, Vorname, Name, Geburtsdatum)

wurde besonders darauf hingewiesen, dass die ärztliche Schweigepflicht und die Grundsätze zur Beachtung des Datenschutzes, insbesondere der Regelungen der DS-GVO nicht nur für den Arzt/Psychotherapeuten selbst gelten, sondern auch für die übrigen Praxismitarbeiter. Eine Arzt-/Psychotherapeutenpraxis arbeitet mit besonders sensiblen personenbezogenen Daten, die einen hohen Schutz genießen. Herr/Frau …..... wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Artikel 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Transparenz);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiter verarbeitet werden (Zweckbindung);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Richtigkeit);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Speicherbegrenzung);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung Ihrer Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar dieser Verpflichtung habe ich erhalten.

….....
(Ort, Datum)

….....
(Unterschrift des Verantwortlichen)

….....
(Unterschrift des Verpflichteten)

6 Muster für Patienteninformation

Patienteninformation zum Datenschutz

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutz-Grundverordnung (DS-GVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Praxis Daten erhebt, speichert oder weiterleitet. Der Information können Sie auch entnehmen, welche Rechte Sie in puncto Datenschutz haben.

1. VERANTWORTLICHKEIT FÜR DIE DATENVERARBEITUNG

Verantwortlich für die Datenverarbeitung ist:
Praxisname:
Adresse (Straße, Hausnummer, Postleitzahl, Ort):
Kontaktdaten (z. B. Telefon, E-Mail-Adresse):

Sie erreichen die/den zuständige/n Datenschutzbeauftragte/n unter:
Name:
Anschrift:
Kontaktdaten:

2. ZWECK DER DATENVERARBEITUNG

Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag zwischen Ihnen und Ihrem Arzt und die damit verbundenen Pflichten zu erfüllen. Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen, Therapievorschläge und Befunde, die wir oder andere Ärzte erheben. Zu diesen Zwecken können uns auch andere Ärzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfügung stellen (z. B. in Arztbriefen). Die Erhebung von Gesundheitsdaten ist Voraussetzung für Ihre Behandlung. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

3. EMPFÄNGER IHRER DATEN

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn dies gesetzlich erlaubt ist oder Sie eingewilligt haben. Empfänger Ihrer personenbezogenen Daten können vor allem andere Ärzte/Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern und privatärztliche Verrechnungsstellen sein. Die Übermittlung erfolgt überwiegend zum Zwecke der Abrechnung der bei Ihnen erbrachten Leistungen, zur Klärung von medizinischen

und sich aus Ihrem Versicherungsverhältnis ergebenden Fragen. Im Einzelfall erfolgt die Übermittlung von Daten an weitere berechtigte Empfänger.

4. SPEICHERUNG IHRER DATEN

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies für die Durchführung der Behandlung erforderlich ist. Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren. Nach anderen Vorschriften können sich längere Aufbewahrungsfristen ergeben, z. B. 30 Jahre bei Röntgenaufzeichnungen laut § 28 Abs. 3 der Röntgenverordnung.

5. IHRE RECHTE

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten Auskunft zu erhalten. Auch können Sie die Berichtigung unrichtiger Daten verlangen. Darüber hinaus steht Ihnen unter bestimmten Voraussetzungen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu.

Die Verarbeitung Ihrer Daten erfolgt auf Basis von gesetzlichen Regelungen. Nur in Ausnahmefällen benötigen wir Ihr Einverständnis. In diesen Fällen haben Sie das Recht, die Einwilligung für die zukünftige Verarbeitung zu widerrufen.

Sie haben ferner das Recht, sich bei der zuständigen Aufsichtsbehörde für den Datenschutz zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.
Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:
Name:
Anschrift:

6. RECHTLICHE GRUNDLAGEN

Rechtsgrundlage für die Verarbeitung Ihrer Daten ist Artikel 9 Absatz 2 lit. h) DS-GVO in Verbindung mit § 22 Abs. 1 Nr. 1 Buchst. b BDSG. Sollten Sie Fragen haben, können Sie sich gern an uns wenden.

Ihr Praxisteam

7 Muster Auskunftsersuchen nach Art. 15 DS-GVO

Auskunftsersuchen nach Art. 15 DS-GVO

Sehr geehrte/r Frau/Herr ……,

anbei erhalten Sie die Auskunft über Ihre von mir/uns verarbeiteten personenbezogenen Daten nach Art. 15 DS-GVO.

Verarbeitungszwecke:

Ihre personenbezogenen Daten werden zu folgenden Zwecken verarbeitet:

……

……

……

……
(Bsp.: Behandlung, Behandlungsdokumentation, Kontaktaufnahme, ...)

Kategorien personenbezogener Daten:

- Personenstammdaten:
  - ……
  - ……
    (Bsp.: Name, Vorname, Geburtsdatum)

- Versichertenstammdaten
  - ……
  - ……
    (Bsp.: Krankenkasse, Versichertennummer)

- Kontaktdaten:
  - ……
  - ……
    (Bsp.: Adresse, Handynummer, Telefonnummer, E-Mail-Adresse)

- Gesundheitsdaten
  - ……
  - ……
    (Bsp.: Befunde, Diagnosen, Angaben zur Arbeitsunfähigkeit)

Empfänger der Daten:

Ihre personenbezogenen Daten werden, soweit nötig, an folgende Empfänger übermittelt:

- ……
- ……
- ……..
  (Bsp.: Kassenärztliche Vereinigung, mit- oder weiterbehandelnde Ärzte, Kostenträger)

Speicherdauer:

Soweit der Löschung keine Aufbewahrungsvorschriften entgegenstehen, werden Ihre Daten gelöscht, sobald diese für die oben genannten Zwecke nicht mehr benötigt werden. Aufgrund gesetzlicher Vorschriften werden die Daten jedoch für mindestens zehn Jahre nach Ende der Behandlung aufbewahrt.

Betroffenenrechte:

Ihnen steht das Recht auf Berichtigung oder Löschung der Sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder ein Widerspruchsrecht gegen die Verarbeitung zu. Zur Ausübung dieser Rechte wenden Sie sich bitte an:

……
(E-Mail-Adresse oder Telefonnummer der Kontaktperson)

Beschwerderecht:

Sie haben, unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs, das Recht auf Beschwerde bei der Aufsichtsbehörde :

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Postfach 90 04 55 | 99107 Erfurt
Häßlerstraße 8 | 99096 Erfurt

Herkunft der Daten:

Soweit die personenbezogene Daten nicht bei Ihnen selbst erhoben wurden, stammen die Daten von:

- ……
- ……..
  (Bsp.: mit- oder weiterbehandelnder Arzt, Krankenkasse)

Automatisierte Entscheidungsfindung und Profiling:

Automatisierte Entscheidungsfindungen und Profiling finden nicht statt.

Übermittlung an ein Drittland oder eine internationale Organisation:

Übermittlungen an ein Drittland oder eine internationale Organisation findet nicht statt.
(Sollte doch eine Übermittlung stattfinden, sind hier die geeigneten Garantien nach Art 46 DS-GVO zu nennen.)

III Begriffsbestimmungen – Datenschutz von A bis Z

Aufsichtsbehörde	Aufsichtsbehörde für den Datenschutz ist in Thüringen der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit. Dr. Lutz Hasse Häßlerstraße 8 99096 Erfurt Postanschrift: Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Postfach 900455 99107 Erfurt poststelle@datenschutz.thueringen.de Tel.: 03 61 / 57 311 29 00 Fax : 03 61 / 57 311 29 04
Auftragsverarbeitung	Auftragsverarbeitung ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gem. den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages. Beispiel: Firma zur Wartung Praxis EDV, Firma, die Daten vernichtet oder Akten aufbewahrt
Betroffenenrechte	Die Rechte desjenigen, dessen personenbezogene Daten verarbeitet, erhoben, gespeichert oder übermittelt werden. Beispiel: Informationspflicht, Auskunftsrecht, Löschung, Berichtigung
Datenschutzbeauf-tragter	Der Datenschutzbeauftragte unterrichtet und berät den Verantwortlichen (Arzt) oder den Auftragverarbeiter sowie die Beschäftigten, überwacht die Einhaltung datenschutzrechtlicher Vorschriften, führt Schulungen durch und arbeitet mit der Aufsichtsbehörde zusammen. Der Datenschutzbeauftragte muss vom Verantwortlichen (Arzt) oder dem Auftragsverarbeiter in allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Der Datenschutzbeauftragte ist weisungsfrei und berichtet unmittelbar der jeweiligen Leitungsebene. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden und ist zur Geheimhaltung verpflichtet.
Datenschutz-Folgen-abschätzung	Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten, muss der Verantwortliche (Arzt) bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen. Hierzu müssen Umfang und Zweck der Datenverarbeitung im Verhältnis zu dem Datenschutzrisiko abgewogen werden. (Beispielsweise im Zusammenhang mit dem Einsatz neuer Technologien)
DS-GVO	Datenschutz-Grundverordnung

Einwilligung	Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Beispiel: die Einwilligung des Patienten in die Übermittlung von Befunden an einen weiterbehandelnden Arzt, sofern keine Überweisung vorliegt
Empfänger	Jede Person oder andere Stelle, der personenbezogene Daten offengelegt werden. Beispiel: Patient, Krankenkassen, MDK, weiterbehandelnde Ärzte
Gesundheitsdaten	Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
Patienteninformation	Arztpraxen müssen Patienten darüber informieren, was mit ihren Daten passiert. Die Information muss in der Regel zum Zeitpunkt der Datenerhebung erfolgen. Sie muss in erster Linie die Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung enthalten sowie die Kontaktdaten der Praxis und ggf. des Datenschutzbeauftragten.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Betroffener). Beispiele: - Name - Geburtsdatum - Alter - Geburtsort - Anschrift - E-Mail-Adresse - Telefonnummer - Onlinedaten - Geschlecht - Haus-, Haar- und Augenfarbe - Gesundheitsdaten Auch Meinungen, Einschätzungen und Prognosen sind personenbezogene Daten, z. B. Angaben über - Herkunft - politische Ansichten - religiöse Ansichten - Gewerkschaftszugehörigkeit - Gesundheit einer Person - Sexualität eines Menschen
Rechenschaftspflicht	Der Verantwortliche (Arzt/Psychotherapeut) ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach der DS-GVO verantwortlich und muss dies gegenüber der Aufsichtsbehörde (TLfDI) nachweisen können. Der Nachweis muss schriftlich oder elektronisch vorliegen.
TLfDI	Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit

Impressum

Herausgeber
Kassenärztliche Vereinigung Thüringen
Zum Hospitalgraben 8
99425 Weimar

Redaktion
Ass. jur. Christin Kirschmann, Justitiariat
Ass. jur. André Müller

Gestaltung und Satz
Babette Landmann, Stabsstelle Kommunikation/Politik

Illustrationen
Olaf Schumacher

Stand
Mai 2022, 2. Auflage