Berufsverband der Kinder- und Jugendärzte e. V. Chausseestr. 128/129 10115 Berlin

Berufsverband der
Kinder- und Jugendärzte e.V.

Chausseestr. 128/129
10115 Berlin

Fon
(030) 28 04 75 10
Fax (0221) 68 32 04
kathrin.jackel-neusser@uminfo.de
www.kinderaerzte-im-netz.de
www.bvkj.de

Berlin, 21.02.2020

Stellungnahme des Berufsverbandes der Kinder- und Jugendärzte e.V.
zum
Referentenentwurf
des Bundesministeriums für Gesundheit
Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutzgesetz – PDSG)

Generelle Bewertung des Referentenentwurfes

Das Bundesgesundheitsministerium (BMG) formuliert im Referentenentwurf zum Patientendaten-Schutzgesetz (PDSG) zwei grundsätzliche Ziele: digitale Lösungen schnell an den Patienten[1] zu bringen und dabei sensible Gesundheitsdaten zu schützen. Das PDSG konkretisiert die datenschutzrechtlichen Anforderungen, die sich aus dem Digitale Versorgung-Gesetz (DVG) ergeben. Die jetzt vorgelegten Regelungen sollen schrittweise erweitert und stetig dem technologischen Fortschritt angepasst werden.

Beide Ziele sind wichtig und werden von uns im Grundsatz unterstützt.

Elektronische Patientenakte (ePA)

Sinnvoll und längst überfällig ist aus unserer Sicht, dass Krankenkassen ihren Versicherten ab 2021 eine elektronische Patientenakte (ePA) zur Verfügung stellen müssen, wie bereits durch das DVG bestimmt.

Nicht klar ist, inwiefern es aus therapeutischer Sicht überhaupt möglich sein kann, aufgrund der ePA-Daten zu einer fundierten ärztlichen Entscheidung zu gelangen, wenn die Nutzung der ePA freiwillig ist und der Patient allein entscheidet, welche Daten dort gespeichert, für den behandelnden Arzt sichtbar oder wieder gelöscht werden. Hier kommt aus unserer Sicht der von der KBV mehrfach eingebrachte Vorschlag einer elektronischen Arztakte (eAA) ins Spiel, den wir befürworten.[2]

Generell begrüßen wir, dass Patienten, die kein Smartphone oder Tablet haben, die Möglichkeit bekommen sollen, die ePA zu nutzen: Die Krankenkassen werden verpflichtet, ihren Versicherten ab 2022 geeignete Geräte zur Verfügung zu stellen – z.B. in den Filialen – und so den Zugang zur ePA zu ermöglichen.

[1] Im Folgenden sind immer alle Geschlechter (w/m/d) gemeint.
[2] Zum Beispiel hier: https://www.kbv.de/media/sp/2018_06_20_Diskussionsforum_KBV_Hofmeister.pdf

Wir begrüßen auch ausdrücklich, dass in der ePA ab 2022 Impfausweis, Mutterpass, das Gelbe Heft für die Kinderuntersuchungen sowie das Bonusheft für den Zahnarzt hinterlegt werden können.

Es ist sinnvoll, dass die Versicherten mit dem PDSG einen Anspruch darauf erhalten, dass ihr Arzt Daten in die ePA einträgt. Bei einem Kassenwechsel können Versicherte ihre Daten aus der ePA übertragen lassen.

Dieser Aufwand ist allerdings enorm zeitaufwändig und wird viele Ressourcen in den Praxen binden, wenn dies gewissenhaft durchgeführt werden soll. Für die Verwaltung und Erstbefüllung der Akte sollen Ärzte laut dem PDSG ein Honorar i.H.v. von 10,00 Euro erhalten. Diese Vergütung deckt nicht annähernd den Aufwand, den die Praxen mit der Befüllung der ePA haben. Es erhöht sich vielmehr der bürokratische Aufwand, der wieder Ressourcen der medizinischen Versorgung zieht.

Auch geregelt werden muss, inwiefern die Beratung der Ärzte und des Arztpersonals bezüglich der Befüllung der ePA zusätzlich vergütet wird. Die Patienten werden Fragen zur ePA haben, werden wissen wollen ob und welche Daten in der ePA gespeichert werden etc. Wie dieser zusätzliche Aufwand gelöst werden soll, ist noch völlig unklar.

Telematik-Infrastruktur / Datenschutz

Das Gesetz sieht darüber hinaus allgemeine Regeln für Datenschutz und -sicherheit vor. So ist jeder Nutzer der TI – egal ob Arzt, Krankenhaus oder Apotheker – für den Schutz der von ihm verarbeiteten Patientendaten verantwortlich. Betreiber von Diensten und Komponenten der TI werden unter Androhung eines Bußgeldes von bis zu 250.000 Euro dazu verpflichtet, Störungen und Sicherheitslücken unverzüglich an die Gesellschaft für Telematikanwendungen der Gesundheitskarte (Gematik) zu melden.

Hier kritisieren wir ganz ausdrücklich – und dies schon seit Bekanntwerden – dass alle Ärzte Konnektoren zu installieren haben[3] und die Verantwortung für den Datenschutz und die IT-Sicherheit bislang alleinig bei den Ärzten verbleibt, es dabei aber versäumt wurde, rechtzeitig mit der Verpflichtung der Etablierung einer TI auch eine gültige Sicherheitsrichtlinie eingeführt zu haben (Sie wird derzeit erst von der KBV entwickelt, die dafür nicht früher einen gesetzlichen Auftrag erhalten hatte!).

Sinnvoll wäre es gewesen, gleichzeitig mit der Einführung der TI ein Daten-Sicherheitskonzept für die Leistungserbringer zu entwickeln.

Die Verantwortung für die IT-Sicherheit der Komponenten darf nicht auf die Arztpraxen abgewälzt werden. Das gilt auch für die erheblichen Kosten, die ihnen im Zuge der mit der Digitalisierung verbundenen großen strukturellen Veränderungen entstehen werden. Hier ist der Gesetzgeber aufgefordert, klare Vorgaben zur Finanzierung der Strukturkosten zu setzen. Auch dies ist ein im Sinne der Akzeptanz notwendiges Signal.

Der Gesetzgeber hat die Ärzte hier bislang völlig allein gelassen, überfordert und durch Sanktionen dann auch noch abgestraft – mit dem Ergebnis, dass nun die Verunsicherung und Ablehnung sehr groß sind. Obgleich der BVKJ immer ein konstruktiver Partner bei der Umsetzung der Digitalisierung sein wird, kritisieren wir doch dieses Versäumnis ganz eindringlich!

Wir unterstützen daher auch die aktuelle Forderung der KBV, dass notwendigerweise mehr Geld für IT-Sicherheit in Praxen bereitgestellt werden muss.[4] Hier wird eine Finanzierungshilfe durch die Krankenkassen notwendig sein – im Interesse des Datenschutzes für die Patientinnen und Patienten.

[3] Siehe hier https://www.bvkj.de/presse/pressemitteilungen/ansicht/article/forderungen-des-berufsverbandes-der-kinder-und-jugendaerzte-bvkj-ev-zur-telematik/
[4] https://www.aerztezeitung.de/Wirtschaft/KBV-fordert-mehr-Geld-fuer-IT-Sicherheit-in-Praxen-406538.html

Denn die KBV hat neulich (am 7. Februar 2020) selbst angegeben, dass sie „enorme Investitionskosten“ für Arztpraxen befürchtet, wenn sie im Sommer 2020 ihre neue Datensicherheitsrichtlinie bekannt gibt, mit der die Anforderungen zur Gewährleistung der IT-Sicherheit verbindlich festgelegen werden sollen. Zusätzlicher Investitionsaufwand muss entsprechend auch von den Krankenkassen finanziert werden.

Der BVKJ hat sich bereits in seiner Stellungnahme zum Digitale Versorgung-Gesetz (DVG) konstruktiv-kritisch zu digitalen Neuerungen und zum Thema Datenschutz positioniert.[5]

In einer aktuellen Beschlussfassung zur Digitalisierung vom 19.01.2020 des BVKJ-Länderrates, der Versammlung der Landesverbandsvorsitzenden, wird erneut klar die Chance gesehen, durch eine sektorenübergreifende digitale Vernetzung sowie durch den Einsatz von Telekonsilen, Videosprechstunden und die Verschreibung von Gesundheits-Apps die Expertise der Ärzte zu stärken und die Patientenversorgung verbessern zu können. Hierbei müssen aber unbedingt die spezifischen Erfordernisse zur Behandlung im Kindes- und Jugendalter berücksichtigt werden.

Unser BVKJ-Länderrat schreibt: „Durch den digitalen Wandel in der Medizin bekommt das Arzt-Patienten-Verhältnis eine neue Dimension. Wir stehen zu unserer ärztlichen Verantwortung und müssen dafür Sorge tragen, dass unseren Patienten kein Schaden erwächst. So fordern wir Transparenz aller Datenflüsse in der Telematik-Infrastruktur und die freie Selbstbestimmung über die sensiblen Gesundheitsdaten durch den Patienten. Datensicherheit und Datenschutz sind unverzichtbare Grundlage und vor der Einführung sämtlicher digitaler Innovationen sicherzustellen. Sie müssen durch die Hersteller garantiert und durch unabhängige Stellen geprüft werden.

Eine Haftung für Mängel an digitalen Innovationen darf nicht auf unsere Praxen übertragen werden.

Digitalisierung muss praxistauglich und adäquat honoriert sein und einen nachweislichen Nutzen für die Patienten und deren Betreuung in der ambulanten und stationären Medizin aufweisen sowie einen Mehrwert für die Arzt-Patienten Beziehung darstellen.“

Diese Forderung wird sicher von den meisten Arztgruppen geteilt werden, das Bundesgesundheitsministerium muss die Belange der Ärzteschaft hier besser als bislang im Blick haben – im Interesse der zu versorgenden Patientinnen und Patienten.

Im Folgenden nehmen wir konkret zu den einzelnen Paragraphen des RefE Stellung:

Zu Artikel 1

Änderung des Fünften Buches Sozialgesetzbuch

Zu S. 14 f. / § 291b (Verfahren zur Nutzung der elektronischen Gesundheitskarte als Versicherungsnachweis)

„(5) Den an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringern und Einrichtungen, die ab dem 1. Januar 2019 ihrer Pflicht zur Prüfung nach Absatz 2 nicht nachkommen, ist die Vergütung vertragsärztlicher Leistungen pauschal um 1 Prozent, ab dem 1. März 2020 um 2,5 Prozent, so lange zu kürzen, bis sie sich an die Telematikinfrastruktur angeschlossen haben und über die für die

[5] https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP19/DVG/BVKJ_zum_Gesetzesentwurf_DVG.pdf

Prüfung nach Absatz 2 erforderliche Ausstattung verfügen. Von der Kürzung nach Satz 1 ist abzusehen, wenn der an der vertragsärztlichen Versorgung teilnehmende Leistungserbringer oder die an der vertragsärztlichen Versorgung teilnehmende Einrichtung gegenüber der jeweils zuständigen Kassenärztlichen oder Kassenzahnärztlichen Vereinigung nachweist, bereits vor dem 1. April 2019 die Anschaffung der für die Prüfung nach Absatz 2 erforderlichen Ausstattung vertraglich vereinbart zu haben. Die zur Teilnahme an der vertragsärztlichen Versorgung ermächtigten Ärzte, die in einem Krankenhaus tätig sind, ermächtigte Krankenhäuser und die nach § 75 Absatz 1b Satz 3 auf Grund einer Kooperationsvereinbarung mit der Kassenärztlichen Vereinigung in den Notdienst einbezogenen zugelassenen Krankenhäuser sind von der Kürzung nach Satz 1 bis zum 31. Dezember 2020 ausgenommen."

Unsere Bewertung:

Wie schon oben ausgeführt, kritisieren wir wiederholt[6], dass bei der Einrichtung der TI die Verantwortung bislang völlig bei den Ärztinnen und Ärzten verbleibt und es versäumt wurde, rechtzeitig mit der Verpflichtung der Etablierung einer TI auch eine gleichzeitig gültige Sicherheitsrichtlinie eingeführt zu haben (die derzeit erst von der KBV entwickelt wird, die dafür nicht früher einen gesetzlichen Auftrag erhalten hatte!). Die Verantwortung für die IT-Sicherheit der Komponenten darf nicht auf die Arztpraxen abgewälzt werden. Das gilt auch für die erheblichen Kosten, die ihnen im Zuge der mit der Digitalisierung verbundenen großen strukturellen Veränderungen entstehen werden. Hier ist der Gesetzgeber aufgefordert, klare Vorgaben zur Finanzierung der Strukturkosten zu setzen. Auch dies ist ein im Sinne der Akzeptanz notwendiges Signal.

Der Gesetzgeber hat die Ärzte hier bislang völlig allein gelassen, überfordert und durch Sanktionen dann auch noch abgestraft – mit dem Ergebnis, dass nun die Verunsicherung und Ablehnung sehr groß ist. Obgleich der BVKJ immer ein konstruktiver Partner bei der Umsetzung der Digitalisierung sein wird, so kritisieren wir doch dieses Versäumnis ganz eindringlich!

Wir unterstützen in diesem Zusammenhang die aktuelle Forderung der KBV, dass notwendigerweise mehr Geld für IT-Sicherheit in Praxen bereitgestellt werden muss.[7] Hier wird eine Finanzierungshilfe durch die Krankenkassen notwendig sein – im Interesse des Datenschutzes für die Patientinnen und Patienten. Denn die KBV hat neulich (am 7. Februar 2020) selbst angegeben, dass sie „enorme Investitionskosten" für Arztpraxen befürchtet, wenn sie im Sommer 2020 ihre neue Datensicherheitsrichtlinie bekannt gibt, mit der die Anforderungen zur Gewährleistung der IT-Sicherheit verbindlich festgelegen werden sollen. Zusätzlicher Investitionsaufwand muss entsprechend auch von den Krankenkassen finanziert werden.

[6] Siehe hier https://www.bvkj.de/presse/pressemitteilungen/ansicht/article/forderungen-des-berufsverbandes-der-kinder-und-jugendaerzte-bvkj-ev-zur-telematik/
[7] https://www.aerztezeitung.de/Wirtschaft/KBV-fordert-mehr-Geld-fuer-IT-Sicherheit-in-Praxen-406538.html

Zu

Elftes Kapitel

Telematikinfrastruktur

Erster Abschnitt

Anforderungen an die Telematikinfrastruktur

Zu S. 17f. / § 306 (Telematikinfrastruktur)

Absatz 3

„(…)Die Telematikinfrastruktur hat durch die diesem Schutzniveau angemessenen technischen und organisatorischen Maßnahmen die besonders schutzwürdigen personenbezogenen Daten gegen unbefugte Kenntnisnahme und Verwendung zu schützen.“

Unsere Bewertung:

Dies begrüßen wir. Der Arzt kann nur für die korrekte Internetanbindung seiner Praxis durch einen geeigneten IT-Anbieter verantwortlich gemacht werden. Die Verantwortung für den Datenschutz und die technische Sicherheit darüber hinaus muss nach korrekter Installation der TI in den Praxen bei den Anbietern liegen, nicht bei den Ärzten.

Zu S. 18 / § 307 (Datenschutzrechtliche Verantwortlichkeiten)

„(1) Die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 liegt in der Verantwortlichkeit derjenigen, die diese Komponenten für die Zwecke der Authentifizierung und zur sicheren Übermittlung von Daten in die zentrale Infrastruktur nutzen. Dies sind insbesondere die Leitungserbringer.

(2) Der Betrieb der durch die Gesellschaft für Telematik spezifizierten und zugelassenen Zugangsdienste nach § 306 Absatz 2 Nummer 2 Buchstabe a liegt in der Verantwortung des jeweiligen Anbieters des Zugangsdienstes.“

Unsere Bewertung:

Siehe weiter oben unsere generellen Ausführungen zu den Aspekten *Telematik-Infrastruktur / Datenschutz.*

Zu S. 20f. / § 311 (Aufgaben der Gesellschaft für Telematik)

„(1) Im Rahmen des Auftrags nach § 306 Absatz 1 hat die Gesellschaft für Telematik nach Maßgabe der Anforderungen gemäß § 306 Absatz 3 folgende Aufgaben:

1. zur Schaffung der Telematikinfrastruktur

a) die funktionalen und technischen Vorgaben einschließlich eines Sicherheitskonzepts zu erstellen,

b) Inhalt und Struktur der Datensätze für deren Bereitstellung und Nutzung festzulegen, soweit dies nicht nach § 355 durch die Kassenärztliche Bundesvereinigung oder die Deutsche Krankenhausgesellschaft erfolgt,

c) Vorgaben für den sicheren Betrieb der Telematikinfrastruktur zu erstellen und ihre Umsetzung zu überwachen,

d) die notwendigen Test-, Bestätigungs- und Zertifizierungsmaßnahmen sicherzustellen und

e) Verfahren einschließlich der dafür erforderlichen Authentisierungsverfahren festzulegen zur Verwaltung

aa) der Zugriffsberechtigungen nach dem Fünften Abschnitt und

bb) der Steuerung der Zugriffe auf Daten nach § 334 Absatz 1 Nummer 1 bis 6, (…)“

Unsere Bewertung:

Leider gilt dieses Datenschutzkonzept noch nicht, was zu großen Problemen für die medizinischen Leistungserbringer geführt hat. Siehe weiter oben unsere generellen Ausführungen zu den Aspekten *Telematik-Infrastruktur / Datenschutz.*

Zu S. 33 / § 329 (Maßnahmen zur Abwehr von Gefahren für die Funktionsfähigkeit und Sicherheit der Telematikinfrastruktur)

„(1) Soweit von Komponenten und Diensten eine Gefahr für die Funktionsfähigkeit oder Sicherheit der Telematikinfrastruktur ausgeht, ist die Gesellschaft für Telematik befugt, die erforderlichen technischen und organisatorischen Maßnahmen zur Abwehr dieser Gefahr entsprechend dem Stand der Technik zu treffen. Die Gesellschaft für Telematik informiert das Bundesamt für Sicherheit in der Informationstechnik unverzüglich über die Gefahr und die getroffenen Maßnahmen (…)“

Unsere Bewertung:

Siehe weiter oben unsere generellen Ausführungen zu den Aspekten *Telematik-Infrastruktur / Datenschutz.*

Es ist für die Praxen ein wahres Schreckensszenario, wenn ein solches verpflichtendes elektronisches System ausfällt. Bei Ausfall ist Chaos vorprogrammiert: Kein Rezept, Formular, Patienten in der Warteschleife. Das ist die Versorgungswirklichkeit. Diese – im Konkreten immer denkbare – Ausfallssituation muss ohne große Probleme gemanagt werden können.

Zu S. 34 / § 332 (Anforderungen an die Wartung von Diensten)

„(1) Dienstleister, die mit der Herstellung und der Wartung des Anschlusses von informationstechnischen Systemen der Leistungserbringer an die Telematikinfrastruktur einschließlich der Wartung hierfür benötigter Komponenten sowie der Anbindung an Dienste der Telematikinfrastruktur beauftragt werden, müssen besondere Sorgfalt bei der Herstellung und Wartung des Anschlusses an die Telematikinfrastruktur walten lassen und über die notwendige Fachkunde verfügen, um die Verfügbarkeit,

Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme und Komponenten zu gewährleisten."

Unsere Bewertung:

Uns ist unklar, wie diese „notwendige Fachkunde" konkret zertifiziert werden wird.

Zu S. 36 / § 335 (Diskriminierungsverbot)

„(1) Von Versicherten darf der Zugriff auf Daten in einer Anwendung nach § 334 Absatz 1 nicht verlangt werden."

Unsere Bewertung:

Siehe auch oben: Nicht klar ist, inwiefern es aus therapeutischer Sicht überhaupt möglich sein kann, dass die Nutzung der ePA freiwillig ist und der Patient allein entscheidet, welche Daten dort gespeichert, nicht sichtbar oder wieder gelöscht werden. Denn wie kann dann der Arzt bzw. die Ärztin den Überblick über die notwendigen Therapien und Medikationen behalten? Hier kommt der von der KBV mehrfach eingebrachte Vorschlag einer elektronischen Arztakte (eAA) ins Spiel, den wir befürworten.[8]

Zu S. 39f. / § 341 (Elektronische Patientenakte)

*„(…) 3. Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft
für Kinder), (…)" (…)*

5. Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation), (…)"

Unsere Bewertung:

Wir begrüßen ganz ausdrücklich, dass in der ePA ab 2022 Impfausweis, Mutterpass, das gelbe Heft für die Kinderuntersuchungen sowie das Bonusheft für den Zahnarzt hinterlegt werden können. Diese ist eine langjährige Forderung von uns.

Zu S. 42 / § 342 (Angebot und Nutzung der elektronischen Patientenakte)

„(…) f) die Versicherten die Zugriffsberechtigungen von einem Tag bis zu einer Dauer von höchstens 18 Monaten selbst festlegen können; (…)"

[8] Zum Beispiel hier: https://www.kbv.de/media/sp/2018_06_20_Diskussionsforum_KBV_Hofmeister.pdf

Unsere Bewertung:

Unsere Befürchtung ist, dass dies ggf. sehr häufig schlicht versäumt werden wird, wenn z.B. die Versicherten in der übergroßen Mehrheit eine Verlängerung der Zugriffsberechtigung schlichtweg vergessen sollten.

Zu S. 42 / § 342 (Angebot und Nutzung der elektronischen Patientenakte)

„(…) g) die Versicherten bis einschließlich 31. Dezember 2021 jeweils bei Zugriff auf die elektronische Patientenakte mittels der Benutzeroberfläche eines geeigneten Endgeräts gemäß § 336 Absatz 2 oder § 338 vor der Speicherung eigener Dokumente in der elektronischen Patientenakte auf die fehlende Möglichkeit hingewiesen werden, die Einwilligung sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der elektronischen Patientenakte nach Absatz 2 Nummer 2 Buchstabe b und c zu beschränken…(…)“

Unsere Bewertung:

Uns ist unklar, von wem die Versicherten hierauf hingewiesen werden sollen.

Zu S. 46 / § 346 (Unterstützung bei der elektronischen Patientenakte)

„(…) (4) Für Leistungen nach Absatz 2 erhalten die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer und Einrichtungen sowie Krankenhäuser ab dem 1. Januar 2021 über einen Zeitraum von 12 Monaten einen einmaligen Vergütungszuschlag je Erstbefüllung in Höhe von zehn Euro.“

Unsere Bewertung:

Es ist sinnvoll, dass die Versicherten mit dem PDSG einen Anspruch darauf erhalten, dass ihre Ärztin beziehungsweise ihr Arzt Daten in die ePA ein- bzw. (z.B. bei Krankenkassenwechsel) überträgt.

Dieser Aufwand ist allerdings enorm und wird viele Ressourcen in den Praxen binden, wenn dies gewissenhaft durchgeführt werden soll. Für die Verwaltung und Erstbefüllung der Akte sollen Ärzte laut dem PDSG ein Honorar erhalten. Dieses ist aber unverhältnismäßig gering und völlig unrealistisch!

Zu S. 68 / § 376 (Finanzierungsvereinbarung)

„(…) Die in § 306 Absatz 1 Satz 1 genannten Spitzenorganisationen treffen eine Vereinbarung zur Finanzierung

1. der erforderlichen erstmaligen Ausstattungskosten, die den Leistungserbringern in der Festlegungs-, Erprobungs- und Einführungsphase der Telematikinfrastruktur sowie

2. der Kosten, die den Leistungserbringern im laufenden Betrieb der Telematikinfrastruktur, einschließlich der Aufteilung dieser Kosten auf die in den §§ 377, 378 und 379 genannten Leistungssektoren, entstehen. Die Kosten nach Satz 1 zählen nicht zu den Ausgaben nach § 4 Absatz 4 Satz 2 und 6.“

Unsere Bewertung:

Dies halten wir für sinnvoll und wichtig.

Zu S. 103 / Zu § 307

„(…) Die Zuweisung der Verantwortlichkeit orientiert sich dabei an den für die jeweilige Stelle überblickbaren und beherrschbaren Strukturen, wie sie sich aus den einzelnen Bausteinen der Telematikinfrastruktur ergibt. Jeder Verantwortliche ist für den Bereich zuständig, in dem er über die konkrete Datenverarbeitung entscheidet.

Demnach sind insbesondere die Leistungserbringer für die Verarbeitung der Gesundheitsdaten der Versicherten mittels der in ihrer Umgebung genutzten Komponenten der dezentralen Infrastruktur im Sinne des § 306 Absatz 2 Nummer 1 verantwortlich. Die Verantwortlichkeit erstreckt sich schwerpunktmäßig auf die Sicherstellung der bestimmungsgemäßen Nutzung der Komponenten, deren ordnungsgemäßen Anschluss und die Durchführung der erforderlichen fortlaufenden Software-Updates.

Für den sicheren Zugangsdienst in die zentrale Infrastruktur im Sinne des § 306 Absatz 2 Nummer 2 Buchstabe a) ist der jeweilige Diensteanbieter verantwortlich. Dem besonderen Schutzbedarf der Inhaltsdaten beim Transport wird durch eine entsprechende Anwendung des Fernmeldegeheimnisses Rechnung getragen.

Für die Datenverarbeitung im gesicherten Netz im Sinne des § 306 Absatz 2 Nummer 2 Buchstabe b) ist der Anbieter datenschutzrechtlich verantwortlich, dem von der Gesellschaft für Telematik der Auftrag zum alleinverantwortlichen Betrieb erteilt wurde (Absatz 3 Satz 1). Damit wird zum einen klargestellt, dass die Gesellschaft für Telematik nicht selbst als Anbieter des gesicherten Netzes tätig wird. (…)“

Unsere Bewertung:

Siehe weiter oben unsere generellen Ausführungen zu den Aspekten *Telematik-Infrastruktur / Datenschutz.*

Diese Regelungen sind nach dem DVG wichtig und überfällig.

Schlussbemerkung:

Änderungen im weiteren Stellungnahmeverfahren behalten wir uns vor. Für Rückfragen stehen wir gerne zur Verfügung.