kvt
Kassenärztliche
Vereinigung Thüringen

Datenschutz

Handbuch für die Mitglieder der KVT

INHALTSVERZEICHNIS

I Fragen und Antworten

1 Checkliste
2 Das Verzeichnis der Verarbeitungstätigkeiten
3 Aufstellung der technischen und organisatorischen Maßnahmen zum Datenschutz
4 Datenschutzverpflichtung – Mitarbeiter
5 Patienteninformation
6 Auftragsverarbeitung
7 Datenschutzbeauftragter in der Praxis
8 Datenschutz-Folgenabschätzung
9 Übermittlung von Daten – Einwilligung
10 Datenschutzerklärung auf der Internetseite
11 Meldungen von Datenschutzverletzungen
12 Auskunftsanspruch des Patienten
13 Fragen aus dem Praxisalltag

II Muster

1 Checkliste
2 Verarbeitungsverzeichnis
3 Technische und organisatorische Maßnahmen
4 Datenschutzverpflichtung – Mitarbeiter
5 Patienteninformation
6 Einwilligung

III Begriffsbestimmungen – Datenschutz von A bis Z

I Fragen und Antworten

1 Checkliste

Was benötigen die Arztpraxen?

Alle	• Verzeichnis der Verarbeitungstätigkeiten (tabellarisch) • Aufstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift (interner Datenschutzplan) • Patienteninformation zum Datenschutz • Vereinbarung zur Auftragsverarbeitung
große Praxen und MVZ	• Datenschutzbeauftragten
ggf.	• Datenschutz-Folgenabschätzung • Ergänzung von Einwilligungserklärungen • Anpassung von Internet- und Facebook-Seiten

2 Das Verzeichnis der Verarbeitungstätigkeiten

2.1 Was ist unter einer Verarbeitungstätigkeit zu verstehen?

Eine Verarbeitungstätigkeit stellt jeder hinreichend abstrakte Geschäftsprozess dar, dem ein eigener Zweck zugrunde liegt. Jeder neue, abgrenzbare Zweck einer Verarbeitung stellt eine Verarbeitungstätigkeit dar.

2.2 Was beinhaltet das Verarbeitungsverzeichnis und wie wird es erstellt?

In dem Verzeichnis der 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:

- **Patientenbezogene Verarbeitungstätigkeiten, zum Beispiel:**
  - » 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

2.3 Welche Angaben sind zu jeder Verarbeitungstätigkeit erforderlich?

- 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 personenbezogenen Daten offengelegt worden sind oder noch werden (z. B. Krankenkassen, Kassenärztliche Vereinigungen, MDK, Finanzamt)
- Löschung der Daten (z. B. zehn Jahre nach Abschluss der Behandlung)
- Das Verzeichnis muss außerdem den Namen und die Kontaktdaten Ihrer Arztpraxis enthalten und, soweit vorhanden, die Angaben zur Person des Datenschutzbeauftragten.
- Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

2.4 Was ist zu tun, wenn bestimmte Datenverarbeitungsvorgänge ein besonders hohes Risiko bergen?

Wenn Sie bei der Erstellung des Verarbeitungsverzeichnisses bemerken, dass die Form der Verarbeitung personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten birgt, muss vor der Verarbeitung eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchgeführt werden. Hierzu müssen Umfang und Zweck der Datenverarbeitung im Verhältnis zu dem Datenschutzrisiko abgewogen werden. Das kann beispielsweise im Zusammenhang mit dem Einsatz neuer Technologien oder auch einer systematischen Videoüberwachung der Praxisräume der Fall sein.

Wenn eine Datenschutz-Folgenabschätzung erforderlich ist, muss in der Praxis ein Datenschutzbeauftragter bestellt werden, der bei der Folgenabschätzung zu beteiligen ist. Zeigt die Datenschutz-Folgenabschätzung ein verbleibendes hohes Risiko, muss zudem die Datenschutz-Aufsichtsbehörde konsultiert werden (TlfDI).

Im Zweifelsfalle sollte der TLfDI mit einbezogen werden.

2.5 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.

2.6 Wo finde ich Muster für das Verzeichnis der Verarbeitungstätigkeit?

Unter II. 2. haben wir für sie ein Muster erstellt. Daneben finden Sie weitere Muster unter:

www.kbv.de/html/datensicherheit.php

www.tlfdi.de/tlfdi/wir/infomaterial-mustervordrucke/mustervordrucke/

www.lda.bayern.de/de/kleine-unternehmen.html

3 Aufstellung der technischen und organisatorischen Maßnahmen zum Datenschutz – Interne Regelung zur Gewährleistung des Datenschutzes –

3.1 Welchen Zweck hat die Aufstellung der Maßnahmen zum Datenschutz?

Die Arztpraxen sind für den Schutz personenbezogener Daten verantwortlich. Dafür müssen sie geeignete technische und organisatorische Maßnahmen ergreifen und diese dokumentieren. Alle Mitarbeiter der Praxis müssen die internen Regeln zur Gewährleistung des Datenschutzes kennen.

3.2 Welche Maßnahmen müssen im Einzelnen dokumentiert werden?

Eine konkrete Vorgabe, welche Maßnahmen im Einzelnen dokumentiert werden müssen, gibt es nicht. Es kommt aber insbesondere darauf an zu dokumentieren, welche technischen und organisatorischen Maßnahmen getroffen werden, damit die personenbezogenen Daten der Patienten besonders geschützt werden.

Es ist darauf zu achten, dass Patientendaten, Patientenakten, Auskünfte über oder an Patienten streng vertraulich sind und keinen anderen nicht berechtigten Personen (z. B. anderen Patienten) zur Kenntnis gelangen dürfen.

Es ist wichtig darzustellen, dass alles Mögliche getan wird, um den Schutz der Vertraulichkeit, der Integrität und Verfügbarkeit der Patientendaten zu gewährleisten.

Bei der Beurteilung der zu treffenden Maßnahmen kann es 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. Insbesondere sollten Sie auch an die Sicherheit (IT-Sicherheit) und Verfügbarkeit elektronischer Daten denken.

Dokumentiert werden sollte auch, dass die Mitarbeiter des Praxisteams zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DS-GVO verpflichtet wurden.

Ferner ist festzulegen, wie im Falle einer Datenpanne zu verfahren ist.

3.3 Gibt es ein Muster für die Dokumentation der technisch und organisatorischen Maßnahmen?

Unter II. 3 haben wir für Sie ein Muster sowie eine Erarbeitungshilfe zusammengestellt, welche Ihnen bei der Aufstellung der Maßnahmen helfen soll.

4 Datenschutzverpflichtung – Mitarbeiter

Der Arzt/Psychotherapeut bzw. Praxisinhaber muss sicherstellen, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Es ist nicht verbindlich geregelt, wie der Arzt/Psychotherapeut bzw. Praxisinhaber diese gesetzliche Verpflichtung umsetzen muss. Es wird jedoch empfohlen, dies mit einer entsprechenden Verpflichtungserklärung umzusetzen.

4.1 Wer muss verpflichtet werden?

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

4.2 Wann muss die Verpflichtung erfolgen?

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

4.3 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 Beachtung der datenschutzrechtlichen Anforderungen 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, möglichst unter Nennung von Beispielfällen.

4.4 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.

4.5 Gibt es ein Muster zur Datenschutzverpflichtung?

Ein Muster zur Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen finden Sie unter Punkt II. 4.

5 Patienteninformation

5.1 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.

5.2 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.

5.3 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.

5.4 Gibt es ein Muster für die Information der Patienten?

Sie finden ein Muster auf der Internetseite der KBV unter

www.kbv.de/html/datensicherheit.php.

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 zeigen zu lassen, welches dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten beim Auftragnehmer dient (z. B. ISO/IEC 27001).

6.6 Gibt es eine Mustervorlage für entsprechende Verträge?

Ja, eine entsprechende Formulierungshilfe finden Sie unter www.tlfdi.de/tlfdi/gesetze/europaeische-dsgvo.

7 Datenschutzbeauftragter in der Praxis

7.1 Wann muss ein Datenschutzbeauftragter bestellt werden?

Ein Datenschutzbeauftragter ist zu bestellen, wenn mindestens zehn 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.

In Ausnahmefällen kann eine Bestellpflicht auch unabhängig von der Anzahl der in der Praxis tätigen Personen bestehen. Dies ist der Fall, wenn durch den Praxisinhaber eine sogenannte Datenschutz-Folgenabschätzung (siehe Punkt 8) durchgeführt werden muss.

7.2 Wer kann zum Datenschutzbeauftragten bestellt werden?

Mit der Aufgabe des Datenschutzbeauftragten kann sowohl ein fachlich qualifizierter Mitarbeiter, welcher nicht der Praxisinhaber selbst sein darf, oder ein externer Datenschützer betraut werden. Der Name und die Kontaktdaten des Datenschutzbeauftragten müssen dem TLfDI mitgeteilt werden.

Die Person des Datenschutzbeauftragten muss die nötige Fachkunde und Zuverlässigkeit haben. Das bedeutet, dass er die gesetzlichen Regelungen kennen und sicher anwenden muss.

7.3 Welche Aufgaben hat der Datenschutzbeauftragte?

Der Datenschutzbeauftragte hat die Aufgabe, die Einhaltung des Datenschutzes und der Datensicherheit in der Praxis zu kontrollieren und geeignete Maßnahmen festzulegen. Er informiert und berät das Praxisteam über ihre Pflichten nach dem Datenschutzrecht. Darüber hinaus ist er Ansprechpartner für die Aufsichtsbehörde.

8 Datenschutz-Folgenabschätzung

8.1 Wann muss eine Datenschutz-Folgenabschätzung erfolgen?

Wenn Sie bemerken, dass eine Fom der Verarbeitung personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten birgt, muss vor der Verarbeitung eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchgeführt werden. Hierzu müssen Umfang und Zweck der Datenverarbeitung im Verhältnis zu dem Datenschutzrisiko abgewogen werden. Das kann beispielsweise im Zusammenhang mit dem Einsatz neuer Technologien oder auch einer systematischen Videoüberwachung der Praxisräume der Fall sein.

Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist und veröffentlicht diese.

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 konsultiert werden.

Im Zweifelsfalle sollte der TLfDI mit einbezogen werden. Dieser hat eine Liste veröffentlicht, für welche Formen der Verarbeitung eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist.

Diese finden Sie unter www.tlfdi.de/tlfdi/europa/europaeischedsgvo/imdx.aspx.

8.2 Was muss eine solche Datenschutz-Folgenabschätzung beinhalten?

- 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)

9 Übermittlung von Daten – Einwilligung

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

Grundsätzlich ist das Erfassen, Bearbeiten, Speichern usw. von Patientendaten in der Praxis gesetzlich gestattet, so dass es keiner gesonderten Einwilligung bedarf. Anders ist es bei der Übermittlung von Patientendaten an einen Dritten. Ist diese gesetzlich verpflichtend oder erlaubt, bedarf es keiner gesonderten Einwilligung des Patienten. Liegt eine gesetzliche Pflicht oder Befugnis zur Datenübermittlung nicht vor, ist die Einwilligung des Patienten erforderlich.

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

- Übermittlung an privatärztliche Verrechnungsstellen oder private Versicherungsgesellschaften
- Übermittlung an den Arbeitgeber oder Agentur für Arbeit
- bei einer Praxisveräußerung
- bei Teilnahme am HZV
- bei Teilnahme an DMP
- bei Teilnahme an Selektivverträgen

9.3 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 einer gesetzlicher Mitteilungspflichten, z. B. gegenüber:
  - » Unfallversicherungsträger
  - » Krankenkassen
  - » Gesundheitsämter auf der Grundlage des Infektionsschutzgesetzes
  - » Jugendämter bei Kindeswohlgefährdung
  - » Kassenärztliche Vereinigung
  - » MDK im Rahmen der gesetzlichen Krankenversicherung
  - » Übermittlung an das Labor

9.4 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 weiter 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.

9.5 Was ist bei der Einwilligungserklärung besonders zu beachten?

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

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

Eine pauschale Einwilligung in alle denkbaren Varianten der Datenweitergabe, gleichgültig an wen und zu welchem Zweck, stellt keine rechtswirksame Einwilligung dar.

Die Einwilligung des Patienten muss in jedem Falle freiwillig erfolgen.

Die Einwilligung muss erkennen lassen, wer an wen (Empfänger der Daten) in welchem Umfang personenbezogene Daten übermittelt sowie den Grund (Zweck der Verarbeitung), aus welchem die Verarbeitung notwendig ist.

9.6 Gibt es ein Muster?

Ein Muster haben wir Ihnen unter Punkt II. 6 zur Verfügung gestellt.

10 Datenschutzerklärung auf der Internetseite

Welche Angaben muss die Datenschutzerklärung auf der Internet- oder Facebook-Seite beinhalten?

Es sollte darauf hingewiesen werden, dass personenbezogene Daten ausschließlich in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht erhoben und genutzt werden.

Die Daten dürfen nur gespeichert werden, wenn sie aktiv übermittelt werden.

Die Daten dürfen zum Beispiel nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial verwendet werden.

Kontaktdaten, die im Rahmen von Anfragen angegeben werden, dürfen ausschließlich für die Korrespondenz verwendet werden.

E-Mail-Adressen, die Nutzer für den Bezug eines Newsletter angegeben haben, dürfen nur dafür genutzt werden.

Der Nutzer der Internetseite ist umfangreich über die Datenverarbeitungen, welche mit der Nutzung der Seite verbunden sind, zu informieren. Insofern empfiehlt sich eine Rücksprache mit dem jeweiligen Anbieter seiner Internetseite.

11 Meldungen von Datenschutzverletzungen

11.1 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.

11.2 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.

12 Auskunftsrecht von Patienten

12.1 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 erheblich therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Nunmehr ergibt sich dieser Anspruch auf Auskunft auch unmittelbar aus der Datenschutz-Grundverordnung. Einer Begründung des Patienten, warum er Einsicht nehmen möchte, bedarf es nicht.

12.2 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. Eine Ablehnung ist in jedem Fall gegenüber dem Patienten zu begründen.

12.3 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.

13 Fragen aus dem Praxisalltag

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

Ja, aber nur unter bestimmten Voraussetzungen. Beim Telefaxverfahren können sich Fehler bei der Anwahl des Adressaten durch einen Zahlendreher ergeben oder aber das Telefax von einer unbefugten Person beim Adressaten eingesehen werden.

Sensible Daten, wie die Gesundheitsdaten des Patienten, sollten nur unter Einhaltung zusätzlicher, datenschutzgerechter Vorkehrungen per Fax übermittelt werden. Beispielweise ist es denkbar, dass man mit dem Empfänger den Sendezeitpunkt und das Empfangsgerät abstimmt. Darüber hinaus sollten alle von den Telefaxgeräten angebotenen Sicherheitsmaßnahmen, wie die Anzeige der störungsfreien Übertragung, die gesicherte Zwischenspeicherung, der Abruf nach Passwort und Sperrung der Fernwartungsmöglichkeit genutzt werden.

13.2 Darf man die Patienten im Wartezimmer weiterhin beim Namen aufrufen?

Ja, dies ist auch weiterhin möglich. Diesbezüglich erfolgte auch eine Rücksprache mit dem TLfDI, der keinen Verstoß gegen geltende Datenschutzbestimmungen sieht, wenn Patienten mit Namen aufgerufen werden.

13.3 Wer ist die zuständige Aufsichtsbehörde 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

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

Die datenschutzrelevanten Informationen einer E-Mail bilden einerseits die Inhalte der Nachricht sowie die beigefügten Anhänge und anderseits die Adresse des Absenders sowie des Empfängers, das Datum und der Betreff der E-Mail.

Sollen über eine E-Mail Gesundheitsdaten von Patienten übermittelt werden, so ist eine Ende-zu-Ende-Verschlüsselung notwendig. Der Inhalt als auch die beigefügten Anhänge werden hierdurch chiffriert, nicht jedoch der Betreff einer E-Mail. Der Betreff einer E-Mail sollte aus diesen Gründen so neutral wie möglich formuliert werden und nicht zu viel über den Inhalt aussagen.

13.5 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 welche 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.

13.6 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 (bis zu 30 Jahren). Auch unter dem Gesichtspunkt der Rechtsverteidigung vor Ansprüchen von Patienten ist eine Aufbewahrung von personenbezogenen Daten denkbar.

13.7 Dürfen personenbezogene 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 Personen 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.

II Muster

Muster KBV: http://www.kbv.de/html/datensicherheit.php

1 Checkliste

CHECKLISTE:
DAS IST IN PUNCTO DATENSCHUTZ ZU TUN

Ab 25. Mai 2018:
Nach der neuen Datenschutz-Grundverordnung der Europäischen Union müssen Ärzte und Psychotherapeuten nicht nur die datenschutzrechtlichen Vorgaben einhalten, sondern dies auch nachweisen.

ALLE PRAXEN UND MEDIZINISCHEN VERSORGUNGSZENTREN

- Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten, die in der Praxis anfallen.
- Zusammenstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift.
- Bereitstellung einer Patienteninformation zum Datenschutz in der Praxis, zum Beispiel als Aushang in den Praxisräumen und auf der Praxis-Website.
- Verträge zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern anpassen oder neu abschließen. Solche Verträge sind notwendig, wenn Auftragnehmer auf Patienten- oder Mitarbeiterdaten zugreifen können.

GROßE PRAXEN UND MEDIZINISCHE VERSORGUNGSZENTREN

- Beauftragen eines Datenschutzbeauftragten, wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang oder bei der Abrechnung. Übernimmt ein Mitarbeiter diese Aufgabe, benötigt dieser eventuell eine Schulung.
- Melden der Kontaktdaten des Datenschutzbeauftragten der Praxis an die zuständige Aufsichtsbehörde.

DAS KANN AUßERDEM ERFORDERLICH SEIN

- In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, zum Beispiel wenn große Mengen an personenbezogenen Daten verarbeitet oder die Praxisräume systematisch videoüberwacht werden. Diese Praxen benötigen unabhängig von ihrer Größe ebenfalls einen Datenschutzbeauftragten.
- Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel zur Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen.
- Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden.

Informationen, die Ihnen bei der Erledigung der Aufgaben helfen sollen, finden Sie in der Praxisinformation der KBV „Ab 25. Mai gelten neue Vorschriften zum Datenschutz: Was Praxen jetzt wissen müssen" sowie auf der Internetseite der KBV www.kbv.de/datenschutz.

Quelle: Kassenärztliche Bundesvereinigung, März 2018

+++ MUSTER +++

kvt Kassenärztliche Vereinigung Thüringen

Verzeichnis der Verarbeitungstätigkeiten

Angaben zum Verantwortlichen: (Name und Kontaktdaten)	**Angaben zur Person des Datenschutzbeauftragten:** (ggf. soweit benannt)
Dr. Max Mustermann Straße des Datenschutzes 1 12345 Musterstadt Tel.: 0123/456789 E-Mail: praxis@mustermann.de ggf. Internet-Adresse	Anna Gewissenhaft Straße des Datenschutzes 1 12345 Musterstadt Tel.: 0123/456789-1 E-Mail: datenschutzpraxis@mustermann.de

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
1	Anlegen einer Patienten-akte	Dr. Max Mustermann 0123/456789	24.05.2018	Behandlungs-dokumen-tation	Patienten	- Personenstamm-daten - Anamnesedaten - Diagnosedaten - Befunddaten - Labordaten - Fremdbefunde	- Mitarbeiter Arztpraxis - Vor-, Mit- und Nachbehandler - Krankenkassen - MDK - Pflegeeinrich-tungen - Krankenhäuser - Unfallversicher-ungsträger - Rentenver-sicherungsträger - Gerichte - Angehöriger - Erben - Versicherungen	Nein	frühestens 10 Jahre nach Abschluss der Behandlung (gesetzliche Aufbe-wahrungsfrist) ggf. Aufbe-wahrung bis zu 30 Jahren (Röntgenbe-handlung, Strahlenbe-handlung, Auf-zeichnungen gem. Trans-plantations-gesetz)

+++ MUSTER +++

kvt
Kassenärztliche
Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
2	Erhebung von Patientendaten zur Behandlung des Patienten unter Einsatz und Nutzung PVS	Dr. Max Mustermann 0123/456789	24.05.2018	Untersuchung / Diagnostik	Patienten	- Personenstammdaten - Versichertennummer - Anamnesedaten - Diagnosedaten - Labordaten - Fremdbefunde	- Vor-, Mit- und Nachbehandler - Mitarbeiter Arztpraxis - Apotheken und Hilfsmittellieferanten - Physio- oder Ergotherapeuten - Pflegeeinrichtungen - Krankenkasse - MDK - Rentenversicherungsträger - Unfallversicherungsträger	Nein	frühestens 10 Jahre nach Abschluss der Behandlung (gesetzliche Aufbewahrungsfrist) ggf. ist eine Aufbewahrung bis zu 30 Jahren erforderlich oder gesetzlich vorgeschrieben
3	Übermittlung von Patientendaten zur Abrechnung der erbrachten Leistungen für gesetzlich Krankenversicherte	Dr. Max Mustermann 0123/456789	24.05.2018	Abrechnung GKV-Versicherte	Patienten	- Personenstammdaten - Versichertennummer - Diagnosedaten - Behandlungszeitpunkt - Behandlungsdaten - Befunddaten	- Mitarbeiter Arztpraxis - Kassenärztliche Vereinigung Thüringen - DMP-Datenstelle - Krankenkasse	Nein	10 Jahre nach Wirksamwerden des zugehörigen Jahreseinkommenssteuerbescheides der Praxis

+++ MUSTER +++

kvt Kassenärztliche Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
4	Übermittlung von Patientendaten zur Abrechnung der erbrachten Leistungen gegenüber Privatpatienten und Individuelle Gesundheitsleistungen	Dr. Max Mustermann 0123/456789	24.05.2018	Abrechnung Privatpatienten und Individuelle Gesundheitsleistungen	Patienten	- Personenstammdaten - Versichertennummer - Diagnosedaten - Behandlungsdaten - Befunddaten - Behandlungszeitpunkt	- Mitarbeiter Arztpraxis - Privatärztliche Verrechnungsstellen	Nein	10 Jahre nach Wirksamwerden des zugehörigen Jahreseinkommenssteuerbescheides der Praxis
5	Bestellbuch/Terminvergabe	Dr. Max Mustermann 0123/456789	24.05.2018	Koordination des Praxisablaufs	Patienten	- Name - Telefonnummer	- Mitarbeiter Arztpraxis	Nein	4 Jahre nach Ablauf des Kalenderjahres
6	Online Terminvergabe	Dr. Max Mustermann 0123/456789	24.05.2018	Koordination des Praxisablaufs	Patienten	- Name - Telefonnummer - E-Mail Adresse	- Mitarbeiter Arztpraxis - (ggf. eingesetzter Dienstleister)	Nein	4 Jahre nach Ablauf des Kalenderjahres
7	Verarbeitung von Patientendaten mittels Langzeit-EKG	Dr. Max Mustermann 0123/456789	24.05.2018	Untersuchung /Diagnostik	Patienten	- Diagnosedaten	- Mitarbeiter Arztpraxis - Vor-, Mit- und Nachbehandler	Nein	10 Jahre (§ 57 Abs. 2 BMV-Ä)

+++ MUSTER +++

kvt
Kassenärztliche
Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
8	Verarbeitung von Patientendaten mittels Ultraschallgerät	Dr. Max Mustermann 0123/456789	24.05.2018	Untersuchung /Diagnostik	Patienten	- Diagnosedaten	- Mitarbeiter Arztpraxis - Vor-, Mit- und Nachbehandler	Nein	frühestens 10 Jahre nach Abschluss der Behandlung (gesetzliche Aufbewahrungsfrist) ggf. ist eine Aufbewahrung bis zu 30 Jahren erforderlich oder gesetzlich vorgeschrieben
9	Führen eins Laborbuches	Dr. Max Mustermann 0123/456789	24.05.2018	Diagnostik	Patienten	- Identifikationsnummer	- Mitarbeiter Arztpraxis	Nein	10 Jahre (§ 57 Abs. 2 BMV-Ä)
10	Erstellung eines ärztlichen Gutachtens	Dr. Max Mustermann 0123/456789	24.05.2018	Bewertung des Gesundheitszustandes	Patienten	- Personenstammdaten - Diagnosedaten - Behandlungsdaten - Befunddaten - Behandlungszeitpunkt	- Mitarbeiter Arztpraxis - MDK - Versicherungen - Berufsgenossenschaften - Gerichte	Nein	10 Jahre (§ 57 Abs. 2 BMV-Ä)

+++ MUSTER +++

kvt Kassenärztliche Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
11	Ausstellen einer Heilmittelverordnung	Dr. Max Mustermann 0123/456789	24.05.2018	Therapie	Patienten	- Personenstammdaten - Diagnosedaten - Befunddaten - Versichertennummer	- Mitarbeiter Arztpraxis - Apotheken und Hilfsmittellieferanten - Physio- oder Ergotherapeuten - Pflegeeinrichtungen - Krankenkasse	Nein	10 Jahre (§ 57 Abs. 2 BMV-Ä), sofern die Heilmittelverordnung die alleinige Dokumentation ist: frühestens 10 Jahre nach Abschluss der Behandlung (gesetzliche Aufbewahrungsfrist)
12	Ausstellen einer Arbeitsunfähigkeitsbescheinigung	Dr. Max Mustermann 0123/456789	24.05.2018		Patienten	- Personenstammdaten - Diagnosedaten - Versichertennummer	- Mitarbeiter Arztpraxis - Krankenkasse - Arbeitgeber	Nein	1 Jahr (Anlage 2 BMV-Ä Muster 1 Vorbemerkung) bzw. frühestens nach 10 Jahren, wenn die Arbeitsunfähigkeitsbescheinigung alleinig der Dokumentation dient

+++ MUSTER +++

kvt Kassenärztliche Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
13	Datensicherung (Back-Up-Verfahren)	Dr. Max Mustermann 0123/456789	24.05.2018	Gewährleistung der Verfügbarkeit	Patienten	- Personenstammdaten - Anamnesedaten - Diagnosedaten - Labordaten - Fremdbefunde - versicherten-nummer	- Mitarbeiter Arztpraxis	Nein	frühestens 10 Jahre nach Abschluss der Behandlung (gesetzliche Aufbewahrungsfrist) ggf. ist eine Aufbewahrung bis zu 30 Jahren erforderlich oder gesetzlich vorgeschrieben
14	Datenvernichtung	Dr. Max Mustermann 0123/456789	24.05.2018	Vernichtung von personenbezogen Daten	- Patienten - Mitarbeiter - Bewerber	- Personenstammdaten - Anamnesedaten - Diagnosedaten - Labordaten - Fremdbefunde - Bewerbungsunterlagen	- Mitarbeiter Arztpraxis - (ggf. Dienstleister zur Entsorgung)	Nein	–
15	Lohnabrechnung Personal	Dr. Max Mustermann 0123/456789	24.05.2018	Lohnzahlung der Mitarbeiter	- Mitarbeiter	- Personenstammdaten - Sozialversicherungsdaten - Lohnmerkmale	- Buchhalter - Steuerberater - Sozialversicherungsträger - Finanzamt	Nein	10 Jahre nach Wirksamwerden des zugehörigen Jahreseinkommenssteuerbescheides der Praxis

+++ MUSTER +++

kvt Kassenärztliche Vereinigung Thüringen

Lfd. Nr.	Benennung der Verarbeitungstätigkeit	Verantwortlicher Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorien betroffener Personen	Kategorien von persönlichen Daten	Kategorien von Empfängern	Transfer Drittland	Löschung von Daten
16	Personalverwaltung	Dr. Max Mustermann 0123/456789	24.05.2018	Verwaltung der laufenden Arbeits-verträge	- Mitarbeiter	- Personenstamm-daten - Bewerbungsunter-lagen - Qualifikationen - Zeugnisse - Sozialver-sicherungsdaten - Lohnmerkmale	--	Nein	3 Jahre nach Beendigung des Arbeits-vertrages
17	Bewerbermanagement	Dr. Max Mustermann 0123/456789	24.05.2018	Rekrutierung neuer Mitarbeiter	- Bewerber	- Personenstamm-daten - Bewerbungsunter-lagen - Qualifikationen - Zeugnisse	- Mitarbeiter Arztpraxis	Nein	6 Monate nach Beendigung des Bewerbungs-verfahrens

3 Technische und organisatorische Maßnahmen in der Arztpraxis

HINWEIS:
Dieses Muster wählt eine mögliche Art und Weise der Dokumentation zu den in einer Arztpraxis ergriffenen technischen und organisatorischen Maßnahmen. Der Aufbau ist dabei nicht zwingend in dieser Form gesetzlich vorgeschrieben, sodass auch jede andere Darstellungsweise möglich ist. Bei der Verwendung dieses Musters ist darauf zu achten, dass dieses jeweils an die Gegebenheiten in der eigenen Arztpraxis angepasst werden muss. Die dargestellten Maßnahmen sind nicht abschließend und jeweils als Beispiele für die einzelnen Kategorien aufgeführt.

Dieses Dokument dient dazu die technischen und organisatorischen Maßnahmen, welche in der Arztpraxis ergriffen werden, zu dokumentieren. Dies betrifft Maßnahmen, welche die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten gewährleisten.

1) Maßnahmen, welche die Vertraulichkeit gewährleisten

a. Zutrittskontrolle

Maßnahmen, welche verhindern, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen haben.

- Schlüsselverwaltung/Dokumentation Schlüsselvergabe
- Alarmanlage

b. Zugangskontrolle

Maßnahmen, welche verhindern,dass Unbefugte Zugang zu Datenverarbeitungssystemen haben.

- persönlicher und individueller User-Log-In bei Anmeldung am System (eigene Benutzerkennung)
- Firewall
- Nutzung von automatisch, kennwortgeschützten Bildschirmsperren
- Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechten auf Betriebssystemadministration

c. Zugriffskontrolle

Maßnahmen, welche verhindern, dass Unbefugte Zugriff auf personenbezogene Daten haben.

- Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechte
- Abschluss von Verträgen zur Auftragsverarbeitung (Pflege, Wartung, Fernwartung von Datenverarbeitungsanlagen)
- Verschlüsselung von externen Datenträgern (externe Festplatten, Laptops, CD/DVD)

2) Maßnahmen, welche die Integrität gewährleisten

a. Weitergabekontrolle

Maßnahmen zur Sicherstellung, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Getunnelte Datenfernverbindung (VPN = Virtuelles Privates Netzwerk)
- Protokollierung von Datentransporten (Back-up)
- Regelung zum Umgang mit mobilen Speichermedien (z. B. Laptop, USB-Stick, Mobiltelefon)
- Gesicherter Datentransport (z. B. SSL)
- Verschlüsselung von Laptop

b. Eingabekontrolle

Maßnahmen zur Prüfung, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- Zugriffsrechte/Rollenverteilung
- Organisatorisch festgelegte Zuständigkeiten
- Mehraugenprinzip

3) Maßnahmen, welche die Verfügbarkeit und Belastbarkeit gewährleisten

Maßnahmen, welche sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und stets verfügbar sind.

- Back-up-Verfahren
- Virenschutz
- Firewall
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)

Erarbeitungshilfe „technischer und organisatorischer Maßnahmen“

EINGANG-ZUTRITTSKONTROLLE

- Wer hat Praxisschlüssel?
- Schließ- und 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).

4 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)

Quelle: KVT, Justitiariat, 2018

5 Muster zur Patienteninformation

PATIENTENINFORMATION ZUM DATENSCHUTZ

MUSTER FÜR IHRE PRAXIS

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutz-Grundverordnung (DSGVO) 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):

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.

der Behandlung aufzubewahren. Nach anderen Vorschriften können sich längere Aufbewahrungsfristen ergeben, zum Beispiel 30 Jahre bei Röntgenaufzeichnungen laut Paragraf 28 Absatz 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) DSGVO in Verbindung mit Paragraf 22 Absatz 1 Nr. 1 lit. b) Bundesdatenschutzgesetz. Sollten Sie Fragen haben, können Sie sich gern an uns wenden.

Ihr Praxisteam

Quelle: KBV / Patienteninformation zum Datenschutz: Muster / März 2018

6 Muster Einwilligung

Patienteneinwilligung in die Datenverarbeitung
gem. § 73 Abs. 1b SGB V

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 angefordert 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)

Quelle: KVT, Justitiariat, 2018

III Begriffsbestimmungen – Datenschutz von A - 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

E-Mail: poststelle@datenschutz.thueringen.de
Telefon: 0361 57311-2900
Telefax: 0361 57311-2904

Auftragsverarbeitung

Auftragsverarbeitung ist die Verarbeitung 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 (z. B. erhoben, gespeichert oder übermittelt) werden.

Beispiel:
Informationspflicht, Auskunftsrecht, Löschung, Berichtigung

Datenschutz-beauftragter	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-Folgenabschätzung	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.
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

Verantwortlicher Verantwortlicher ist derjenige, der über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten entscheidet, z. B. Arzt/Psychotherapeut.

Verarbeitungstätigkeit Eine Verarbeitungstätigkeit stellt jeder hinreichend abstrakte Geschäftsprozess dar, dem ein eigener Zweck zugrunde liegt. Jeder neue abgrenzbare Zweck einer Verarbeitung stellt eine Verarbeitungstätigkeit dar. Beispiel: die Verarbeitung von Patientendaten zur Behandlung der Patienten, Dokumentation der ärztlichen Behandlung, Abrechnung erbrachter Leistungen

Verarbeitungsverzeichnis Das Verzeichnis von Verarbeitungstätigkeiten enthält alle Verarbeitungstätigkeiten bzw. Vorgänge, bei denen in der Arztpraxis personenbezogene Daten verarbeitet werden.

Jeder Tätigkeit müssen hinzugefügt werden:

- Zweck der Verarbeitung
- betroffene Personengruppen
- Datenkategorien
- Empfängergruppen
- Fristen für die Löschung

NOTIZEN

Impressum

Herausgeber

Kassenärztliche Vereinigung Thüringen
Zum Hospitalgraben 8
99425 Weimar

www.kvt.de

Redaktion

Ass. jur. Christin Kirschmann, Justitiariat
Ass. jur. Agnes Ehrismann-Maywald, Justitiariat

Satz/Layout

Babette Landmann, Stabsstelle Kommunikation/Politik

Illustration

Olaf Schumacher

Stand

März 2019