Univ.-Prof. Dr. jur. Dirk Heckmann

Lehrstuhl für Recht und Sicherheit der Digitalisierung
TUM School of Governance | Fakultät für Informatik
Technische Universität München

Gutachterliche Stellungnahme

für den Gesundheitsausschuss des Deutschen Bundestages

Sachverständigen-Anhörung vom 27. Mai 2020 zum

Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten
in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)
Drucksache 19/18793 v. 27.4.2020 und weiteren Anträgen

25. Mai 2020

unter Mitwirkung der wiss. Mitarbeiter|innen
Jakob Auer, Pascal Bronner und Marlene Manich

Beurteilung der §§ 307 ff., 342 ff. SGB V-E

1 Die vorliegende Stellungnahme beschränkt sich auf eine Beurteilung der Vorschriften zur datenschutzrechtlichen Verantwortlichkeit (§ 307 i.V.m. §§ 310 ff. SGB V-E) und zum „grob- bzw. feingranularen" Berechtigungskonzept (§§ 342 – 345 SGB V-E) und geht darüber hinaus auf das Verhältnis von Innovationsförderung und Datenschutzrisiken im Gesundheitswesen ein.

I. Allgemeines

2 Der Entwurf für ein Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz, im Folgenden: PDSG) ist – soweit er in dieser gutachterlichen Stellungnahme unter datenschutzrechtlichen Gesichtspunkten zu beurteilen ist – als wichtiger **Baustein für eine wirksame, einer zeitgemäßen Gesundheitsvorsorge dienliche Digitalisierung im Gesundheitswesen** zu begrüßen.[1] Er sorgt für eine rechtssichere Umsetzung der elektronischen Patientenakte und weiterer digitaler Anwendungen im Rahmen der Telematikinfrastruktur. Damit schließt er unmittelbar an das Digitale-Versorgung-Gesetz (DVG) an, um nunmehr eine sichere, vertrauensvolle und nutzerfreundliche digitale Kommunikation zwischen Leistungserbringern und Patienten sowie zwischen den Leistungserbringern untereinander zu ermöglichen. Die aktuelle Covid-19-Pandemie zeigt deutlich, wie wichtig es ist, Prozesse zu digitalisieren, damit Daten und Informationen noch schneller dort sind, wo sie gerade dringend benötigt werden. Der weitere Auf- und Ausbau der Telematikinfrastruktur kann künftig auch dazu beitragen, die Folgen einer solchen Pandemie besser zu bewältigen. Digitalisierung, Automatisierung und Vernetzung tragen auch zum Schutz der Gesundheit bei. So führte auch die **Datenethikkommission** der Bundesregierung im Leitsatz 10 ihres Abschlussberichts aus[2]:

„Mit Blick auf die Vorteile eines digitalisierten Gesundheitswesens spricht sich die DEK für einen raschen Ausbau digitaler Infrastrukturen innerhalb des Gesundheitssektors aus. Der qualitative und quantitative Ausbau digitalisierter Versorgungsmaßnahmen sollte die informationelle Selbstbestimmung des Patienten stärken. Hierzu gehört der partizipative Auf- und Ausbau der elektronischen Patientenakte (ePA) sowie die Weiterentwicklung von Verfahren zur Prüfung und Bewertung digitaler Gesundheitsanwendungen im ersten und zweiten Gesundheitsmarkt."

[1] Zur Notwendigkeit einer Digitalisierung im Gesundheitswesen vgl. schon *Heckmann*, Rechtliche Aspekte der Digitalisierung im Gesundheitswesen, vbw-Studie 2017, S. 1 ff. Abrufbar unter https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Sozialpolitik/2017/Downloads/20170824-Studie-Digitalisierung-Gesundheitswesen-final.pdf

[2] https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf, S. 19, 113 und 114: *In diesem Zusammenhang betont die DEK die Dringlichkeit des Auf- und Ausbaus der elektronischen Patientenakte (ePA), um die Qualität, Transparenz und Wirtschaftlichkeit der medizinischen Versorgung zu verbessern*".

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

3 Der Gesetzentwurf geht zu Recht von einem Prozess aus, in dem Digitale Innovationen kontinuierlich immer wieder neu ansetzen, iterativ weiterentwickelt und vorangetrieben werden müssen. Das hängt zum einen mit der dynamischen technologischen Entwicklung, zum anderen mit der erst langsam wachsenden Akzeptanz mancher Akteure für Veränderungen in ihrem gewohnten beruflichen bzw. privaten Umfeld zusammen. Innerhalb bestimmter Vorgaben höherrangigen Rechts, insbesondere des Gleichheitssatzes, der Berufsfreiheit und des rechtsstaatlichen Vertrauensschutzes, hat der Gesetzgeber einen **Gestaltungsspielraum**, wie, in welchem Umfang und mit welchem Tempo er Innovationen in einzelnen Tätigkeitsfeldern zulässt, fördert oder vorschreibt. Handlungsleitend kann insoweit insbesondere der Schutz höherrangiger Interessen, wie hier der Gesundheitsschutz, sein. Vor diesem Hintergrund ist vorliegend nicht zu beanstanden, dass der Gesetzentwurf der Digitalisierung im Gesundheitswesen Vorschub leistet, zumal er dies in moderater Form mit verhältnismäßigen Mitteln tut.

3 Digitalisierung und die damit verbundene (Teil-) Automatisierung von Prozessen und die Vernetzung der Akteure im Gesundheitswesen erfordern die Einhaltung hoher **Standards für Datenschutz und IT-Sicherheit**.[3] Zu Recht legt der Gesetzentwurf großen Wert darauf, dass nur Befugte Zugriff auf die sensiblen Gesundheitsdaten der Versicherten (wie Befunde, Diagnosen, Medikationen oder Behandlungsberichte) bekommen sollen. Ebenso müssen die Leistungserbringer, wie beispielsweise die Ärztinnen und Ärzte, Apothekerinnen und Apotheker u.a.m., zumal in ihrer besonderen Rolle als Berufsgeheimnisträger, darauf vertrauen können, dass die sensiblen Gesundheitsdaten sicher über die Telematikinfrastruktur übermitteltet werden. Die wesentlichen Schutzstandards hierfür ergeben sich bereits aus der Datenschutzgrundverordnung (DSGVO). Der Gesetzentwurf ergänzt und konkretisiert diese Vorschriften in dem notwendigen Maße.

II. Datenschutzrechtliche Verantwortlichkeit

4 Dies gilt in erster Linie im Hinblick auf die datenschutzrechtliche Verantwortlichkeit. Diese ergibt sich zwar im Grundsatz bereits aus der DSGVO, die aber insoweit Spielräume zur Spezifizierung lässt. Im Grundsatz trägt immer und soweit derjenige die Verantwortung, der für bestimmte Maßnahmen der Datenverarbeitung die Mittel und Zwecke bestimmt (Art. 4 Nr. 7 DSGVO). **Zwecke** der Datenverarbeitung sind vom Wortlaut ausgehend die Ziele und Gründe, aus denen der Verantwortliche die Datenverarbeitung

[3] Vgl. *Paschke*, Datenschutz im Medizinsektor, in: Specht/Mantz, Handbuch Europäisches und Deutsches Datenschutzrecht, 2019, § 13 Rn. 45 ff.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

durchführt oder durchführen lässt.[4] Ihnen kommt bei der Bestimmung des Verantwortlichen ein besonderes Gewicht zu.[5]

5 **Mittel** der Datenverarbeitung sind zunächst einmal die organisatorischen und technischen Mittel,[6] mit denen die Datenverarbeitung durchgeführt wird. Darunter fallen die für die Datenverarbeitung genutzte Hard- und Software und der Einsatz von Personal. Auffällig ist mit Blick auf den Wortlaut des Art. 4 Nr. 7 DSGVO, dass die zentralen Begriffe Zweck und Mittel der Datenverarbeitung in der gerichtlichen Praxis und in der Literatur selten differenziert und häufig nur als Begriffspaar verwendet werden. Überdies erfolgt regelmäßig keine dezidierte Subsumtion im Hinblick auf die Zwecke und Mittel.[7] Vielmehr wird die Verantwortlichkeit über den Sinn und Zweck des Art. 4 Nr. 7 DSGVO bestimmt: Nach der Grundkonzeption der DSGVO soll es **keine leeren Räume datenschutzrechtlicher Verantwortlichkeit** geben. Für die Einhaltung der Datenschutzbestimmungen und für die Ausübung der Rechte der betroffenen Personen soll es stets mindestens einen Verantwortlichen geben. In der Praxis entstehen bei komplexen IT-Infrastrukturen allerdings eher „zu viele" als zu wenige Verantwortliche. Genau hier, nämlich der Vermeidung solcher leeren Räume datenschutzrechtlicher Verantwortlichkeit, setzt auch der Gesetzentwurf in § 307 SGB V-E an.

6 Im Kern geht es bei Art. 4 Nr. 7 DSGVO darum, die Verantwortlichkeit solchen Personen konkret zuzuweisen, die eine derartige Entscheidungsgewalt über die Datenverarbeitung haben, dass sie die Einhaltung der Datenschutzbestimmungen und die Ausübung der Betroffenenrechte gewährleisten können.[8] Gegenstand der Verantwortlichkeit ist dabei immer ein **konkreter Datenverarbeitungsvorgang**,[9] so dass die Beurteilung für jeden einzelnen Datenverarbeitungsvorgang und jede Ebene der Datenverarbeitung separat vorzunehmen ist. Maßgeblich ist dabei die Entscheidungsgewalt des Verantwortlichen. Diese kann faktischer oder rechtlicher Natur sein.[10] Die faktische Entscheidungsgewalt folgt aus der Vornahme und Durchführung sowie technischen Ausgestaltung und Umsetzung der Datenverarbeitungsvorgänge im operativen Betrieb. Die Person, die die

---

[4] *Piltz*, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 26, Rn. 5; vgl. Artikel-29-Datenschutzgruppe, WP 169, S. 16.
[5] Artikel-29-Datenschutzgruppe, WP 169, S. 17.
[6] *Piltz*, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 26, Rn. 6.
[7] Exemplarisch: EuGH, Urt. v. 13.5.2014 – C-131/12 (Google Spain SL u. Google Inc./Agencia Española de Protección de Datos (AEPD) u. Mario Costeja González, Rn. 32 ff.; *Schild*, in: BeckOK Datenschutzrecht, 28. Edition 2019, Art. 4, Rn. 87 ff.
[8] Vgl. Artikel-29-Datenschutzgruppe, WP 169, S. 6; *Raschauer*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 4, Rn. 121.
[9] *Raschauer*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 4, Rn. 121.
[10] *Schantz*, in: Schantz/Wolff: Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 361; Artikel-29-Datenschutzgruppe, WP 169, S. 11.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

Datenverarbeitungsvorgänge **zu eigenen Zwecken in „Eigenregie“** durchführt, ist alleiniger Verantwortlicher aufgrund der faktischen Herrschaft über den Datenverarbeitungsvorgang.

7 Auch eine (bloß) **organisatorische und koordinierende Hoheit** kann eine Verantwortlichkeit indizieren[11], dies allerdings nur insoweit, als die operativ handelnden Personen (also jene, die die Daten unmittelbar verarbeiten), **„im Eigeninteresse“ der koordinierenden Stelle** tätig werden[12] (was bei der Gesellschaft für Telematik gerade nicht der Fall ist, weil diese kein „Eigeninteresse“ hat, sondern nur ihre gesetzlichen Aufgaben erfüllt). Insoweit ist zu beachten, dass die Entscheidung über die Zwecke der Datenverarbeitung im Vordergrund steht und die Mittel – sei es auch im Rahmen einer koordinierenden Tätigkeit – letztlich diesen „eigenen“ Zwecken dienen müssen. Insofern muss sich die Zwecksetzungsbefugnis stets auf die **Verarbeitung eines konkreten Datensatzes** beziehen; die abstrakte Bestimmung von Verarbeitungszwecken und -mitteln führt zu keiner Stellung als Verantwortlicher.[13]

8 In einer **komplexen Gemengelage wie der Telematikinfrastruktur**, in der eine Vielzahl von Akteuren, von den Leistungserbringern und den Leistungsträgern über die Netzwerkbetreiber bis zu den IT-Herstellern und IT-Dienstleistern, an der Generierung, Übermittlung und Nutzung von (Gesundheits-) Daten beteiligt sind, ist die Bestimmung des datenschutzrechtlich Verantwortlichen alles andere als trivial. Der Gesetzentwurf greift die Systematik der DSGVO deshalb in § 307 SGB V-E auf und wendet sie auf die Telematikinfrastruktur an: Danach ist jeder Verantwortliche jeweils für den Bereich zuständig, in dem er über die konkrete Datenverarbeitung entscheidet:

- **Nutzer der dezentralen Infrastruktur** (bestehend aus Komponenten zur Authentifizierung und zur sicheren Übermittlung von Daten in die zentrale Infrastruktur, § 306 Abs. 2 Nr. 1 SGB V-E) für die Datenverarbeitung im Rahmen dieser Nutzung, § 307 Abs. 1 SGB V-E
- **Anbieter von sicheren Zugangsdiensten** als Schnittstelle zur dezentralen Infrastruktur (§ 306 Abs. 2 Nr. 2a SGB V-E) für die Datenverarbeitung im Rahmen des Betriebs des jeweiligen Zugangsdienstes, § 307 Abs. 2 SGB V-E
- der **Anbieter des gesicherten Netzes** (§ 306 Abs. 2 Nr. 2b SGB V-E) für die Übertragung von personenbezogenen Daten, insbesondere von Gesundheitsdaten der Versicherten, zwischen Leistungserbringern, Kostenträgern sowie Versicherten und für die Übertragung im Rahmen der Anwendungen der elektronischen Gesundheitskarte, § 307 Abs. 3 SGB V-E

[11] *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 Rn. 171.
[12] EuGH, Urt. v. 10.7.2018, C-25/17 – Zeugen Jehovas - Rz. 68 ff.
[13] *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 Rn. 175.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

- der jeweilige **Anbieter von Diensten der Anwendungsinfrastruktur** (§ 306 Abs. 2 Nr. 3 SGB V-E) für die Datenverarbeitung im Rahmen der Nutzung des jeweiligen Dienstes, § 307 Abs. 4 SGB V-E
- die **Gesellschaft für Telematik**, soweit sie im Rahmen ihrer Aufgaben nach § 311 Absatz 1 die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist, § 307 Abs. 3 SGB V-E.

9 Die Regelung des § 307 SGB V-E zur datenschutzrechtlichen Verantwortlichkeit ist keineswegs redundant, sondern sorgt für **Rechtssicherheit in der Abgrenzung**. Insbesondere wird die Rolle der Gesellschaft für Telematik genauer definiert und abgegrenzt. Nach § 307 Abs. 5 Satz 1 SGB V-E ist sie Verantwortlicher für die Verarbeitung personenbezogener Daten in der Telematikinfrastruktur, soweit sie im Rahmen ihrer Aufgaben nach § 311 Abs. 1 die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist. Dies knüpft an die Rollenverteilung innerhalb der Telematikinfrastruktur an: Die Zwecke der Verarbeitung der insoweit relevanten (Gesundheits-) Daten werden durch die Leistungserbringer (in ihren berufsmäßigen Kontexten, insbesondere zur Heilbehandlung und Gesundheitsvorsorge), die Leistungsträger (nach Maßgabe ihres gesetzlichen Auftrags) und die Intermediäre im operativen Betrieb (entsprechend ihren vertraglichen Pflichten zur Funktionserfüllung der Telematikinfrastruktur) bestimmt. Für die Gesellschaft für Telematik in ihrer überwiegend strategischen Rolle verbleibt deshalb nur eine subsidiäre Verantwortlichkeit. **Dieses Konzept ist schlüssig** und steht mit den Vorgaben der DSGVO im Einklang.

10 Eine zentrale und begrüßenswerte Neuregelung findet sich in § 307 Abs. 5 Satz 2 und 3 SGB V-E: Danach richtet die Gesellschaft für Telematik für die Betroffenen eine koordinierende Stelle ein. Die **koordinierende Stelle** erteilt den Betroffenen allgemeine Informationen zur Telematikinfrastruktur sowie Auskunft über Zuständigkeiten innerhalb der Telematikinfrastruktur, insbesondere zur datenschutzrechtlichen Verantwortlichkeit nach dieser Vorschrift. Damit greift der Gesetzentwurf ein Grundanliegen der DSGVO auf, das diese mit der Bestimmung der datenschutzrechtlichen Verantwortlichkeit verbindet: Der Betroffene soll eine Person/Institution als Verantwortlichen haben, an die er sich im Streitfall wenden kann und der gegenüber auch die Betroffenenrechte (Art. 12 ff. DSGVO) und Sanktionen greifen; dies schafft Transparenz.[14] Weil genau diese Zuordnung innerhalb der Telematikinfrastruktur zuweilen schwerfällt, avanciert die Gesellschaft für Telematik zu einer Art datenschutzrechtlichem „Beistand“ (als einheitlicher Ansprechpartner) der Versicherten bzw. Patienten als datenschutzrechtlich Betroffenen. Eine solche

[14] Vgl. *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2019, Art. 12 Rn. 1 ff.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

Stelle zugunsten der Betroffenen durch nationales Recht einzusetzen, ergibt sich aus der Spezifizierungsermächtigung in Art. 9 Abs. 4 DSGVO (speziell für Gesundheitsdaten).

Fazit

Das Regelungskonzept zur datenschutzrechtlichen Verantwortlichkeit steht nicht nur mit höherrangigem Recht im Einklang. Es ist der Sache nach auch wegen der Schutzwirkung für die Betroffenen zu begrüßen.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

III. Berechtigungskonzept zum Zugriff auf Daten der elektronischen Patientenakte

1. Ausgangspunkt: Verpflichtende Einführung der elektronischen Patientenakte

11 Nach § 342 Abs. 1 SGB V-E, der mit dem Patientendatenschutzgesetz (PDSG) eingeführt werden soll, sind die Krankenkassen ab spätestens 1. Januar 2021 verpflichtet, auf Antrag und mit Einwilligung der Versicherten eine nach § 325 Abs. 1 SGB V-E von der Gesellschaft für Telematik zugelassene **elektronische Patientenakte (ePA)** zur Verfügung zu stellen. Die Erstellung und Nutzung ist für den Versicherten (Patienten) gemäß § 341 Abs. 1 SGB V-E freiwillig. Sie kann auch jederzeit wieder abgelehnt werden. Dies ist Ausdruck der **Patientensouveränität** sowie der Stärkung des Selbstbestimmungsrechts der Versicherten.[15]

2. Umsetzungsstufen und Berechtigungskonzept

12 Die Zugriffserteilung durch die Versicherten hinsichtlich ihrer Daten soll in verschiedenen Umsetzungsstufen geregelt werden, welche in § 342 Abs. 2 SGB V-E näher beschrieben werden. In § 342 SGB V-E wird zunächst das bisher in § 291a Absätze 5 und 5c SGB V zur elektronischen Patientenakte enthaltene geltende Recht übernommen. Darüber hinaus wird klargestellt, dass die Einführung der elektronischen Patientenakte hinsichtlich ihres inhaltlichen Umfangs sowie ihrer Funktionalitäten und der Weiterentwicklung der Möglichkeiten zur Steuerung der Zugriffsfreigabe durch die Versicherten in **Umsetzungsstufen** erfolgt, die von den Krankenkassen jeweils zu berücksichtigen sind. Das **Berechtigungsmanagement soll danach zweistufig erfolgen**[16], was mit der technischen Machbarkeit der Gestaltung und Umsetzung der ePA in der Praxis einschließlich ihrer Zugriffssysteme in vordefinierten Zeiträumen zusammenhängt.[17]

---

[15] BT-Drucksache 19/18793, S. 112; zur Patientensouveränität auch *Paschke* (o. Fn. 3), Rn. 50 ff.
[16] Darüber hinaus müssen die Krankenkassen ab dem 1.1.2023 nach Nummer 3 sicherstellen, dass in den von ihnen zur Verfügung gestellten elektronischen Patientenakten mit Einwilligung der Versicherten auch die Daten nach § 341 Absatz 2 Nummer 9, 10, 12 und 13 bereitgestellt und verarbeitet werden können. Ab 2023 müssen die Krankenkassen darüber hinaus gewährleisten, dass die elektronische Patientenakte die Voraussetzungen nach Nummer 4 erfüllt, wonach die Versicherten die Möglichkeit haben müssen, Daten ihrer elektronischen Patientenakte zu Forschungszwecken zur Verfügung zu stellen.
[17] BT-Drucksache 19/18793, S. 112.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

a) Berechtigungen und Zugriff der Versicherten in der 1. Umsetzungsstufe 2021

13 Nach § 342 Abs. 2 Nr. 1 SGB V-E soll die ePA ab dem 1. Januar 2021 sowohl für Frontend-Nutzer[18] als auch für Versicherte, welche kein Frontend nutzen können[19] oder wollen, mit einem **grobgranularen Berechtigungsmanagement**[20] starten. Danach muss die ePA gewährleisten, dass Daten nach § 341 Abs. 2 Nr. 1 SGB V-E[21] und nach § 341 Abs. 2 Nr. 6 SGB V-E[22] barrierefrei bereitgestellt werden können und Versicherte über eine Benutzeroberfläche eines geeigneten Endgeräts ihre Zugriffs- und Verarbeitungsrechte aus den §§ 336, 337 SGB V-E wahrnehmen können (§ 342 Abs. 2 Nr. 1 lit. a und b SGB V-E). Dabei haben Versicherte innerhalb des grobgranularen Berechtigungsmanagements aber eine Wahlmöglichkeit, ob sie die Einwilligung in den Zugriff durch zugriffsberechtigte Leistungserbringer nicht insgesamt, sondern auf Daten i.S.d. § 341 Abs. 2 Nr. 1 oder Nr. 6 SGB V-E erstrecken wollen. Auch dies wurde als **Ausdruck der Patientensouveränität** in den Gesetzesentwurf in § 342 Abs. 2 Nr. 1 lit. c SGB V-E mit aufgenommen und vermeidet auch innerhalb des grobgranularen Zugriffs ein Zurückgreifen auf das „Alles oder Nichts"-Prinzip.[23] Dabei sind den Versicherten über die Benutzeroberfläche eines geeigneten Endgeräts die Protokolldaten nach § 309 Abs. 1 SGB V-E in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache[24] und in auswertbarer Form sowie barrierefrei bereitzustellen, § 342 Abs. 2 Nr. 1 lit. d SGB V-E.

14 Die elektronische Patientenakte muss es schließlich Versicherten ermöglichen, Leistungserbringern **zeitlich und inhaltlich eingrenzbare Zugriffsberechtigungen** auf Daten ihrer elektronischen Patientenakte zu erteilen, diese inhaltlich auszuweiten, zeitlich zu verlängern oder erteilte Zugriffsberechtigungen auch jederzeit wieder einzuschränken oder vollständig zu entziehen. Die technische Voreinstellung für die Dauer einer Zugriffsberechtigung beträgt eine Woche (§ 342 Abs. 2 Nr. 1 lit. e SGB V-E). Auch wenn die Dauer der Zugriffsberechtigung von den Versicherten verkürzt oder auch leistungserbringerspezifisch von einem Tag bis zu einer Dauer von 18 Monaten erteilt werden kann (§ 342 Abs. 2 Nr. 1 lit. f SGB V-E), ist zu erwägen, ob man entsprechend dem **Grundsatz**

---

[18] Frontend-Nutzer sind diejenigen Versicherten, die über die Benutzeroberfläche eines geeigneten Endgeräts (z.B.: App auf dem Smartphone) auf die ePA zugreifen können.
[19] Frontend-Nichtnutzer sind hingegen all diejenigen Versicherten, die mangels geeigneten Endgeräts nicht auf die ePA zugreifen können.
[20] Unter einem grobgranularen Berechtigungsmanagement versteht man ein Zugriffssystem, in welchem die Versicherten nur auf alle Daten im elektronischen Patientensystem insgesamt bzw. in der in § 342 Abs. 1 Nr. 2 lit. c SGB V-E beschriebenen Wahlmöglichkeit zugreifen und Dritten Zugriff gewähren können.
[21] Medizinische Informationen über den Versicherten für eine einrichtungsübergreifende, fachübergreifende und sektorenübergreifenden Nutzung.
[22] Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden.
[23] BT-Drucksache 19/18793, S. 112.
[24] Zu diesen an Art. 12 DSGVO angelehnten Anforderungen *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2019, Art. 12 Rn. 8 ff.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO) die Default-Einstellung auf ganz wenige Tage (eben für den Regelfall der praktischen Zugriffszeit) verkürzt. In dieser Zeit kann der ausgewählte Leistungserbringer jederzeit ohne weiteres Zutun des Versicherten im Rahmen seiner Berechtigungen Daten in der elektronischen Patientenakte verarbeiten. Die Krankenkassen haben sicherzustellen, dass die Versicherten bei einer Nutzung der elektronischen Patientenakte vor dem 1. Januar 2022 jeweils auf die fehlende Möglichkeit des feingranularen Zugriffsberechtigungsmanagements hingewiesen werden (§ 342 Abs. 2 Nr. 1 lit. g SGB V-E).[25]

b) Berechtigungen und Zugriff der Versicherten in der 2. Umsetzungsstufe 2022

15 In der zweiten Umsetzungsstufe der elektronischen Patientenakte müssen die Krankenkassen ab dem 1.1.2022 sicherstellen, dass in den von ihnen zur Verfügung gestellten elektronischen Patientenakten mit Einwilligung der Versicherten auch die Daten nach § 341 Absatz 2 Nummern 2 bis 5, 7 und 8 sowie 11 SGB V-E bereitgestellt und verarbeitet werden können.[26] Darüber hinaus sind sie verpflichtet, ihren Versicherten ausschließlich eine elektronische Patientenakte zur Verfügung zu stellen, die es Versicherten ermöglicht, den Zugriff von Leistungserbringern zum einen über ihre persönliche Benutzeroberfläche sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der elektronischen Patientenakte vorab technisch zu berechtigen bzw. einzuschränken (**feingranulares Berechtigungsmanagement**[27]), und zum anderen unter Nutzung der dezentralen Infrastruktur der Leistungserbringer mindestens auf Kategorien von Dokumenten und Datensätzen, insbesondere medizinische Fachgebietskategorien, zu beschränken (**mittelgranulares Berechtigungsmanagement**[28]). Somit richtet sich der Umfang der technischen Möglichkeiten der Versicherten zur Zugriffsfreigabe danach, ob die Versicherten das Zugriffsmanagement unter Nutzung ihrer persönlichen Benutzeroberfläche (sog. Patienten-Frontend der elektronischen Patientenakte) ausüben oder die dezentrale Infrastruktur der Leistungserbringer zur Erteilung ihrer technischen Zugriffsfreigabe nutzen.[29]

---

[25] BT-Drucksache 19/18793, S. 112, 113.
[26] BT-Drucksache 19/18793, S. 113.
[27] Das feingranulare Berechtigungsmanagement beschreibt ein System, in welchem Versicherte dokumentenbezogen auf einzelne Dokumente bzw. Dateien in der ePA zugreifen und über diese disponieren können.
[28] Ein mittelgranulares Berechtigungsmanagement ist ein Zugriffssystem, in dem die Versicherten nur auf bestimmte Kategorien von Dokumenten und Datensätzen zugreifen und über diese disponieren können.
[29] BT-Drucksache 19/18793, S. 113.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

3. Kritik am Stufenkonzept des Berechtigungsmanagements

16 Von verschiedenen Seiten wird kritisiert, dass es bereits zum Start der ePA kein feingranulares Berechtigungssystem gibt und ein solches erst in der zweiten Umsetzungsphase starten soll.[30] Bei der elektronischen Patientenakte müsse schnellstmöglich gemäß den ausdrücklichen Aufforderungen des Bundesbeauftragten für die Informationsfreiheit und den Datenschutz stufenweise ein sogenanntes feingranulares Dokumentenmanagement für alle freiwilligen Nutzerinnen und Nutzer unabhängig von deren individuellen Abrufmöglichkeiten angeboten werden, um die erforderliche Nutzertransparenz gewährleisten zu können.[31] Materiell-rechtliche Gründe, die die Einräumung eines zeitlich gestaffelten Berechtigungskonzepts zumindest inhaltlich rechtfertigen könnten, seien dem Gesetzentwurf nicht zu entnehmen. Im Gegenteil: Sofern in der Einführungsphase der elektronischen Patientenakte die Versicherten nicht von der Möglichkeit einer feingranularen Zugriffsrechtegewährung Gebrauch machen können, bestünde die Gefahr, dass sich eine dazu in Widerspruch stehende Verfahrensweise etabliere, die im Nachhinein möglicherweise nicht mehr rückgängig gemacht werden könne.[32]

17 Bei einer versichertengeführten Patientenakte überwiege der potenzielle Nutzen die realen Risiken nur, wenn die Versicherten einzelnen Leistungserbringer nur für ausgewählte Dokumente und nicht pauschal auf alle Dokumente in der elektronischen Patientenakte den Zugriff erlauben können. Um Patienten das Angebot einer elektronischen Patientenakte empfehlen zu können, müsse ein differenziertes feingranulares Berechtigungsmanagement zwingend ab Verfügbarkeit der elektronischen Patientenakte integriert sein.[33]

18 Auch der Deutsche Caritasverband kritisiert, dass in dieser ersten Stufe die Versicherten keine feingranulierten, nach Leistungserbringern oder Leistungserbringergruppen differenzierte Berechtigungen vergeben können.[34]

19 Diese **Kritik am Stufensystem des Berechtigungskonzepts überzeugt nicht**. Sie übersieht, dass das Grundrecht auf informationelle Selbstbestimmung ebenso wenig wie Art. 16 Abs. 1 AEUV sowie das in der DSGVO verkörperte europäische Datenschutzrecht einen Anspruch auf ein bestimmtes technisches System verleiht. Das Recht, jederzeit bestimmen zu können, wer was wann über einen erfährt, gilt nur auf der Grundlage der in bestimmten Situationen geltenden, eingeführten Informations- und Kommunikationsbedingungen. Pointiert ausgedrückt: Es ist ein **Recht „aus" diesen Bedingungen und nicht**

[30] Stellungnahme des BfDI, S. 2; Ärzteblatt v. 01.04.2020; BR-Drucksache 164/20, S. 17.
[31] BT-Drucksache 19/19137, II Nr. 3.
[32] BR-Drucksache 164/20, S. 17.
[33] Bundespsychotherapeutenkammer, Stellungnahme zum PDSG vom 19. Mai 2020.
[34] Deutscher Caritasverband e.V., Stellungnahme zum PDSG vom 19. Mai 2020.

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

„auf" alternative Bedingungen. Schafft man ein neues Kommunikationssystem, das zur im Einzelfall unerwünschten Preisgabe personenbezogener Daten führen würde, genügt es, dass ein alternativer Kommunikationsrahmen angeboten wird, der diese Preisgabe ausschließt, auch wenn damit zugleich bestimmte Vorteile der Kommunikation nicht mehr verbunden sind. Es gibt keinen grundrechtlich fundierten Anspruch auf ein aus Sicht des Betroffenen optimales Kommunikationssystem. Auch das Recht auf informationelle Selbstbestimmung ist in erster Linie ein Abwehrrecht des Grundrechtsträgers und kein Leistungsrecht.

20 Legt man demzufolge das System zeitlich abgestufter Dispositionsbefugnisse der Versicherten/Patienten als gegeben zugrunde, behält der Betroffene die **Datenhoheit in jeder Phase**: Er kann zunächst bestimmen, ob er sich überhaupt auf dieses System und seine Bedingungen einlassen möchte. Die Einrichtung und Nutzung der elektronischen Patientenakte ist für den Versicherten freiwillig. Darauf wird er auch ausdrücklich hingewiesen, genauso wie auf den Umstand, dass ein sog. feingranulares Berechtigungsmanagement erst ab dem Jahr 2022 zur Verfügung steht. Lehnt er diese Kommunikationsbedingungen ab, steht es dem Versicherten frei, die elektronische Patientenakte erst zu diesem späteren Zeitpunkt zu nutzen und bis dahin in konventioneller Weise zu kommunizieren. Daraus erwächst ihm kein prinzipieller Nachteil.

21 Diese stufenweise Digitalisierung der Kommunikation innerhalb der Telematikinfrastruktur ist sachlich begründet, weil eine frühere Realisierung des feingranularen Berechtigungskonzepts laut Gesetzesbegründung aus technisch-organisatorischen Gründen nicht möglich ist. Aus Sicht des Gesetzentwurfs gab es deshalb nur zwei Möglichkeiten: Entweder man hätte den gesamten Digitalisierungsprozess um die elektronische Patientenakte um ein weiteres Jahr aufgeschoben oder man musste den skizzierten Stufenbau wählen. Dass man sich für Letzteres entschieden hat, ist aus grundrechtlicher Sicht nicht zu beanstanden. Die **Vorteile dieser Vorgehensweise** (frühere Etablierung der elektronischen Patientenakte, bessere Möglichkeit, die Belastbarkeit des Systems zu testen, schrittweises Heranführen aller Akteure) überwiegen den Nachteil für diejenigen, die sich einen schnelleren Zugang zu einem feingranularen Berechtigungskonzept gewünscht hätten.

22 Bei alledem darf man eines nicht übersehen: Das **Arzt-/Patientenverhältnis beruht in großem Maße auf Vertrauen**. Das gilt für die ärztliche Untersuchung, die Befundung, Diagnosen und Therapien genauso wie für die Einhaltung der ärztlichen Schweigepflicht. Es ist nicht unredlich, anzunehmen, dass ein Großteil der Patienten davon ausgeht, dass ein Arzt beim Blick in die elektronische Patientenakte jene Informationen „ausblendet", die für ihn nicht relevant sind. Ferner ist der behandelnde Arzt nur zur Verarbeitung

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de

derjenigen Daten berechtigt, die für die Behandlung erforderlich sind, Art. 9 Abs. 2 lit c bzw. h DSGVO. Die Offenlegung weiterer Daten kann im vorliegenden Fall nicht als ausdrückliche Einwilligung einer weitergehenden Verarbeitung gewertet werden, vgl. Art. 9 Abs. 1 lit. a DSGVO. Für diesen Personenkreis sollte das Berechtigungskonzept daher im ersten Betriebsjahr 2021 eine **verfassungsmäßige Übergangslösung** bieten. Das bedeutet umgekehrt nicht, dass schon aufgrund dieses vermuteten Vertrauensverhältnisses jegliche Feingranulierung (bis hin zur Dokumentenebene) obsolet wäre. Deshalb erfolgt die zweite Stufe – verpflichtend – ab dem Jahr 2022. In der Zwischenzeit kann derjenige, der den tatsächlich möglichen Blick auf weitere Daten verhindern will, auf den Einsatz der elektronischen Patientenakte vorübergehend verzichten. Außerdem besteht bereits ab 2021 die **Möglichkeit, den Zugriff einzelnen Ärzten gegenüber zu versagen**. Die Einrichtung der elektronischen Patientenakte und ihre Nutzung etwa durch den Hausarzt führt nicht automatisch zu einem beliebigen Zugriff durch beteiligte Ärzte. Vielmehr hat der Patient auch bereits in der ersten Phase der Nutzung (2021) das Recht, festzulegen, ob etwa ein Facharzt, zu dem eine Überweisung erfolgt, auf die elektronische Patientenakte zugreifen darf oder ob einzelne Befunde, Dokumente etc. auf bisheriger Weise (FAX, Brief etc.) übermittelt werden. Dies ergibt sich unter anderem auch aus den einzelnen Einwilligungsregelungen in den §§ 337 Abs. 3, 339, 352, 353 Abs. 1 SGB V-E.[35] Somit wird der Datenhoheit und Patientensouveränität ausreichend Rechnung getragen.

Fazit

Das Konzept eines zeitlich gestuften Berechtigungskonzepts ist datenschutzkonform und auch rechtspolitisch zu begrüßen. Es schränkt die Datenhoheit des Patienten nicht ein, sondern trägt der technischen Entwicklung Rechnung. Damit forciert es die Digitalisierung im Gesundheitswesen mit all ihren Vorteilen und überlässt es dem Patienten/Versicherten, in welchem Tempo er an dieser Entwicklung teilhaben möchte.

[35] Vgl. auch die Gesetzesbegründung: *„Die Dauer der Zugriffsberechtigung kann von den Versicherten verkürzt oder **auch leistungserbringerspezifisch** von einem Tag bis zu einer Dauer von 18 Monaten erteilt werden. In dieser Zeit kann **der ausgewählte Leistungserbringer** jederzeit ohne weiteres Zutun des Versicherten im Rahmen seiner Berechtigungen Daten in der elektronischen Patientenakte verarbeiten.“ (BT-Drucksache 19/18793 S. 112 f.)*

TUM School of Governance | Richard-Wagner-Str. 1, 80333 München | Tel. 089-907793-301 | dirk.heckmann@tum.de