



Agenda

- Auskunftsrecht hat Anspruch auf Mitarbeiter-Liste
- Schadenersatz wegen verspäteter Auskunft nach 19 Tagen
- Daten ohne Personendaten noch schützenswert?
- Künstliche Intelligenz - Rechtsgrundlagen
- Einwilligung
- Einwilligung bei Internet-Diensten
- e-Patientenakte Widerspruch, worauf kommt es an?

Inhalt

1. Praxisvorfall Auskunftsrecht	2
2. Schadenersatz wegen verspäteter Auskunft nach 19 Tagen.....	4
3. Sind Daten ohne Personenstammdaten noch schützenswert?	6
3.1. Mögliche Rechtsgrundlagen für den Einsatz von KI	7
4. Künstliche Intelligenz	8
4.1. DIHVA: Ein Projekt nimmt Fahrt auf.....	8
4.2. KI im gastroenterologisch-internistischen Arztbereich	8
4.3. KI für Hausarzt-Anwendungen.....	8
4.4. KI für Diabetes-Behandlungen.....	9
4.5. KI in der Radiologie	9
4.6. KI in der Psychiatrie	9
5. Einwilligung.....	10
5.1. Form der Einwilligung	10
5.2. Inhalt	10
• Klare Formulargestaltung	10
• Konkretheit.....	10
• Informiertheit	10
• Widerrufbarkeit	10
• Freiwilligkeit	10
5.3. Weitergabe	11
6. Einwilligungs-Beispiele:.....	11
7. Widerrufbarkeit der ePa	12
• Kann ein Patient dem "eRezept" widersprechen?	12
• Kann ein Patient der "eAU" widersprechen?.....	12
• Kann ein Patient bei einer Befundübermittlung mit "eArztbrief" widersprechen?.....	12
• Wie ist der aktuelle Status der „eÜberweisung“?.....	13
• Kann ein Patient der "ePatientenakte" widersprechen und die Auswirkung auf eRezept, eAU, eArztbrief ...	13
• Gibt es bestimmte Kriterien, die ein Patient erfüllen muss, um gegen die ePA Einspruch einlegen zu können?.....	13
• Muss der Einspruch schriftlich sein?	13
• Bis wann kann ich die elektronische Patientenakte ablehnen?	13
Anlage1: Musterschreiben, Ablehnung elektronische Patienten-Akte.....	15
Anlage 2: Inhalt einer Mitarbeiterliste im Rahmen eines Auskunftsanspruchs.	16
Anlage 3: Laufzettel	17
Anlage 3: Notfallkarte	18

1. Praxisvorfall Auskunftsrecht

Die Auskunftspflicht ist gesetzlich normiert.

Die Rechtsgrundlagen ist das MBO, das BGB, das BDSG sowie die DSGVO.

1. Musterberufsordnung (MBO)

Das Berufsrecht der Ärzte (MBO) ist Teil des Standesrechts, das von den Berufsständen selbst verwaltet wird. Es können spezifischen Repressalien von Verwarnung, Disziplinarmaßnahmen, Sperre der Berufsausübung, Rechtliche Schritte oder Öffentliche Erwähnung ausgesprochen werden.

Auskunftsrecht § 10 Abs. 2 MBO. Der Arzt ist verpflichtet, seinen Patienten Einsicht in die objektiven Teile der Krankenunterlagen zu gewähren und seine Patienten schnellstmöglich die komplette Originalakte einsehen zu lassen, Kopien anzufertigen oder eine Auskunft über einzelne Abschnitte der Akte zu gewähren, je nachdem, was der Patient verlangt. Der Patient hat jedoch kein Recht auf die Aushändigung des Originals. Eine Ausnahme bilden Röntgenbilder (§ 28 Abs. 8 Röntgenverordnung), die zur Weiterbehandlung notwendig sind.

2. BGB

Das Bürgerliche Gesetzbuch (BGB) ist die Hauptquelle des deutschen Zivilrechts und umfasst die Regelungen zum Privatrecht, einschließlich des Sachen-, Schuld-, Familien-, Erbrechts und des Gesellschaftsrechts. Repressalien können sein, Geldstrafen, Verweisstrafen, Verbote und Berufsausübungs-Verbot.

Auskunftsrecht § 630g BGB: Der Patient hat einen einklagbaren Rechtsanspruch auf Einsicht in und Auskunft aus sämtlichen ihm betreffenden Krankenakten, ohne dass dies vor der Behandlung vereinbart werden muss. Der Rechtsanspruch gilt auch nach Abschluss der Behandlung. Der Patient kann zugleich die Anfertigung von Kopien verlangen. Eine Ablehnung der Einsichtnahme ist nur zulässig, wenn ein Verweigerungsgrund im Sinne von § 630g Abs. 1 Satz 1 BGB vorliegt, wie zum Beispiel erhebliche Persönlichkeitsrechte Dritter oder aus therapeutischen Gründen eine Einsichtnahme für den Betroffenen zu einer erheblichen Gesundheitsgefahr führen würde.

3. BDSG

Das Bundesdatenschutzgesetz (BDSG) ist ein deutsches Gesetz, das die Regelungen zum Datenschutz in Deutschland umfasst. Es ergänzt die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union und regelt die Verarbeitung personenbezogener Daten in Deutschland.

Bei Verstößen gegen das BDSG und die DSGVO können verschiedene Sanktionen verhängt werden, die sich nach der Art und Schwere des Verstoßes richten. Mögliche Sanktionen sind:

Bußgelder bis 300.000,- Schadensersatz für betroffene Personen, Anordnungen Verstöße zu beheben, z.B. die Löschung von personenbezogenen Daten oder die Umsetzung von technischen und organisatorischen Maßnahmen, vorübergehende oder dauerhafte Einschränkung der Datenverarbeitung, Strafrechtliche Verfolgung, wie Geldstrafen oder Freiheitsstrafen.

Auskunftsrecht § 19 BDSG der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten in Deutschland, ob überhaupt Daten (evtl. Negativauskunft) verarbeitet werden und welche Informationen zu diesen Daten verarbeitet werden, einschließlich deren Zweck, die Kategorien der betroffenen Personen, der geplanten Speicherung oder der anderen Verarbeitung sowie der geplanten Übertragung der Daten an Dritte oder an Drittländer außerhalb der Europäischen Union.

4. DSGVO

Die Datenschutz-Grundverordnung (DSGVO) verhält sich zum nationalen Recht, insbesondere zum Bundesdatenschutzgesetz (BDSG), als Verordnung unmittelbar und geht als europäisches Recht dem nationalen Recht vor. Sie enthält jedoch in verschiedenen Konstellationen sogenannte Öffnungs- oder Spezifizierungsklauseln. Diese erlauben es den Mitgliedstaaten, für die in diesen Klauseln genannten Fälle eigene Regelungen zu erlassen, die z.B. eigene Rechtsgrundlagen für eine Datenverarbeitung schaffen können, eigene Bereiche selbständig (unter Einhaltung wesentlicher Aspekte der DSGVO) zu regeln, oder Regelungen der DSGVO zu spezifizieren. Das BDSG bleibt insoweit insbesondere für den Bereich der öffentlichen Verwaltung relevant; es enthält aber auch allgemein anwendbare Normen wie etwa den § 26 BDSG, der den Beschäftigtendatenschutz regelt. Zur Beurteilung datenschutzrechtlicher Fragestellungen sind somit die Datenschutz-Grundverordnung und die Regelungen im Allgemeinen sowie gegebenenfalls

auch im bereichsspezifischen nationalen Datenschutzrecht (sei es im Landes- oder Bundesrecht) im Zusammenhang zu lesen und anzuwenden.

Repressalien können Bußgelder bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes des Unternehmens umfassen.

Praxisvorfall Auskunftrecht

• Gesetzliche Grundlage -> MBO -> BGB -> BDSG -> DSGVO

1. Berufsrecht § 10 Abs. 2, Repressalien -> Verwarnung, Disziplinarverfahren, Rechtsschritte
2. BGB § 630g, Repressalien -> Geldstrafen, Verweisstrafen, Verbote und Berufsausübung-Verbot
3. BDSG § 19, Repressalien -> Bußgelder bis 300.000, Schadensersatz, Löschung von Daten, Umsetzung von technischen und organisatorischen Maßnahmen, vorübergehende oder dauerhafte Einschränkung der Datenverarbeitung, Strafrechtliche Verfolgung, Geldstrafen, 2-jährige Freiheitsstrafe
4. DSGVO Artikel 15, Repressalien -> Bußgelder bis zu 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr

• Was ist passiert?

1. Bearbeitung unter BGB-Aspekt   Rechtsanwältin
2. Fristsetzung der Beantwortung 
3. Bestätigung der Richtigkeit  
4. Verlangen nach komplette Behandlungsunterlagen, incl. Liste der Behandlungsbeteiligten/Mitarbeiter 

• Mitarbeiter-Liste

Gemäß § 10 Abs. 1 MBO besteht Aufzeichnungs-Pflicht zu getroffenen Maßnahmen.  ist ein Mitarbeiter im Rahmen eines Auskunftsanspruchs?

• To Do

Überprüfen: Können alle Behandlungen und Anwendungen einem Mitarbeiter zugeordnet werden?

Auskunftsrecht Artikel 15 DSGVO der betroffenen EU-Bürger hat ein Recht auf Auskunft über seine personenbezogenen Daten und auf folgende Informationen:

- Verarbeitungszwecke;
- Daten Kategorien;
- Empfänger, gegenüber denen die personenbezogenen welche Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder

bei internationalen Organisationen; geplante Speicherdauer, die Kriterien für die Festlegung dieser Dauer;

- Grund der Datenweitergabe, Beschreibung deren Teilaufgabe;
- alle verfügbaren Informationen über die Herkunft der Daten, wenn sie von anderer Stelle herkamen;
- (Besteht eine automatisierte Entscheidungsfindung einschließlich Profilerstellung gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.)

5. Was ist passiert?

Ein Patient bittet um eine Datenauskunft mit vier zu erfüllenden Punkten:

- a) Die Auskunft soll gemäß § 630 BGB erteilt werden.
 - b) Für die Erledigung wird eine Frist von 14 Tagen gesetzt.
 - c) Neben der Patientenakte wird eine Liste der an der Behandlung beteiligten Mitarbeiter verlangt.
 - d) Abschließend wird eine ausdrückliche Bestätigung verlangt, dass alle gemachten Angaben richtig und vollständig sind.
- e)

zu a) Bearbeitung gemäß § 630 BGB

Bei der Auskunft-Beantwortung haben wir 2 Möglichkeiten. Nach DSGVO oder BGB. Das Ziel der DSGVO ist eine völlig transparente Darstellung der Datenflüsse aufzuzeigen. Das Ziel der BGB-Auskunft hingegen ist lediglich der Inhalt der Patienten-Akte. Egal woher die Daten kamen und wohin die Daten abgefließen sind.

zu b) Fristsetzung der Beantwortung

Die Frage nach einer Fristsetzung von zwei Wochen bei der Beantwortung eines Auskunftsersuchens nach § 630g BGB könnte sich auf die Interpretation von "unverzüglich" beziehen. In der Praxis könnte dies bedeuten, dass eine Auskunft innerhalb einer angemessenen Frist erteilt werden muss, die jedoch nicht explizit im Gesetzestext festgelegt ist. Die Rechtsprechung und die Anwendung des § 630g BGB in verschiedenen Fällen könnten Hinweise darauf geben, wie "unverzüglich" zu interpretieren ist.

zu c). komplette Behandlungsunterlagen

Patientenakte

Liste der Behandlungsbeteiligten

zu d) Bestätigung der Richtigkeit

Der Arzt ist nicht verpflichtet, eine ausdrückliche Bestätigung über die Vollständigkeit und Richtigkeit der übersandten Unterlagen zu liefern.

Begründung: Der Patient kann die Unterlagen selbst überprüfen, um sicherzustellen, dass sie vollständig und korrekt sind. Sollte jedoch der Patient feststellen, dass die Unterlagen nicht vollständig, oder nicht korrekt sind, könnte dies als vorsätzliche Falsch-Auskunft gewertet werden.

Mitarbeiter-Liste (siehe Anlage 2)

Gemäß § 10 Abs. 1 Musterberufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä 1997) hat der Arzt die erforderlichen Aufzeichnungen über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen zu machen. Diese Regelung impliziert, dass auch Delegationsentscheidungen, die als Feststellungen oder Maßnahmen im Sinne des Arztes gewertet werden können, schriftlich dokumentiert werden müssen. Die schriftliche Dokumentation ist für die zeitgerechte Dokumentation der Delegation einer ärztlichen Aufgabe auf das medizinische Fachpersonal in erster Linie der delegierende Arzt verantwortlich. Siehe Muster-Vorschlag.

ToDo

Prüfen Sie in der Software, ob alle Delegationen automatisch oder nur manuell einer Behandlung und Anwendung des Personals zugeordnet werden können? Auch ausgeschiedene Mitarbeiter müssen reidentifizierbar und benennbar sein.

2. Schadenersatz wegen verspäteter Auskunft nach 19 Tagen

Schadenersatz wegen „verspäteter“ Auskunft nach 19 Tagen

- **Schon wieder ein Urteil zum Auskunftsanspruch**
- **Was ist passiert?**
- **Verletzung des Gebots der Unverzüglichkeit**
 - Keine besondere Komplexität
 - Temporärer Kontrollverlust als Schaden
- **Die vermeintliche Monatsfrist beim Recht auf Auskunft**
 - Monatsfrist nur noch für komplexe Fälle?
- **Bedeutung des Urteils für den Auskunftsanspruch**

Schon wieder ein Urteil zum Auskunftsanspruch

Das wohl relevanteste Betroffenenrecht ist auch wieder Gegenstand eines Urteils des Arbeitsgerichts Duisburg vom 03. November 2023 (Az. 5 Ca 877/23). Im Fokus steht dieses Mal allerdings nicht der Umfang des Anspruchs, sondern die Frist zur Beantwortung durch den Verantwortlichen. Trotz Beauskunftungen innerhalb von 19 Tagen nach Antragseingang sprach das Arbeitsgericht dem Betroffenen einen Schadenersatzanspruch wegen verspäteter Auskunftserteilung zu.

Was war passiert?

Der Sachverhalt, der dem Urteil zu Grunde liegt, ist nicht außergewöhnlich: Der Betroffene bewarb sich am 14.03.2017 auf eine Stellenanzeige bei einem Inkassodienstleister und sandte diesem hierzu seine Bewerbungsunterlagen zu.

Am 18.05.2023 – sechs Jahre später – beehrte der Betroffene schließlich Auskunft darüber, ob und welche Daten zu seiner Person durch den Verantwortlichen noch verarbeitet werden. In seiner E-Mail setzte der Kläger außerdem eine Frist zur Auskunftserteilung bis zum 02.06.2023.

Der verantwortliche Inkassodienstleister reagierte hierauf zunächst nicht, weshalb der Betroffene einen Tag nach Ablauf seiner eigens gesetzten Frist, am 03.06.2023 erneut an sein Auskunftsbegehren erinnerte. Dieses Mal mit Erfolg: Der Verantwortliche erteilte dem Betroffenen am 05.06.2023 eine Negativauskunft: „Daten des Betroffenen wurden zu diesem Zeitpunkt nicht mehr verarbeitet.“

Der Betroffene wandte sich daraufhin erneut an den Verantwortlichen und bat um Stellungnahme, weshalb die Negativauskunft nicht innerhalb seiner eigens gesetzten Frist erteilt wurde. Ganz zum Empören des Verantwortlichen, der nämlich davon ausging, er habe mit Blick auf Art. 12 DSGVO die Auskunft fristgerecht innerhalb eines Monats erteilt.

Verletzung des Gebots der Unverzüglichkeit

Obwohl der Verantwortliche innerhalb von 19 Kalendertagen dem Auskunftsverlangen des Betroffenen nachkam, zog dieser vor Gericht – (teilweise) mit Erfolg:

Das Arbeitsgericht vertritt in seinem Urteil die Auffassung, der Verantwortliche habe mit der zögerlichen Beantwortung des Auskunftsanspruchs gegen das Gebot der Unverzüglichkeit aus Art. 12 Abs. 3 DSGVO verstoßen und sprach dem Betroffenen aufgrund der verspäteten Auskunft schließlich einen Schadenersatzanspruch nach Art. 82 Abs. 1 DSGVO in Höhe von 750 Euro zu.

Die Vorgabe des Art. 12 Abs. 3 DSGVO enthalte die Pflicht des Verantwortlichen zur unverzüglichen Unterrichtung, unabhängig davon, ob es sich um eine Negativ- oder Positivauskunft handele. Bei der in Art. 12 Abs. 3 S. 1 DSGVO genannten Monatsfrist handelt es sich um eine Höchstfrist, die „nicht routinemäßig, sondern nur in schwierigeren Fällen ausgeschöpft werden dürfe“.

„Unverzüglich“ sei in Anlehnung zu § 121 BGB als „ohne schuldhaftes Zögern“ zu verstehen. Ein sofortiges Handeln oder eine starre Zeitvorgabe sei dem Begriff der Unverzüglichkeit zwar nicht zu entnehmen. Für

die Entscheidung, wann einem Verantwortlichen ein solches „schuldhaftes Zögern“ vorgeworfen werden könne, müssten daher die jeweiligen Interessen der Beteiligten abgewogen werden.

Das Gericht zitiert hierbei das Urteil des BAG vom 27.02.2020 (Az.: 2 AZR 390/19), in welchem zur Auslegung der Legaldefinition von „Unverzüglich“ entschieden wurde, dass zumindest *„Nach einer Zeitspanne von mehr als einer Woche (...) ohne das Vorliegen besonderer Umstände grundsätzlich keine Unverzüglichkeit mehr gegeben ist.“*

Etwaige Umstände, die eine längere Bearbeitungszeit des Verantwortlichen rechtfertigen würden, seien im vorliegenden Fall für das Gericht nicht ersichtlich gewesen. Auch der Umstand, dass dem Verantwortlichen zwischen Antragsstellung und Erteilung der Auskunft aufgrund von Feier- und Brückentagen zur Beantwortung nur insgesamt 9 Werktage zur Verfügung stand, fand keine Berücksichtigung.

Keine besondere Komplexität

Das Gericht stellte darauf ab, dass der Negativauskunft des Verantwortlichen keine besondere Komplexität innewohnte. Ein etwaig aufwändiges Sichten oder Zusammenstellen von Daten, wie sie bei einer Positivauskunft anfallen würden, entfielen für den Verantwortlichen im vorliegenden Fall. Es seien keine Anhaltspunkte ersichtlich, weshalb für einen einfachen Suchvorgang mehr als eine Woche benötigt wurde.

Nicht zu berücksichtigen sei außerdem, dass es sich um eine sechs Jahre alte Bewerbung des Betroffenen handelte, die aus subjektiver Sicht des Verantwortlichen möglicherweise deshalb nicht so dringend sein könne, wie bspw. „aktuellere“ Auskunftsanfragen anderer Betroffener. Art. 12 DSGVO setze schließlich keine objektive Dringlichkeit des geltend gemachten Betroffenenrechts voraus.

Temporärer Kontrollverlust als Schaden

Durch den Verstoß des Verantwortlichen gegen das in Art. 12 Abs. 3 S. 1 DSGVO verankerte Beschleunigungsgebot sei dem Betroffenen schließlich auch ein immaterieller Schaden entstanden, den er nach Art. 82 Abs. 1 DSGVO vom Verantwortlichen ersetzt verlangen kann.

Durch die nach Auffassung des Gerichts verspätete Auskunft habe der Betroffene immerhin einen temporären Kontrollverlust bezüglich seiner personenbezogenen Daten erlitten – auch wenn der Verantwortliche zu diesem Zeitpunkt wohlgemerkt keine solchen Daten des Betroffenen mehr verarbeitet:

„Durch die verspätete Auskunft war der Kläger im Ungewissen und ihm die weitere Prüfung verwehrt, ob und ggf. wie die Beklagte seine personenbezogenen Daten verarbeitet.“

Die vermeintliche Monatsfrist beim Recht auf Auskunft

Ohne näher auf den Schaden eingehen zu wollen, der darin liegen soll, dass der Betroffene einen temporären Kontrollverlust über seine personenbezogenen Daten erlitten habe, (wo doch gar keine Daten durch den Verantwortlichen verarbeitet wurden), stieß das Urteil bereits im Netz auf vermehrte Kritik. Oftmals liest sich, der Verantwortliche habe doch die Monatsfrist eingehalten.

In der Tat hält sich vielfach die Vorstellung, es genüge, wenn man grundsätzlich bei jedem beliebigen Auskunftersuchen die einmonatige Frist zur Beantwortung nach Art. 12 Abs. 3 DSGVO einhält. Diese allgegenwärtige Annahme entspricht so aber nicht dem Wortlaut und der Systematik des Art. 12 Abs. 3 S. 1 DSGVO:

„Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung.“

Anders, als in Abs. 3 S. 3 wird die Monatsfrist in Abs. 3 S. 1 als einzuhaltendes Höchstmaß genutzt, um die Rechte des Betroffenen nicht einer ungewissen Zeitkomponente zu unterwerfen, die im Ermessen des Verantwortlichen liegt. Auch Erwägungsgrund 59 S. 3 betont, dass die Beantwortung unverzüglich erfolgen *solle*, spätestens aber innerhalb eines Monats zu erfolgen hat.

Die Ausschöpfung der Monatsfrist stellt demnach bereits dem Wortlaut und der Systematik der Norm nach einer Ausnahme dar, die – wie das Arbeitsgericht betonte – richtigerweise nicht routinemäßig und ohne Anlass ausgereizt werden darf.

Monatsfrist nur noch für komplexe Fälle?

Der Verantwortliche hat somit geeignete Maßnahmen zu treffen, um der Verpflichtung zur unverzüglichen Auskunft nachzukommen. Er sollte in der Lage sein, die eingehenden Anfragen beschleunigt und damit grundsätzlich **unverzüglich** beantworten zu können. Doch die Annahme, die in Art. 12 Abs. 3 S. 1 DSGVO genannte Höchstfrist von einem Monat sei nur noch schwierigen Fällen vorbehalten, dürfte sich in der Praxis wohl kaum durchsetzen.

Zum einen wird es schwierig sein eine klare Linie zu ziehen, bis wann welche Auskünfte zu erteilen sind, um die Unverzüglichkeit nach Auffassung des Arbeitsgerichts zu bedienen. Erfahrungsgemäß dürfte zwar eine Negativauskunft mit weniger Aufwand verbunden sein als die Erteilung einer vollumfänglichen Positivauskunft. Doch welchen Umfang müssen Positivauskünfte erreichen, um die Ausschöpfung der Monatsfrist nach Auffassung des ArbG Duisburgs zu rechtfertigen?

Zum anderen ist es fraglich, inwiefern die Fristverlängerung nach Art. 12 Abs. 3 S. 2 DSGVO dann überhaupt noch von Bedeutung wäre. Denn hiernach kann die – wohlgerneht nur für schwierige Fälle auszuschöpfende – Monatsfrist nach Art. 12 Abs. 3 S. 1 DSGVO um weitere zwei Monate verlängert werden,

wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

Bedeutung des Urteils für den Auskunftsanspruch

Die Bedeutung des Urteils für den Auskunftsanspruch ist schwer auszumachen, insbesondere deshalb, weil der Verantwortliche (Beklagte) scheinbar an vielen Stellen seiner Darlegungslast nicht nachkam.

Selbstverständlich sollte die Monatsfrist zur Beantwortung von Auskunftsansprüchen nicht routinemäßig ausgeschöpft werden. Gerade dann, wenn es sich um einfache Fälle handelt, wie bspw. Negativauskünfte, die keine besondere Such- und Recherchearbeit verlangen. Doch die Ausführungen und Anforderungen im Urteil gehen deutlich zu weit und entfernen sich von der umsetzbaren Realität in den wohl meisten unternehmerischen Strukturen.

Erkenntnis:

Generell ist bei jeder Geltendmachung von Rechten (Auskunft, Löschung, Berichtigung etc.) der Datenschutzbeauftragte ist direkt zu informieren. Außerdem ist ihm der ausgefüllte "Datenschutz-Laufzettel" (siehe Anlage 3) zu übermitteln, das den Vorgang dokumentiert. Der Datenschutz-beauftragte legt daraufhin mit der Praxis die Frist für die Beantwortung fest. Die Praxis informiert den Betroffenen die Komplexität des Vorgangs und wann er mit einer Antwort/Erledigung rechnen kann.

3. Sind Daten ohne Personenstammdaten noch schützenswert?

Sind Daten ohne Personenstammdaten noch schützenswert?

- Anonymisierung und Pseudonymisierung
- Art.9 DSGVO: Gesundheits-Daten unterliegen den Datenschutzbestimmungen auch ohne Personenbezug!
- Gibt es Ausnahmen
- Ist das Einverständnis der betroffenen Personen nötig, auch wenn die Daten anonymisiert sind?
- Mögliche Rechtsgrundlagen für den Einsatz von KI nach DSGVO
 - Einwilligung, Art. 6 Abs. 1 lit. a
 - Erfüllung eines Vertrages, Art. 6 Abs. 1 lit. b
 - Erfüllung einer gesetzlichen Verpflichtung, Art. 6 Abs.1 lit. c
 - Schutz lebenswichtiger Interessen, Art. 6 Abs. 1 lit. d
 - ~~Berechtigter-Eigen-Interesse Art. 6 Abs. 1 lit. f~~

Bußgeld

800.000 Euro wegen datenschutzrechtlichen Verstoßes.
Das Unternehmen verwendet nicht anonymisierte Gesundheitsdaten, die im Rahmen der Nutzung seiner Softwareprogramme erhoben wurden, ohne Genehmigung für Studien und Statistiken genutzt

5/11 ▶

Wenn die Daten keinen Personenbezug mehr haben. Die Daten stehen für sich allein. Wenn also die Daten von den Personendaten getrennt sind, spricht man von anonymisierten oder pseudonymisierten Daten.

Der Unterschied zwischen Anonymisierung und Pseudonymisierung besteht darin, dass bei der Anonymisierung der Personenbezug vollständig gelöscht wird, während bei der Pseudonymisierung der Personenbezug durch ein Kennzeichen, ein sogenanntes Pseudonym, z.B. eine

Patientennummer erhalten bleibt, um bei Rechercheursuchen den Patienten wieder aufzufinden, um dessen Rechte nachzukommen.

Große Frage bei der Erstellung von Studien, große Frage beim Training künstlicher Intelligenz, wo nur die Daten der Untersuchungsergebnisse oder des Krankheitsverlaufs benötigt werden, die zugehörigen Personenstammdaten sind irrelevant.

Gibt es Ausnahmen oder spezielle Bedingungen, unter denen die Verarbeitung von Gesundheitsdaten ohne Personenbezug erlaubt sein könnte?

JA, wenn Gesundheitsdaten ohne Personenbezug für wissenschaftliche, historische, statistische oder Archivzwecke verarbeitet werden, könnte eine solche Verarbeitung zulässig sein. Die Grundsätze der DSGVO, insbesondere die Grundsätze der Transparenz, der Rechenschaftspflicht, der Zugänglichkeit und der Speicherbegrenzung, müssen jedoch eingehalten werden.

Es ist wichtig zu beachten, dass diese Ausnahmen und Bedingungen nicht dazu führen dürfen, dass die rechtlichen Anforderungen der DSGVO umgangen werden.

Ist das Einverständnis der betroffenen Personen nötig, auch wenn die Daten anonymisiert sind?

Ja, laut Artikel 6 der Datenschutz-Grundverordnung (DSGVO) kann die Verarbeitung personenbezogener Daten nur erfolgen, wenn eine der in der DSGVO genannten Rechtsgrundlagen vorliegt. Dazu gehören beispielsweise die Zustimmung des Betroffenen (Art. 6 Abs. 1 a DSGVO). Das bedeutet, dass auch wenn die Daten anonymisiert sind, ist das Einverständnis der betroffenen Personen erforderlich.

Dabei bleiben die Rechte der betroffenen Personen gewahrt. Gemäß Artikel 15 der DSGVO haben betroffene Personen das Recht, Auskunft über die von ihnen verarbeiteten personenbezogenen Daten zu erhalten, diese unverzüglich berichtigen zu lassen, wenn sie unrichtig sind, oder ihre Löschung zu verlangen. Wenn Daten anonymisiert werden, ist es aber für den Datenverarbeiter problematisch, die anonymisierten Daten wieder einer Person zuzuordnen. Daher wird häufig die schwächere Form der Verschlüsselung, die Pseudonymisierung, mit zusätzlich notwendigen höheren Sicherheitsanforderungen verwendet.

3.1. Mögliche Rechtsgrundlagen für den Einsatz von KI

1. Einwilligung aus Art. 6 Abs. 1 lit. a DSGVO weist die Datenschutzaufsichtsbehörde darauf hin, dass die datenschutzkonforme Einholung bei komplexen KI-Systemen erschwert werden könnte, wenn diese aufgrund ihrer Komplexität intransparent und auch für Fachleute nicht mehr eindeutig nachvollziehbar werden. Auch die Widerruflichkeit der erteilten Einwilligung stelle die Verantwortlichen vor Probleme, wenn sie sich für diese Rechtsgrundlage entscheiden, da dann die betroffenen Daten nur mit unverhältnismäßig hohem Aufwand separiert werden können. Insgesamt ein eher schwieriges Thema.

2. Erfüllung eines Vertrages, Art. 6 Abs. 1 lit. b DSGVO: Einsatz von KI-Systemen innerhalb der medizinischen Behandlung zur Diagnostik gem. Art. 6 Abs. 1 lit. b DSGVO i.V.m. § 630a Abs. 1 BGB.

3. Erfüllung einer rechtlichen Verpflichtung

Klinische Studien und Forschung: Wenn Gesetze oder regulatorische Vorgaben verlangen, dass bestimmte klinische Daten für die Durchführung von Studien gesammelt und analysiert werden, kann KI eingesetzt werden, um diese Daten effizient zu verarbeiten. Die Verarbeitung von Patientendaten zur Überprüfung der Wirksamkeit und Sicherheit von Behandlungen könnte unter diese rechtliche Verpflichtung fallen.

Epidemiologische Überwachung:

Gesundheitsbehörden können KI-gestützte Systeme nutzen, um Daten über Krankheitsausbrüche oder andere öffentliche Gesundheitsfragen zu analysieren. Wenn nationale oder internationale Vorschriften erfordern, dass bestimmte Gesundheitsdaten gesammelt werden, um Infektionskrankheiten zu überwachen, dann kann der Einsatz von KI zur Datenanalyse gerechtfertigt sein

4. Schutz lebenswichtiger Interessen, Art. 6 Abs. 1 lit. d DSGVO. Ein KI-System unter Eingabe personenbezogener Daten etwa beim lebensrettenden Einsatz mit einem KI-System (die nicht zum Training verwendet werden) als Anwendungsfall in Betracht gezogen wird.

5. Berechtigten Interessen als Verarbeitungsgrundlage, Art. 6 Abs. 1 lit. f DSGVO. Mit dieser Vorschrift kann Rechtsunsicherheit verbunden sein. Folgende Aussagen/rechtliche Einschätzungen hat die Datenschutzaufsichtsbehörde Baden-Württemberg getroffen:

- Falls die Entwicklung eines KI-Systems auch ohne personenbezogene Daten oder mit anonymisierten Daten möglich ist, kann diese Rechtsgrundlage **nicht genutzt werden**. Es müssen andere rechtliche Grundlagen in Betracht gezogen werden, um den Datenschutz zu wahren.

6. Bußgeld

Die Datenschutzbehörde verhängte gegen ein Unternehmen, welches Verwaltungssoftware für niedergelassene Ärzte entwickelt, eine Geldstrafe in Höhe von 800.000 Euro wegen zweier datenschutzrechtlicher Verstöße.

- Zum einen hatte das Unternehmen nicht anonymisierte Gesundheitsdaten, die im Rahmen der Nutzung seiner Softwareprogramme erhoben wurden, ohne Genehmigung für Studien und Statistiken genutzt. Verarbeitet werden u.a. Patientendaten wie Geburtsjahr, Geschlecht, Allergien, Krankengeschichte, Größe, Gewicht, Diagnose, ärztliche Verschreibungen, Arbeitsunterbrechungen und Analyseergebnisse.

Ein erster Schritt für mehr Rechtssicherheit beim Umgang mit KI

Insgesamt wird deutlich, dass es durchaus schwerwiegende rechtliche „Knackpunkte“ gibt, deren technische Umsetzung erst noch bewerkstelligt werden muss, damit KI rechtssicher entwickelt werden kann.

4. Künstliche Intelligenz



Künstliche Intelligenz

DIHVA: Ein Projekt nimmt Fahrt auf
Der Digitale Hausärztliche Versorgungsassistent, kurz: DIHVA, soll mit Hilfe eines Koffers und KI-Ärzte und Praxispersonal vor allem in ländlichen Bereich entlasten.

Beispiele für Anwendungen

- KI im gastroenterologisch-internistischen Arztbereich
- KI für Hausarzt-Anwendungen
- KI für Diabetes-Behandlungen
- KI für Radiologie

Herausforderung bei KI-Daten:
Ein Personenbezug ist gem. Art. 4 Nr. 1, Hs. 2 DSGVO auch dann gegeben, wenn eine Person aufgrund weiterer (zusätzlicher) Informationen identifizierbar ist.

6/11

4.1. DIHVA: Ein Projekt nimmt Fahrt auf

Immer weniger Hausärzte, immer weitere Wege für immer mehr Patienten - so sieht die Prognose für die nächsten Jahre vor allem in ländlichen Regionen aus. Gleichzeitig bieten Digitalisierung, Telemedizin und KI alle Möglichkeiten, neue und bessere Versorgungsformen zu entwickeln. Das Aufgabenspektrum für nichtärztliches, digital geschultes Personal erweitert sich deutlich. Beginn der „Patientenreise“ medizinisch relevante Daten für die anschließende ärztliche Diagnose.

Ein standardisiertes Set tragbarer Diagnosegeräte, z.B. für EKG, Blut- und Urintests sowie Ultraschall, ermöglicht die Erhebung von über 50 diagnostischen Werten. Die Patientinnen und Patienten buchen die DIHVA-Termine online und können bereits bei der Buchung ihre Symptome eingeben. Anhand dieser Angaben formuliert eine KI im Hintergrund mehrere Arbeitsdiagnosen. Daraus wird abgeleitet, welche Untersuchungen der Versorgungsassistent durchführen soll. Die Ergebnisse werden digital an die jeweilige Arztpraxis übermittelt und stehen so bereits im nächsten Schritt, der Videosprechstunde, zur Verfügung.

4.2. KI im gastroenterologisch-internistischen Arztbereich

- KI-gesteuerte Bildanalyse für Darmpolypen
- Es gibt KI-Systeme zur Erkennung von Darmpolypen und anderen Darmveränderungen durch Bildanalyse. Diese können verdächtige Läsionen frühzeitig erkennen, was die Wirksamkeit der Darmkrebsvorsorge erhöhen kann.
- KI-basierte Unterstützung für Endoskopie
Es gibt KI-gestützte Systeme, die Ärzte bei der Durchführung von Endoskopien unterstützen. Diese können helfen, potenzielle pathologische Befunde zu identifizieren und den Arzt bei der Entscheidungsfindung zu begleiten.
- KI-unterstützte Sonographie mit Handhelds
Mobile Ultraschallgeräte mit KI-basierter Auswertungssoftware können die Routinediagnostik in der Inneren Medizin nachhaltig verändern. Diese Geräte unterstützen Ärzte bei der Diagnose und können möglicherweise das traditionelle Stethoskop in Zukunft ersetzen.

(<https://link.springer.com/article/10.1007/s00108-023-01604-z>)

4.3. KI für Hausarzt-Anwendungen

- **Buoy Health:** (<https://www.buoyhealth.com/>)
Buoy ist ein KI-gestütztes Tool, das Hausärzten hilft, Patientenanfragen zu verstehen und die richtigen nächsten Schritte zu empfehlen. Es kann in die Praxissoftware integriert werden, um die Patientenversorgung zu verbessern und die Effizienz zu steigern.
- **HealthTap:** (<https://www.healthtap.com/>)

HealthTap bietet eine KI-gestützte Plattform, die Hausärzten hilft, Patienteninformationen zu analysieren und personalisierte Empfehlungen zu geben. Die Plattform kann auch für virtuelle Konsultationen genutzt werden, was die Erreichbarkeit für Patienten erhöht.

- **Ginger:** (<https://www.ginger.com/>)
Ginger ist eine KI-gestützte Plattform, die psychische Gesundheitsdienste anbietet. Hausärzte können diese Plattform nutzen, um Patienten mit psychischen Gesundheitsproblemen zu unterstützen und geeignete Ressourcen bereitzustellen.
- **Lumos Diagnostics:** (<https://lumosdiagnostics.com/>)
Lumos bietet KI-gestützte diagnostische Tests, die in der Hausarztpraxis eingesetzt werden können. Diese Tests ermöglichen eine schnelle und präzise Diagnose von Erkrankungen, was die Entscheidungsfindung für Hausärzte erleichtert.

4.4. KI für Diabetes-Behandlungen

- **Medtronic Guardian Connect:** (<https://www.medtronic-diabetes.com>)
Ein kontinuierliches Glukoseüberwachungssystem, das KI verwendet, um Vorhersagen über Glukosewerte zu treffen.
- **IBM Watson Health:** ([IBM watsonx.ai](https://www.ibm.com/watsonx/ai))
Nutzt KI zur Analyse von Gesundheitsdaten, um personalisierte Behandlungspläne für Diabetiker zu erstellen.
- **Glooko:** (<https://glooko.com/de/produkte-fuer-medizinisches-fachpersonal/>)
Eine Plattform, die Daten von verschiedenen Diabetesgeräten sammelt und analysiert, um Patienten und Ärzten Einblicke zu geben.
- **DreaMed Advisor:** (<https://www.dreamed-diabetes.com>)
Eine KI-gestützte Plattform zur Optimierung der Insulintherapie.
- **Virta Health:** (<https://www.virtahealth.com>)
Bietet ein KI-gestütztes Programm zur Umkehrung von Typ-2-Diabetes durch Ernährungsumstellungen.

4.5. KI in der Radiologie

- **KI-gestützte Bildanalyse:**
Systeme, die Röntgen- und MRT-Bilder analysieren, um Frakturen oder Gelenkprobleme zu identifizieren.
Siemens Healthineers: <https://www.healthcare.siemens.com/artificial-intelligence>

4.6. KI in der Psychiatrie und Psychotherapie

- Mina - der erste KI-basierte Chatbot für die Verbesserung der Mentalen Gesundheit
<https://www.ventzke-media.de/de/blog/mina-entwicklung-chatbot-mentale-gesundheit/>

Herausforderung bei KI-Daten

Die Aufsichtsbehörde weist darauf hin, dass bei KI-Systemen auch die Möglichkeit besteht, dass erst im Nachhinein Zusatzinformationen die Identifizierbarkeit einer natürlichen Person ermöglicht werden könnte. Daher lässt sich die Frage, ob die DSGVO bzgl. eines KI-Systems zu berücksichtigen ist, nicht ein für alle Mal beantworten. Relevant bei der Frage, ob ein Personenbezug aktuell oder zu einem späteren Zeitpunkt hergestellt werden kann, sind die zum Einsatz gekommenen maschinellen Lernverfahren sowie die Wahrscheinlichkeit, dass eine (Re-)Identifizierbarkeit natürlicher Personen durch atypisches Einwirken auf die Systeme möglich ist.

5. Einwilligung



Was bedeutet Einwilligung

Die Einwilligung ist eine von 5 möglichen Rechtsgrundlagen, um Patienten-Daten verarbeiten zu dürfen.

5.1. Form der Einwilligung

Der Gesetzgeber schreibt keine Form der Einwilligung vor, weder die DSGVO noch das BGB im Patientengesetz.

Danach kann die Form der Einwilligung: **Stillschweigend** sein, was bedeutet, der Patient weiß

um den Zusammenhang Bescheid und muss nicht weiter gefragt werden, seine Einwilligung wird konkludent angenommen, wenn eine fallbezogene ärztliche Tätigkeit vorliegt.

Mündlich sein, wenn der Patient gegenübersteht und ein sichtbares oder hörbares Einverständnis-Zeichen gibt.

Schriftlich, die klassische Form.

Welche Form gewählt wurde muss in der digitalen oder papierenen Patientenakte dokumentiert werden. Dies genügt als Nachweis der Einwilligung. Dies vereinfacht den Aufwand wesentlich.

Beachte:

Die Fälle und auf welcher Grundlage man sich beruft, müssen im Patienten-Datenschutz-Informations-Blatt aufgelistet sein und in der Datenschutzerklärung auf der Webseite veröffentlicht werden.

5.2. Inhalt

Zur Gültigkeit einer mündlichen oder schriftlichen Einwilligung müssen bestimmte Fakten beinhaltet sein, sonst ist die Einwilligung ungültig und es dürfen keine Daten weitergegeben werden, bzw. es könnte zu einem Datenschutzverstoß führen:

Klare Formulargestaltung

Eine Einwilligung muss von der Formgestaltung klar erkennbar sein und darf nicht mit anderen Inhalten wie Anamnese usw. vermischt werden. Idealerweise ist die Einwilligung auf einem separaten Blatt Papier. Sollte es doch mit anderen Belangen auf einem Dokument stehen, so muss die Einwilligung klar abgetrennt und erkennbar sein. Daher ist es empfohlen, um Missverständnisse vorzubeugen, die Einwilligung getrennt zu führen. Ein Gestaltungsfehler kann zur Ungültigkeit der Einwilligung führen.

Konkretheit

Konkretheit bezieht sich auf die klare und präzise Angabe der Maßnahmen, für die der Patient seine Zustimmung gibt. Es ist wichtig, dass der Patient nicht nur im Großen und Ganzen weiß, worin er einwilligt, sondern es auch genau weiß. Es sind daher genaue Namen, Zeiträume, Örtlichkeiten und Produkte zu nennen.

Informiertheit

Dies umfasst die Bereitstellung aller relevanten Informationen über die Art, den Umfang, die Durchführung, die zu erwartenden Folgen und Risiken der Maßnahme sowie ihre Notwendigkeit, Dringlichkeit, Eignung und Erfolgsaussichten

Widerrufbarkeit

Widerrufbarkeit bezieht sich auf die Möglichkeit, die Zustimmung des Patienten zu einer Maßnahme zu widerrufen. Dies bedeutet, dass der Patient seine Zustimmung jederzeit vor der Durchführung der Maßnahme zurückziehen kann, ohne dass dies rechtliche Konsequenzen für ihn hat. Der Patient kann seinen Widerruf durch eine schriftliche oder mündliche Erklärung kundtun. Der Widerruf der Zustimmung kann in der Regel nur bis zum Beginn der Maßnahme wirksam sein. Nach Beginn der Maßnahme kann der Patient in der Regel nicht mehr widerrufen.

Freiwilligkeit

Die Freiwilligkeit in einer Einwilligung ist ein grundlegendes Prinzip, das die Möglichkeit des Patienten widerspiegelt, seine Zustimmung zu einer Maßnahme frei und ohne äußere Einflussnahme zu geben. Dieses Prinzip ist sowohl ethisch als auch rechtlich von großer Bedeutung und bildet die Grundlage für die Durchführung der Maßnahme.

Merke: Fehlt die Eindeutigkeit der Beschreibungen, oder sind die Punkte missverständlich formuliert, ist die Einwilligung ungültig.

5.3. Weitergabe

Im Rahmen einer Datenweitergabe von Arzt zu Arzt besteht die Möglichkeit einer stillschweigenden Datenweitergabe, sofern ein konkludenter Zusammenhang in der Tätigkeit besteht. Dies gilt auch ausdrücklich für die Mitarbeiter der Arztpraxis, die vom Arzt beauftragt werden, Daten weiterzureichen. Eine Datenweitergabe von Arzt zu Nichtarzt ist nur mit Einwilligung des Patienten zulässig, die mündlich oder schriftlich erfolgen muss. Dabei ist darauf zu achten, dass der Empfänger eindeutig identifiziert wird. In der Dokumentation wird vermerkt, wann die Einwilligung gegeben wurde, ob sie stillschweigend mündlich oder schriftlich verwendet wurde und wie die Identifizierung stattgefunden hat.

6. Einwilligungs-Beispiele:

Internet-Dienste:

AVV = Auftragsverarbeitungs-Vertrag = Datenschutzvertrag

Em = Einspruch möglich

Beispiele Einwilligung

Internet-Dienste:

- DocToLib Termin-Service -> **keine Einwilligung, Eigeninteresse, Datenschutzvertrag (AVV), Em** (=Einspruch möglich)
- Idana Web- Formular-Service -> **keine Einwilligung, Eigeninteresse, AVV, Em**
- Aaron Telefon-Service -> **keine Einwilligung, Eigeninteresse, AVV, Em**

Wartungs-Dienste:

- System-Fernwartung mit Auftragsverarbeitungsvertrag -> **keine Einwilligung, Gesetz, AVV, keine Em**

Praxis-Verwaltung:

- Schreibbüro mit Privatabrechnung im Namen des Arztes -> **keine Einwilligung nur Information, Vertrag, AVV, keine Em**
- Inkasso und Verkauf/Abtretung (Factoring) von Privatabrechnungen -> **Einwilligung schriftlich, AVV, Em**
- Gesundheits-Datenübermittlung an weiterbehandelnde Ärzte (Notarzt, Krankenhaus, Facharzt, Hausarzt), -> **Einwilligung, Em**
- Gesundheits-Datenübermittlung in die Telematik-Infrastruktur ePatienten-Akte -> **keine Einwilligung nur Information, Gesetz, Em (Opt-Out)**

Problem-Lieferant:

Dragon Spracherkennung Internet Version, es ist keine Fernwartung erlaubt, da der Lieferanten die Einhaltung der DSGVO und dem Berufsgeheimnis nicht garantiert. Produkt kann eingeschränkt verwendet werden, wenn bei Verwendung keine Personenstammdaten gesprochen werden.

Bei der reinen lokalen Version-16 ist der Funktionsumfang hingegen voll nutzbar. Jedoch kann nur ein deutsches Lieferunternehmen die Fernwartung mit einem AVV vornehmen, mit Ausschluss von Dragon als Subunternehmen.

8/11 ▶

Internet-Dienste:

- DocToLib Termin-Service -> **keine Einwilligung, Eigeninteresse, AVV, Em**
- Idana Formular-Service -> **keine Einwilligung Eigeninteresse, AVV, Em**
- Aaron Telefon-Service -> **keine Einwilligung Eigeninteresse, AVV, Em**

Wartungs-Dienste:

- System-Fernwartung -> **keine Einwilligung,**

Gesetz, AVV, kein Em

Praxis-Verwaltung:

- Schreibbüro mit Privatabrechnung im Namen des Arztes -> **keine Einwilligung, Vertrag, AVV, kein Em**
- Inkasso und Verkauf/Abtretung (Factoring) von Privatabrechnungen -> **Einwilligung schriftlich(!), AVV, Em**
- Gesundheits-Datenübermittlung an weiterbehandelnde Ärzte (Notarzt, Krankenhaus, Facharzt, Hausarzt), -> **stillschweigende (konkludente), mündliche, schriftliche Einwilligung, Em**
- Gesundheits-Datenübermittlung an Nicht-Ärzte (Versicherung, Therapeuten, usw.), -> **schriftliche Einwilligung, Em**
- Gesundheits-Datenübermittlung in die Telematik-Infrastruktur, ePatienten-Akte -> **keine Einwilligung, Gesetz mit gesetzliche Erlaubnis-Vorbehalt (Opt-In, solange bis Patient nicht aktiv widerspricht)**

Ein Problem-Lieferant:

Spracherkennung Dragon, die Internetversion, es ist keine Fernwartung durch Hersteller-Dragon-Mitarbeiter erlaubt, da der Hersteller die Einhaltung des Berufsgeheimnisses nicht garantiert. Das Produkt darf nur vom deutschen Händler mit AVV ferngewartet werden. Beim Diktieren dürfen keine personenbezogenen Stammdaten (Name, Adresse) gesprochen werden. Grund: Alle Daten gehen in die US-Cloud und werden dort ausgewertet. Empfehlung: Bei der rein lokalen Version, bis Version 16 ist

dagegen der volle Funktionsumfang nutzbar, da alles lokal gespeichert wird und nicht in die Cloud übertragen wird. Die Fernwartung kann nur von einem deutschen Anbieter mit AVV unter Ausschluss von Dragon als Subunternehmer durchgeführt werden.

7. Widerrufbarkeit der ePa

Widerrufbarkeit der ePa

- Kann ein Patient dem "eRezept" widersprechen? **Nein**
- Kann ein Patient der "eAU" widersprechen? **Nein**
- Kann ein Patient bei einer Befundübermittlung mit "eArztbrief" widersprechen? **JA**
- Wie ist der aktuelle Status der „eÜberweisung“?
- Kann ein Patient der "ePatientenakte" widersprechen **JA** und welche Auswirkung hätte das auf eRezept **keine** eAU **keine** eArztbrief **keine**
- Bei welcher Stelle muss der Patient seinen Einspruch zur ePatientenakte einreichen? **KK**
- Gibt es bestimmte Kriterien, die ein Patient erfüllen muss, um gegen die ePA Einspruch einlegen zu können? **Nein**
- Muss der Einspruch schriftlich sein? **JA**
- Bis wann kann ich die elektronische Patientenakte ablehnen? **ab sofort**
- Anlage 1: Musterschreiben zur Ablehnung elektronische Patienten-Akte
- Anlage 2: Inhalt einer Mitarbeiterliste im Rahmen eines Auskunftsanspruchs.
- Anlage 3: Datenschutz-Laufzettel

Kann ein Patient dem "eRezept" widersprechen?

Nein. Das E-Rezept ist jetzt Pflicht: So funktioniert es:

Ab dem 1. Januar 2024 sind sowohl Ärzte als auch Patienten verpflichtet, das eRezept bei der Verordnung von verschreibungspflichtigen Arzneimitteln zulasten der gesetzlichen Krankenversicherung zu nutzen.

Das rosafarbene Papier-Rezept wurde am 1.

Januar 2024 durch das E-Rezept abgelöst (Verlängerung bis Ende 2024). Versicherte erhalten verschreibungspflichtige Arzneimittel nur noch per E-Rezept und können dieses mit ihrer elektronischen Gesundheitskarte (eGK), per App oder mittels Papierausdrucks einlösen.

Die verpflichtende Nutzung gilt seit dem 1. Januar 2024.

Der Privat-Patienten muss jedoch bei seiner Versicherung anfragen, ob diese über eine „eRezept-Infrastruktur“ verfügt, nur dann kann er sie nutzen.

In Bezug auf Wiederholungsrezepte kann die Gültigkeitsdauer des Rezepts vom Arzt bestimmt werden und kann maximal ein Jahr betragen. Falls der Arzt hierzu keinen Vermerk macht, beträgt die Gültigkeit des Wiederholungsrezeptes 3 Monate.

Die Apotheke hat nur Zugriff auf das aktuell vom Arzt verabreichte Medikament. Eine Mehrfachabholung ist nicht möglich. Der Patient hat in seiner elektronischen ePatientenakte die Möglichkeit, den Zugriff der Apotheke auf den Medikationsplan freizuschalten, damit die Apotheke eine Kontraindikation erkennen kann.

Aufgepasst. Durch den Wegfall der Formularfarben rosa=Zuzahlung und grün=Vollzahler ist es ratsam, den Patienten entsprechend zu informieren, bevor er in der Apotheke den Schreck bekommt, dass er nicht nur 5 € zahlen muss, sondern den vollen Medikament Preis.

Kann ein Patient der "eAU" widersprechen?

Nein. Die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) ist ab dem 1. Januar 2023 verpflichtend.

Das bedeutet, dass Arbeitgeber die eAU elektronisch von der Krankenkasse abrufen können, anstatt eine physische Bescheinigung vom Arzt zu erhalten. Dieses Verfahren ist effizienter und schneller, da es Medienbrüche vermeidet und die Erstellung und Übermittlungskosten reduziert.

Allerdings haben Arbeitnehmer weiterhin Anspruch darauf, dass der Arzt ihnen die Arbeitsunfähigkeitsbescheinigung in Papierform aushändigt. Dies dient als gesetzlich vorgesehene Beweismittel mit hohem Beweiswert, um die Arbeitsunfähigkeit in Störfällen, wie z.B. einer fehlgeschlagenen Übermittlung im elektronischen Verfahren, nachzuweisen.

Kann ein Patient bei einer Befundübermittlung mit "eArztbrief" widersprechen?

Ja. Ein Patient hat grundsätzlich das Recht, gegen die Übermittlung seiner Befunddaten als eArztbrief an einen anderen Arzt zu protestieren. Dies kann beispielsweise der Fall sein, wenn er Bedenken hinsichtlich der Datensicherheit oder der Privatsphäre hat. Wenn der Patient gegen die Übermittlungsart widerspricht, muss der Arzt eine andere Übermittlungsart wählen.

Ärzte und Psychotherapeuten sind verpflichtet, die Patienten auf dieses Recht zum Widerspruch hinzuweisen. Außerdem müssen sie jeden Widerspruch nachprüfbar in ihrer

Behandlungsdokumentation protokollieren. Dies stellt sicher, dass die Entscheidungen des Patienten dokumentiert und respektiert werden

Wie ist der aktuelle Status der „eÜberweisung“?

Unbestimmt. Die elektronische Überweisung (eÜberweisung) wäre ein zentraler Bestandteil der digitalen Gesundheitsversorgung in Deutschland. Sie ermöglicht es Ärzten, Patienteninformationen direkt an andere medizinische Einrichtungen zu senden, was die Effizienz der medizinischen Versorgung verbessert und den Informationsaustausch zwischen medizinischen Einrichtungen erleichtert.

Der aktuelle Status der eÜberweisung ist noch offen. Weder bei der KVB noch bei der Gematik findet man Hinweise. Bis heute gibt es noch keine Einführungsplanung.

Kann ein Patient der "ePatientenakte" widersprechen und die Auswirkung auf eRezept, eAU, eArztbrief

Ja. Ein Patient hat grundsätzlich das Recht, Widerspruch gegen die elektronische Patientenakte (ePatientenakte) einzulegen. Dies bedeutet, dass der Arzt die Daten nicht in die Telematik-Infrastruktur übermitteln darf.

Wenn ein Patient der ePatientenakte widerspricht, können folgende Auswirkungen auftreten:

Rezept:

Das eRezept ist ein eigenständiges System und funktioniert auch ohne ePatientenakte. Allerdings kann die Apotheke bei Wegfall der ePatientenakte eine Unverträglichkeit von Medikamenten aus dem Medikationsplan nicht mehr erkennen.

eAU:

Die eAU ist ein eigenständiges System, bei dem der Arzt die eAU an die Krankenkasse schickt und der Arbeitgeber diese von dort abholen muss.

eArztbrief:

Der elektronische Arztbrief ist ein eigenständiger Kommunikationsdienst, ohne dass die elektronische Patientenakte (ePA) aktiv verwendet wird. Der Prozess des Erstellens und Sendens eines eArztbriefs ist so konzipiert, dass er ähnlich wie die Verwendung eines herkömmlichen Arztbriefs funktioniert, mit dem zusätzlichen Vorteil der elektronischen Kommunikation und der damit verbundenen Sicherheit und Effizienz.

Es ist wichtig zu beachten, dass der Widerspruch des Patienten gegen die ePA nicht bedeutet, dass die Krankenkasse alle Daten des Patienten löschen muss, sondern nur diese, die durch die Behandler erzeugt wurden. Nicht gelöscht werden die Versicherungsdaten, wie Stammdaten, Versicherungsprämien und Versichertenkarte-Daten. Stattdessen muss die Krankenkasse diese Daten des Patienten auf andere Weise speichern. Der externe Zugriff von anderen Stellen wird deaktiviert.

Gibt es bestimmte Kriterien, die ein Patient erfüllen muss, um gegen die ePA Einspruch einlegen zu können?

Nein. Es gibt keine spezifischen Kriterien, die ein Patient erfüllen muss, um gegen die elektronische Patientenakte (ePA) Einspruch einlegen zu können. Jeder Patient, der Mitglied einer Krankenkasse ist, die die ePA nutzt, hat das Recht, gegen die Nutzung der ePA zu protestieren.

Muss der Einspruch schriftlich sein?

Ja. Laut dem Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) muss der Widerspruch gegen die elektronische Patientenakte (ePA) schriftlich erfolgen.

Bis wann kann ich die elektronische Patientenakte ablehnen?

Jederzeit. Mit der kommenden Opt-Out Regelung wird ab Januar 2025 automatisch eine elektronische Patientenakte (ePA) von der Krankenkasse angelegt. Der Patient kann der Anlage der ePA jederzeit widersprechen. (Stand 15.05.2024)

Danke für Ihre Aufmerksamkeit



- Fragen
- Wünsche
- Anregungen

Reinhard Knoblich, Datenschutzbeauftragter TÜV Süd - rk@datenschutz-arzt.de 10/11 ▶

Wissens-Test

Um Daten verarbeiten zu dürfen, braucht man eine oder mehrere Rechtsgrundlagen.

1. Frage: Nennen Sie 1 von möglichen 5 Rechtsgrundlagen
Einwilligung – Gesetz – Vertrag – Notfall - Eigeninteresse
2. Frage: Warum sind Einwilligungen manchmal ungünstig
Weil sie widerrufen werden können

Reinhard Knoblich, Datenschutzbeauftragter TÜV Süd - rk@datenschutz-arzt.de

11/11 ▶

Anlage1: Musterschreiben, Ablehnung elektronische Patienten-Akte

Erich Mustermann
Am Tor 251 ·
83456 München

Adresse Krankenkasse

Datum
16.20.2024

Versicherungsnummer xyz

Widerspruch elektronische Patientenakte

Sehr geehrte Damen und Herren,

Hiermit widerspreche ich der Erstellung einer elektronischen Patientenakte über meine Person. Das Bundesverfassungsgericht hat eine Beschwerde und einen Eilantrag gegen die Regelungen zur elektronischen Patientenakte zurückgewiesen. Begründet wurde dies mit der Freiwilligkeit der Patientenakte.

Ich weise daher ausdrücklich darauf hin, dass ich keine elektronische Patientenakte wünsche.

Im Übrigen weise ich auf § 335 SGB V in der Fassung des PDSG hin:

(3) Versicherte dürfen nicht bevorzugt oder benachteiligt werden, weil sie den Zugriff auf Daten in einer Anwendung nach § 334 Abs. 1 Satz 2 ermöglicht oder verweigert haben.

Die von der Bundesregierung vorgesehene Möglichkeit des Opt-Out/Widerspruchs nach Anlage der ePA greift in meinem Fall nicht, da die Akte nicht angelegt werden darf.

Vielen Dank.

Mit freundlichen Grüßen

Ihr Name

Anlage 2: Inhalt einer Mitarbeiterliste im Rahmen eines Auskunftsanspruchs.

1. Name des Arbeitnehmers:

Dies ist das grundlegende Identifikationsmerkmal. Es hilft zu verstehen, wer an Ihrer Behandlung beteiligt war.

2. Funktion oder Rolle des Mitarbeiters:

Dies gibt Aufschluss darüber, welche Rolle der Mitarbeiter bei der Behandlung gespielt hat. Zum Beispiel kann ein Arzt, eine Krankenschwester oder ein Physiotherapeut unterschiedliche Rollen haben, die sich auf die Art der Behandlung auswirken können.

3. Zeitraum der Teilnahme:

Hier soll ein Überblick über den Zeitraum gegeben werden, in dem der Mitarbeiter an der Behandlung beteiligt war. Dies kann helfen, die zeitliche Abfolge von Behandlungen und Leistungen zu verstehen.

4. Besondere Leistungen oder Behandlungen:

Wenn möglich, sollte eine Liste spezifischer Leistungen oder Behandlungen, die von jedem Mitarbeiter durchgeführt wurden, angegeben werden. Dies könnte z. B. eine bestimmte Art von medizinischer Untersuchung, Operation, medikamentöser Behandlung oder Physiotherapie sein.

Beispiel Mitarbeiter-Liste

Mitarbeiterliste, die wir nach unseren Unterlagen identifizieren konnten, die an der Versorgung teilgenommen haben.

Unsere Mitarbeiterinnen und Mitarbeiter unterliegen auch nach ihrem Ausscheiden der Schweigepflicht und Vertraulichkeit gemäß DSGVO. Jeglicher Verstoß wird von uns straf- und zivilrechtlich verfolgt. Die Mitarbeiter-Daten unterliegen dem Datenschutz. Daher werden nur Nachname und Geschlecht angegeben.

Name	Funktion	Zeitraum	Leistung-Behandlung
Frau X,	Erfassen der Laborwerte,	12.10.2023,	Großes Blutbild
		19.12.2023,	Grippe Impfung
Frau Y	Erfassen Kardiodaten,	10.08.2023	Belastungs-EKG
Herr Z	ärztliche Tätigkeit	09.09.2023	Versorgung einer Kniewunde
		09.09.2023	Tetanusspritze
Frau O	Versorgung	12.-18.09.2023	Verbandwechsel

Patienten-Rechteersuchen-Laufzettel

unverzüglich(!), max. 4 Wochen bis zur Erledigung bei komplexen Fällen

1. Ersteller: Tages-Datum:

2. Patient:

Name: Vorname:
 Straße: PLZ/ Ort:
 Telefon: E-Mail:

3. Wie wurde das Ersuchen übermittelt/Identifikation, ----->Eingangs-Datum:

3.1. Brief (4 Wochen beginnen ab hier)

Adresse gleich mit Stammdaten
 Adresse ungleich: Kopie Personalausweis* anfordern, ---->Eingang:
(4 Wochen beginnen ab hier)

3.2. Direkter persönlicher Kontakt

persönlich bekannt
 Gesundheitskarte
 Personalausweis (nicht kopieren, nur zeigen lassen)

3.3. Telefon (Achtung besondere Sorgfalt, nur Ausnahmefälle)

Versicherten-ID Gesundheitskarte sagen lassen, oder
 Abfrage nach Kriterien, 4 müssen richtig sein:
 Geb.-Datum
 PLZ
 Straßen Nummer
 Tag der letzten Untersuchung
 Letzte Diagnose

3.4. E-Mail, Rück-E-Mail von der Praxis, mit der Bitte um die Versichertennummer
 oder einer Personalausweis-Kopie* -----> Eingangs-Datum:

3.5. Vertreter/Angehöriger-Person, (4 Wochen beginnen ab hier)
 nur mit amtlich oder rechtsanwältlich beglaubigter Einwilligung/Vollmacht,
 sonst Rechteersuchen ablehnen ! Einwilligung/Vollmacht (kopieren).

4. Art des Ersuchens:

Auskunft nach **DSGVO** oder **BGB**
 Berichtigung
 Übertragung der Daten
 Löschung
 sonstiges, z.B. Beschwerde über Datenschutz, usw.

5. Keine Patienten-Daten vorhanden, Negativ-Antwort an Patient ----> Datum:

6. Letzter ärztlicher Patientenkontakt -----> Datum:

7. Kopie-Laufzettel Weitergabe an: H.Knoblich ! + Vorgesetzten ! ---> Datum:

8. Antwortschreiben übermittelt -----> Datum:

per Einschreiben
 wurde persönlich abgeholt, sonst amtlich beglaubigte Vollmacht des Abholers (kopieren)
 per E-Mail, Daten verschlüsselt mit Kennwort im 2.E-Mail
 versendet per USB-Stick/CD per Einschreiben (oder verschlüsselt per Brief)
 Download-Link, versendet per Brief-Einschreiben zum geschützten Download-Bereich

9. Ablage in Datenschutz-Handbuch, mit allen Dokumenten in Kapitel „10.2. Fälle“

* unbedingt Hinweis mitgeben, dass die Personal-Felder **Augenfarbe, Größe, IDD-Nummer** geschwärzt werden sollten.

Notfallkarte: Verhalten bei Betroffenenersuchen

- Beschwerden, 
- Forderung nach Auskunft, **BGB** oder **DSGVO** 
- Berichtigung,
- Einschränkung der Verarbeitung,
- Widerspruch,
- Löschung der Daten
- Datenübertragbarkeit (Praxiswechsel)



Das müssen Sie tun:

1. Datenschutzbeauftragten anrufen
2. Laufzettel
 - a) Name der betroffenen Person,
 - b) die Art des Ersuchens und
 - c) eine zuverlässige Kontaktmöglichkeit für Rückfragen (Telefonnummer) aufnehmen.
 - d) **Prüfung der Zuständigkeit sowie Identitätsprüfung der betroffenen Person durchführen.**
 - e) **Weiterleiten des Ersuchens** umgehend an den Datenschutzbeauftragten oder ihren disziplinarischen Vorgesetzten.

Ihr Ansprechpartner ist:

**Herr Knoblich -
Datenschutzbeauftragter**
08092 – 333 33, rk@datenschutz-arzt.de

unverzüglich, max. 4



Wochen

vertretungsweise der Datenschutz- Koordinator
in Ihrem Unternehmen