[ANMERKUNG: Wir empfehlen, zur Durchführung der Datenschutz-Folgeabschätzung die Konsultation Ihres Datenschutzbeauftragten]

DATENSCHUTZ-FOLGENABSCHÄTZUNG
für
Patientenverwaltung und Honorarabrechnung[1]

des

[…(ANMERKUNG: Bitte den Namen des Arztes oder der Ordination angeben)]

(im Folgenden kurz: der Verantwortliche)

1. Beschreibung der Datenverarbeitung

1.1. Einleitung

Das Datenschutzgesetz bestimmt, dass der Verantwortliche zum Schutz der Rechte und berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener eine Datenschutz-Folgenabschätzung gemäß Art 35 Datenschutzgrundverordnung (DSGVO) durchzuführen hat. Dies hat dann zu geschehen, wenn die Form der Verarbeitung (insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung) voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Der Verantwortliche erstellt hiermit eine Datenschutz-Folgenabschätzung für die Datenverarbeitung „***Patientenverwaltung und Honorarabrechnung***“ (dies umfasst die im Verzeichnis der Verarbeitungstätigkeiten genannten Datenanwendungen: Patientenakte, Abrechnung (sowohl Krankenkasse / Privat), Befundanforderung / Befundübermittlung, Untersuchung von Proben, Organisation von Konsilien, Verwaltung von Rezepten und Hausapotheke) in: **[… (ANMERKUNG: Bitte die Bezeichnung der Ordination angeben)]** (zur besseren Lesbarkeit im Folgenden kurz: **Ordination**).

1.2. Beschreibung: Patientenverwaltung und Honorarabrechnung

Patientenverwaltung und Honorarabrechnung beim Verantwortlichen umfasst die Abwicklung und Organisation der Behandlung, Führung von Patientenkarteien zur Dokumentation gemäß § 51 ÄrzteG 1998, Untersuchung und Versand von Proben, Organisation von Konsilien, Verwaltung von Rezepten, Hausapotheke (Betrieb, Verwaltung, Abrechnung und Organisation der Hausapotheke), die Erstellung von medizinischen Gutachten und Honorarverrechnung, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

---

[1] Sollten Sie weitere Datenanwendungen betreiben, die eine Datenschutz-Folgeabschätzung benötigen, müssen Sie diese gesondert durchführen.

(ANMERKUNG: Bitte unzutreffende Punkte streichen).

Gemäß § 2 ÄrzteG 1998 umfasst der Beruf des Arztes die Ausübung des ärztlichen Berufes jede auf medizinisch-wissenschaftlichen Erkenntnissen begründete Tätigkeit, die unmittelbar am Menschen oder mittelbar für den Menschen ausgeführt wird, insbesondere

1. die Untersuchung auf das Vorliegen oder Nichtvorliegen von körperlichen und psychischen Krankheiten oder Störungen, von Behinderungen oder Missbildungen und Anomalien, die krankhafter Natur sind;
2. die Beurteilung von in Z 1 angeführten Zuständen bei Verwendung medizinisch-diagnostischer Hilfsmittel;
3. die Behandlung solcher Zustände (Z 1);
4. die Vornahme operativer Eingriffe einschließlich der Entnahme oder Infusion von Blut;
5. die Vorbeugung von Erkrankungen;
6. die Geburtshilfe sowie die Anwendung von Maßnahmen der medizinischen Fortpflanzungshilfe;

6a. die Schmerztherapie und Palliativmedizin;

7. die Verordnung von Heilmitteln, Heilbehelfen und medizinisch diagnostischen Hilfsmitteln;
8. die Vornahme von Leichenöffnungen.

Darüber hinaus ist jeder zur selbständigen Ausübung des Berufes berechtigte Arzt befugt, ärztliche Zeugnisse auszustellen und ärztliche Gutachten zu erstatten.

Gemäß § 49 ÄrzteG 1998 ist ein Arzt verpflichtet, jeden von ihm in ärztliche Beratung oder Behandlung übernommenen Gesunden und Kranken ohne Unterschied der Person gewissenhaft zu betreuen. Eine umfassende und gewissenhafte Betreuung verlangt auch die Verarbeitung von personenbezogenen Daten.

Gemäß § 51 ÄrzteG 1998 ist der Arzt verpflichtet, Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person, insbesondere über den Zustand der Person bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten und der zur Identifizierung dieser Arzneispezialitäten und der jeweiligen Chargen im Sinne des § 26 Abs 8 des Arzneimittelgesetzes, BGBl. Nr. 185/1983, erforderlichen Daten zu führen.

Ärzte sind zur automationsunterstützten Verarbeitung genannter personenbezogener Daten sowie zur Übermittlung dieser Daten an die Sozialversicherungsträger und Krankenfürsorgeanstalten in dem Umfang, als er für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, sowie an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke

steht, mit Einwilligung des Kranken berechtigt.

Gemäß Art. 9 Abs. 2 lit h ist die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich.

1.3. Verarbeitete Daten

Im Rahmen der ärztlichen Versorgung werden von den Patienten folgende personenbezogene Daten (zur besseren Lesbarkeit im Folgenden kurz: „Daten“) – unterteilt in Kategorien von betroffenen Personen – erhoben:

1.3.1. Patienten

- Name
- Anschrift
- Geburtsdatum/Geburtsort
- SVNR
- Patientennummer
- Sozialversicherungsträger
- Art des Arbeitsverhältnisses, Arbeitgeberinformation
- Daten zu einem privaten Versicherungsverhältnis (Versicherer, Polizzennummer usw.)
- Daten sonstiger Kostenträger
- Datum der Untersuchung
- Name des Behandlers/Betreuers aus dem Team des Verantwortlichen
- Daten zur Verwaltung von Terminen und Wartelisten
- Medizinischer Zustand der Person bei Übernahme der Beratung oder Behandlung
- Besondere Risikofaktoren, z.B. Allergien, tätigkeitsbedingte Einflüsse, familiäre Disposition, ausgeübte Tätigkeit
- Daten zu Impfungen
- Vorgeschichte der Erkrankung und dazugehörige Befunde
- Zusätzliche Daten zu meldepflichtigen Krankheiten (Inhalt der vorgeschriebenen Meldeformulare)

- Angaben zur ärztlichen Untersuchung (Familien- und Eigenanamnese; Berufsanamnese auf Grundlage der tatsächlichen Arbeitsvorgänge und -bedingungen; allgemeine klinische Untersuchung; Laboruntersuchungen; weitere Teiluntersuchungen)
- Diagnosen (auch Fremddiagnosen) zu Behandlungsbeginn und bei Beendigung
- Gutachtliche Äußerungen des Auftraggebers (z.B. gegenüber Arbeitgeber)
- Gesundheitliche Beurteilung (Ergebnis der ärztlichen Untersuchung/Kontrolluntersuchung), Zeugnisse im Sinne des § 36 AllgStrSchV
- Krankheitsverlauf
- Information an Patienten
- Daten zur Zuweisung oder Zweitbefundung an Fachärzte, Labors usw.
- Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen
- Daten zur Anwendung von Arzneispezialitäten und zur Identifizierung dieser Arzneispezialitäten und der jeweiligen Chargen im Sinne des § 26 Abs 8 des Arzneimittelgesetzes, BGBl. Nr. 185/1983
- Verschreibung und Abgabe von Arzneimitteln, Heilbehelfen und Hilfsmitteln
- Daten zur Abrechnung der Gebühren oder Entgelte für Sachverständigen- und Gutachtertätigkeit
- Daten zur Abrechnung von Honoraren, Medikamenten und Laboruntersuchungen
- Zustimmung des Betroffenen zur Teilnahme an Gesundheitspilotprojekten, strukturierten Gesundheitsversorgungsprogrammen (z.B. Disease Management Programmen) und Vorsorge- und Früherkennungsprogrammen (z.B. Nationales Brustkrebsfrüherkennungsprogramm)
- Name und Erreichbarkeit von gewählten, gerichtlich bestellten oder gesetzlichen Vertretern.

[ANMERKUNG: Bitte allfällige weitere Kategorien von Daten anführen bzw. nicht-zutreffende Kategorien streichen]

1.3.2. **Mitarbeiter**

Von den Mitarbeitern des Verantwortlichen werden im Rahmen der Verarbeitung der Patientendaten und der Honorarabrechnung ebenfalls Daten verarbeitet, jedoch keine besondere Kategorie personenbezogener Daten. Daher hat die Verarbeitung für die Datenschutz-Folgenabschätzung keine Relevanz, weshalb darauf nicht genauer eingegangen wird.

1.4. Schritte und Akteure der Verarbeitung

1.4.1. Terminvereinbarung:

Der Verantwortliche verarbeitet die Daten im Rahmen der Terminvereinbarung wie folgt:

[ANMERKUNG: Bitte beschreiben Sie stichwortartig den Ablauf der Datenverarbeitung: Wie und wo werden die Daten erhoben/verarbeitet, wie werden die Daten gespeichert (physisch/elektronisch), welche Personen sind in die Datenverarbeitung involviert usw.]

1.4.2. Patientenadministration

Der Verantwortliche verarbeitet die Daten im Rahmen der der Patientenadministration wie folgt:

[ANMERKUNG: Bitte beschreiben Sie stichwortartig den Ablauf der Datenverarbeitung: Wie und wo werden die Daten verarbeitet, wie werden die Daten gespeichert (physisch/elektronisch), welche Personen sind in die Datenverarbeitung involviert usw.]

1.4.3. Patientendokumentation

Der Verantwortliche verarbeitet die Daten im Rahmen der Patientendokumentation wie folgt:

[ANMERKUNG: Bitte beschreiben Sie stichwortartig den Ablauf der Datenverarbeitung: Wie und wo werden die Daten erhoben/verarbeitet, wie werden die Daten gespeichert (physisch/elektronisch), welche Personen sind in die Datenverarbeitung involviert usw.

Beispiel:

„Die Behandlung wird entweder in der Ordination durchgeführt oder im Rahmen eines Hausbesuches vor Ort beim Patienten. Im Rahmen der ärztlichen Behandlung kommt es aufgrund der notwendigen ärztlichen Versorgung

- ***zur Untersuchung von Proben,***
- ***zur Erstellung des Befundberichts,***
- ***zur Ausstellung eines Rezepts,***
- ***zur Erstellung einer Verordnung bzw. Zuweisung,***
- ***zur Erstellung eines Gutachtens oder eines ärztlichen Zeugnisses,***
- ***zur Kommunikation mit vor- oder nachbehandeln Ärzten oder Gesundheitsdienstleistern;***

Der Arzt dokumentiert die Behandlung des Patienten gemäß Art 51 ÄrzteG 1998.“]

1.4.4. **Hausapotheke**

Der Verantwortliche verarbeitet die Daten im Rahmen der Verwaltung der Hausapotheke wie folgt:

[ANMERKUNG: Bitte beschreiben Sie stichwortartig den Ablauf der Datenverarbeitung: Wie und wo werden die Daten erhoben/verarbeitet, wie werden die Daten gespeichert (physisch/elektronisch), welche Personen sind in die Datenverarbeitung involviert usw.]

1.4.5. **Honorarabrechnung**

Der Verantwortliche verarbeitet die Daten im Rahmen der Honorarabrechnung wie folgt:

[ANMERKUNG: Bitte beschreiben Sie den Ablauf der Datenverarbeitung: Wie und wo werden die Daten verarbeitet, wie werden die Daten gespeichert (physisch/elektronisch), welche Personen sind in die Datenverarbeitung involviert usw.]

1.4.6. **Datenspeicherung & Datensicherung**

Der Verantwortliche speichert die Daten auf folgenden Servern:

[ANMERKUNG: Bitte ergänzen Sie den Ort an dem Ihr Server steht, sollten Sie einen Dienstleister für die Datenspeicherung und/oder Datensicherung in Anspruch genommen haben, ergänzen Sie bitten dessen Namen und Adresse.]

1.4.7. **Auftragsverarbeiter**

Der Verantwortliche setzt die in dem vom Verantwortlichen geführten Verzeichnis der Verarbeitungstätigkeiten genannten Auftragsverarbeiter ein.

1.4.8. **Datenübermittlung**

Der Verantwortliche übermittelt personenbezogene Daten an die im vom Verantwortlichen geführten Verzeichnis der Verarbeitungstätigkeiten genannten Empfänger.

1.4.9. **Vernichtung**

Der Verantwortliche vernichtet die Daten sobald diese für die Zwecke, für die er sie erhoben hat, nicht mehr notwendig sind wie folgt:

[ANMERKUNG: Bitte ergänzen Sie stichwortartig, wie von Ihnen die Daten vernichtet werden (etwa ob die Daten elektronisch oder physisch gelöscht werden).]

1.5. Zweck der Verarbeitung

Der Verantwortliche verarbeitet die Daten für den Zweck der Erfüllung der in Punkt 1.2 genannten berufsrechtlichen Verpflichtungen im Rahmen der „Patientenverwaltung

und Honorarabrechnung“ sowie zur Erfüllung vertraglicher Verpflichtungen (Behandlungsvertrag) bzw. Pflichten aus dem Vertragsverhältnis mit Sozialversicherungsträgern (gesamtvertragliche Vereinbarungen).

Dies umfasst die Organisation (Terminvereinbarung und Patientenadministration) und Abwicklung der Behandlung (Untersuchung von Proben, Erstellung des Befundberichts, Ausstellung von Rezepten und Verwaltung der Hausapotheke, Erstellung einer Überweisung bzw. Zuweisung, Erstellung eines Gutachtens oder eines ärztlichen Zeugnisses, Kommunikation mit vor- oder nachbehandeln Ärzten oder Gesundheitsdienstleistern) sowie zur weiteren Kostenabrechnung mit den dem jeweiligen Kostenträger verarbeitet. Die Abrechnung erfolgt entweder gegenüber dem Patienten selbst oder gegenüber einem Sozialversicherungsträger, einer privaten Versicherung.

Darüber hinaus werden die Daten zur Erfüllung gesetzlicher Dokumentationspflichten verarbeitet.

1.6. Interesse an der Erhebung

Gemäß § 49 ÄrzteG 1998 ist ein Arzt verpflichtet, jeden von ihm in ärztliche Beratung oder Behandlung übernommenen Gesunden und Kranken ohne Unterschied der Person gewissenhaft zu betreuen. Eine umfassende und gewissenhafte Betreuung verlangt auch die Verarbeitung von personenbezogenen Daten.

Das Interesse des Verantwortlichen an der Erhebung und Verarbeitung der personenbezogenen Daten ergibt sich insbesondere aus der gesetzlichen Pflicht zur Verarbeitung gemäß § 51 ÄrzteG 1998 „Dokumentationspflicht und Auskunftserteilung“ sowie aus dem Behandlungsvertrag, etwaigen gesamtvertraglichen Vereinbarungen sowie weiteren gesetzlichen Grundlagen (etwa Epidemiegesetz) im Gesundheitswesen.

1.7. Speicherdauer

Gemäß § 51 Abs 3 ÄrzteG 1998 sind Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person **mindestens** zehn Jahre aufzubewahren. Konkret werden die Aufzeichnungen für 30 Jahre nach Leistungserbringung aufbewahrt, da der Verantwortliche bis zum Ablauf der langen Verjährungsfrist gemäß § 1489 ABGB mit Schadenersatzansprüchen von Betroffenen konfrontiert werden kann. Der Grund für diese Speicherdauer ist die Verteidigung von Schadenersatzansprüchen, welche sich aus der Leistungserbringung ergeben. Darüber hinaus können Gesundheitsdaten für den Betroffenen oder die Hinterbliebenen in einem Zeitraum von 30 Jahren von Relevanz sein, sodass die lange Speicherdauer auch dem Interesse der Betroffenen dient.

2. Rechtmäßigkeit der Verarbeitung

2.1. Rechtsgrundlagen

Nachfolgend werden die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert.

Artikel 9 DSGVO
Die Verarbeitung besonders Kategorien personenbezogener Daten, den Gesundheitsdaten, im konkreten Fall die Patientendaten, ist untersagt, jedoch kennt der Artikel 9 DSGVO folgende Ausnahme:

Art 9 Abs 2 lit h: Gesundheitsvorsorge
Im Erwägungsgrund 53 zur DSGVO wird erläutert, dass die gesundheitsbezogene Verarbeitung besondere Kategorien personenbezogener Daten zulässig sein soll, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist. Die Verwaltung im Dienst des Gesundheits- und Sozialbereichs sowie die Überwachung der Gesundheit durch Gesundheitsbehörden, die auf national oder Unionsrecht beruht wird explizit erwähnt. Das trifft auch auf die Verwendung zwecks Abrechnung mit den Kostenträgern der Behandlung zu.

Das für die Verarbeitung zuständige Personal hat gem. Art 9 Abs 3 DSGVO ein dem Berufsgeheimnis unterliegendes Fachpersonal zu sein oder einer anderen gesetzlichen Geheimhaltungspflicht zu unterliegen. Bei Ärzten und deren Gehilfen ist dies gemäß § 54 ÄrzteG 1998 der Fall.

Gemäß § 49 ÄrzteG 1998 ist ein Arzt verpflichtet, jeden von ihm in ärztliche Beratung oder Behandlung übernommenen Gesunden und Kranken ohne Unterschied der Person gewissenhaft zu betreuen. Im Rahmen dieser Betreuung sind Ärzte gemäß § 51 ÄrzteG 1998 zur Dokumentation der Diagnose und Behandlung verpflichtet.

Die Rechtmäßigkeit einer Übermittlung ergibt sich darüber hinaus auch aus einer Reihe von Gesetzen (Epidemiegesetz, Tuberkolosegesetz, AIDS-Gesetz, Geschlechtskrankheitengesetz), die der Verhütung und Bekämpfung von übertragbaren Krankheiten in Österreich dienen und eine Meldepflicht bei Verdacht oder Diagnose vorsehen.

2.2. Notwendigkeit und Verhältnismäßigkeit

Notwendig ist die Verarbeitung von persönlichen Daten dann, wenn derselbe Zweck nicht mit anderen, weniger invasiven Mitteln erreicht werden kann. Die Speicherung und Ablage der Daten ist der einzige Weg um die Dokumentationspflicht gemäß Art 51 ÄrzteG 1998 und in weiterer Folge die Abrechnung zu ermöglichen, ein gelinderes Mittel zur Erreichung des gesetzlich normierten Zwecks steht nicht zur Verfügung.

Bei der Beurteilung der Verhältnismäßigkeit ist der Datenverarbeitungsprozess in seiner konkreten Ausgestaltung dem Zweck, den der Verantwortliche verfolgt, gegenüberzustellen und abzuwägen. Je umfassender und intensiver die Datenverarbeitung ist, desto hochrangiger hat der Zweck zu sein.

Bei Gesundheitsdaten handelt es sich um besondere Kategorien von Daten und damit besonders schützenswerte personenbezogene Daten. Die datenschutzrechtlichen Regeln sehen vor, dass die betroffenen Personen das Recht haben sollen, selbst zu entscheiden, welche personenbezogenen Daten über sie verarbeitet werden. Die Verarbeitung des Verantwortlichen berühren dieses Recht. Die Rechte der betroffenen Person kollidieren im konkreten Fall mit der gesetzlichen Verpflichtung zur Dokumentation

des Verantwortlichen.

Die Verhältnismäßigkeit der beschriebenen Verarbeitung ergibt sich aus dem hohen Wert des zu schützenden Gutes, nämlich des Lebens und der Gesundheit der betroffenen Personen sowie der öffentlichen Gesundheit und Sicherheit.

Die Rechte der betroffenen Personen werden nur in dem Ausmaß beeinträchtigt, wie es zur Zweckerreichung unbedingt notwendig ist. Es werden ausschließlich jene Daten verarbeitet, die im konkreten Fall für die Gesundheit des Betroffenen relevant sind oder zur Erfüllung gesetzlicher Pflichten erforderlich sind. Eine andere Möglichkeit, die Dokumentation durchzuführen, besteht nicht.

Übermittelt der Verantwortliche ausnahmsweise die Daten an einen Dritten handelt sich bei den Empfängern jeweils um Angehörige von Gesundheitsberufen oder Behörden, welche ihrerseits einer strengen Verschwiegenheitspflicht unterliegen und zur Durchführung von Datenschutz-Folgeabschätzungen verpflichtet sind.

Sowohl der Verantwortliche als auch die Empfänger der übermittelten Daten haben technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes der besonderen Kategorien von Daten gemäß Artikel 32 DSGVO ergriffen (siehe Punkte 3.1.2. und 3.1.3).

2.3. Datenminimierung

Gemäß Art 5 Abs 1 lit c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sein, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt. Es werden im konkreten Fall daher nur jene personenbezogenen Daten erhoben, die für eine Weiterbehandlung oder zur Abrechnung oder zur gesetzlich normierten Erfüllung von Aufgaben durch andere Behörden notwendig sind.

2.4. Speicherbegrenzung

Gemäß § 51 Abs 3 ÄrzteG 1998 muss der Verantwortliche personenbezogene Daten mindestens 10 Jahr aufheben. Der hier Verantwortliche speichert Daten für 30 Jahre, da der Verantwortliche bis zum Ablauf der langen Verjährungsfrist gemäß § 1489 ABGB mit Schadenersatzansprüchen von Betroffenen konfrontiert werden kann. Die Speicherung dient zur Abwehr rechtlicher Ansprüche.

2.5. Maßnahmen im Sinne der Rechte der Betroffenen

Die DSGVO räumt den Betroffenen zahlreiche Rechte ein. Eine der zentralen Betroffenenrechte ist das Recht auf Information gemäß Art 15 DSGVO. Der Verarbeiter hat dem Betroffenen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Der Verantwortliche hat genaue Schritte definiert, wie im Fall einer solchen Anfrage bzw. Aufforderung vorzugehen ist. Es liegt ein diesbezügliches Handbuch für die Mitarbeiter in der Ordination vor bzw. wurden die zuständigen Mitarbeiter geschult, um den gesetzlichen Rechten der Betroffenen zu entsprechen.

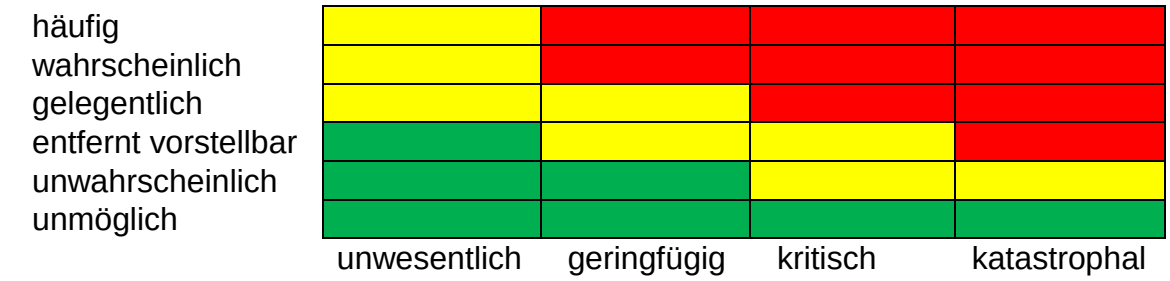
Der Verantwortliche hat organisatorische Maßnahmen ergriffen, um die Rechte der Betroffenen fristgerecht und gemäß den gesetzlichen Bestimmungen umzusetzen.

3. Risiken

Die Risiken werden anhand ihrer Eintrittswahrscheinlichkeit und des potentiellen Schadensausmaßes bewertet.

Eintrittswahrscheinlichkeit x Schadensausmaß = Risiko

Dies lässt sich mit einer Risikomatrix darstellen:



Im Ergebnis bedeutet das:

akzeptabler Bereich, vernachlässigbares Risiko
Maßnahme zur Risikoreduktion werden gesetzt
inakzeptabler Bereich, das Risiko wird vermieden

3.1. Risikoidentifikation

[ANMERKUNG: Im Folgenden beschreiben Sie bitte mögliche Szenarien, die ein Risiko für Patientendaten bedeuten können. Gleichzeitig müssen Sie die von Ihnen getroffenen Maßnahmen zur Risikoreduktion beschreiben.

Beispiel:

Unbefugte Offenlegung von Patientendaten (etwa durch Falschkuvertierung von Briefen).

Ergriffene Maßnahme zur Reduktion des Risikos: Schulung von Mitarbeiter (Vier-Augen-Prinzip), regelmäßige Aufsicht durch den Arzt usw.

Abhängig vom erwarteten Risiko (siehe Punkt 3) und von den von Ihnen getroffenen Maßnahmen, ergänzen Sie bitte beim jeweiligen Szenario in den untenstehenden Tabellen in der mittleren Spalte einen der folgenden Textbausteine:

- ***akzeptabler Bereich, vernachlässigbares Risiko oder***
- ***Maßnahme zur Risikoreduktion werden gesetzt oder***
- ***inakzeptabler Bereich, das Risiko wird vermieden.***

In der rechten Spalte ergänzen Sie bitte die dazugehörige Farbauswahl, grün für akzeptabel, gelb für Maßnahme zur Risikoreduktion werden gesetzt oder rot für

inakzeptablen Bereich. Wenn Sie zum Ergebnis kommen, dass die Verarbeitung inakzeptabel ist, dürfen Sie die Datenverarbeitung nicht durchführen.

Im Folgenden haben wir bereits für Sie typische Risiken identifiziert und beschrieben.]

3.1.1. **Rechtliche Risiken**

Änderung der Gesetzeslage

Bewertung des Risikos:	***akzeptabler Bereich***	

Eine Änderung der datenschutzrechtlichen Gesetzeslage, die die Verarbeitung besonderer Kategorien personenbezogener Daten betrifft, ist durchaus möglich. Dies geschieht jedoch mit höchster Wahrscheinlichkeit mit einer Übergangsfrist, so dass, wenn nötig, genug Zeit besteht, die Datenschutz-Folgenabschätzung zu aktualisieren.

3.1.2. **Organisatorische Risiken**

Unbefugte Offenlegung von Patientendaten durch Mitarbeiter oder den Verantwortlichen selbst.

Bewertung des Risikos:	***[ANMERKUNG: vermutlich handelt es sich hierbei – abhängig von den getroffenen Maßnahmen – um ein mittleres Risiko]*** **Maßnahmen zur Risikoreduktion werden gesetzt**	

Der Verantwortliche hat folgende Maßnahmen zur Risikoreduktion getroffen:

[ANMERKUNG: Im Folgenden müssen Sie die von Ihnen getroffenen Maßnahmen zur Risikoreduktion beschreiben.]

Beispiel:

Ärzte unterliegen einer gesetzlichen Verschwiegenheitspflicht. Ordinationsassistenzen, Angehörige eines nicht-ärztlichen Gesundheitsberufs oder Lehrpraktikanten verarbeiten Daten nur unter der Verantwortung eines Arztes und unterliegen einer vertraglichen sowie gesetzlichen (§ 6 DSG) Verschwiegenheitspflicht. Darüber hinaus müssen diese einen Kurs besucht haben, in dem sie auch im angemessenen Umgang mit den Gesundheitsdaten geschult wurden. Sollte es zu einer ungewollten Veröffentlichung kommen, wird der Betroffene informiert. Alle Mitarbeiter werden regelmäßig über den Datenschutz geschult und

sensibilisiert. Um Falschkuvertieren von Briefen bei der Versendung von Befunden zu verhindern, hat der Verantwortliche einen Freigabeprozess (Vier-Augen-Prinzip) integriert. Die Einhaltung der gesetzlichen Datenschutzvorschriften wird vom jeweils zuständigen Vorgesetzen kontrolliert.

3.1.3. **Technische Risiken**

Datenzugriff durch unbefugte Personen

Bewertung des Risikos:	***[ANMERKUNG: Qualifikation des Risikos ergänzen]***	

Der Verantwortliche hat folgende Sicherheitsvorkehrungen zur Risikoreduktion getroffen:

[ANMERKUNG: Im Folgenden müssen Sie die von Ihnen getroffenen Maßnahmen zur Risikoreduktion beschreiben. Wir empfehlen Ihnen die technischen Risiken mit Ihrem IT-Dienstleister abzuklären.]

Ausfall der IT Infrastruktur

Bewertung des Risikos:	***[ANMERKUNG: Qualifikation des Risikos ergänzen]***	

Der Verantwortliche hat folgende Sicherheitsvorkehrungen zur Risikoreduktion getroffen:

[ANMERKUNG: Im Folgenden müssen Sie die von Ihnen getroffenen Maßnahmen zur Risikoreduktion beschreiben. Wir empfehlen Ihnen die technischen Risiken mit Ihrem IT-Dienstleister abzuklären.]

3.1.4. **Externe Risiken**

Hackangriff

Bewertung des Risikos:	***[ANMERKUNG: Qualifikation des Risikos ergänzen]***	

Der Verantwortliche hat folgende Sicherheitsvorkehrungen zur Risikoreduktion getroffen:

[ANMERKUNG: Im Folgenden müssen Sie die von Ihnen getroffenen Maßnah-

men zur Risikoreduktion beschreiben. Wir empfehlen Ihnen die technischen Risiken mit Ihrem IT-Dienstleister abzuklären.]

Datenschutzverletzung durch Dritte

Bewertung des Risikos:	***[ANMERKUNG: Qualifikation des Risikos ergänzen]***	

Der Verantwortliche hat folgende Sicherheitsvorkehrungen zur Risikoreduktion getroffen:

[ANMERKUNG: Im Folgenden müssen Sie die von Ihnen getroffenen Maßnahmen zur Risikoreduktion beschreiben. Wir empfehlen Ihnen die technischen Risiken mit Ihrem IT-Dienstleister abzuklären.]

3.2. Zur Risikovermeidung

Eine Risikovermeidung wird dadurch erreicht, dass lediglich jene Daten verarbeitet und übermittelt werden, die zur Erfüllung der gesetzlichen Verpflichtung des Verantwortlichen unmittelbar erforderlich sind und hinsichtlich derer die Verhältnismäßigkeit gewahrt ist.

4. Abschließende Beurteilung

[ANMERKUNG: Wenn Sie auf Basis Ihrer Überlegung zum Schluss kommen, dass im Rahmen Ihrer Ordination kein hohes Risiko für die Rechte und Freiheiten der Betroffenen im Rahmen der Patientenverwaltung und Honorarabrechnung besteht, beschreiben Sie in einem kurzen Statement, wie Sie zu dieser Einschätzung gekommen sind.]