

Zur Rechtskonformität des Erfordernisses eines Lichtbildes für die eGK unter besonderer Berücksichtigung des Rechts auf informationelle Selbstbestimmung sowie der Vorgaben der DSGVO (Teil I)

Luisa Lorenz

Wiederholt war die elektronische Gesundheitskarte (eGK) Gegenstand von Gerichtsverfahren. Speziell die gesetzlich normierte Pflicht zur Beibringung eines aktuellen Lichtbildes zum Schutz vor Verwechslungen und Missbrauch und damit der unberechtigten Inanspruchnahme von Leistungen ist regelmäßig Anlass zur Klage.

Bereits mehrmals entschied das BSG, dass die verpflichtende Aufnahme eines Lichtbildes eines Versicherten auf der eGK rechtmäßig sei¹. Ende 2021 (Az. L 4 KR 651/19) hat das LSG Bayern diese Rechtsauffassung bestätigt². Kommen Versicherte ihrer Mitwirkungsobliegenheit zur Überlassung eines aktuellen Fotos zur Ausstellung des Versicherungsnachweises in Form der eGK trotz mehrmaliger Abmahnung der Krankenkasse nicht nach, dürfe die Ausstellung einer befristeten Ersatzbescheinigung für die eGK rechtmäßig versagt werden. Weder das Lichtbilderfordernnis selbst noch der Auf- und Ausbau der Telematikinfrastruktur (TI) verstießen gegen das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG). Auch habe der Gesetzgeber den Vorgaben der DSGVO³ ausreichend Rechnung getragen. Art. 4 GG sei ebenfalls nicht verletzt.

Die Linie der Gerichte ist eindeutig; das LSG Bayern sorgt für zusätzliche Rechtssicherheit und Rechtsklarheit auf Betroffenen- und Leistungserbringerseite. Während etwa die Speicherdauer des Lichtbildes inzwischen gesetzlich geregelt ist, ist zur Beantwortung gesetzgeberisch bislang nicht aufgegriffener Rechtsfragen – etwa, inwieweit überlassene Fotos bearbeitet werden dürfen –, allem voran die jeweils einschlägige Rechtsprechung heranzuziehen.

Dieses Rechtsgefüge berücksichtigend, soll im Folgenden ein Überblick zum Lichtbilderfordernnis der eGK aus maßgeblich datenschutzrechtlicher Perspektive gewährt werden⁴. Die inhaltliche Darstellung erfolgt anhand des gesetzlichen Ordnungsrahmens sowie ausgewählter (höchstrichterlicher) Judikatur der jüngeren Vergangenheit. In Rede steht v.a. die Vereinbarkeit mit den Vorgaben der DSGVO, speziell die Gewährleistung einer angemessenen Datensicherheit sowie die Verfassungskonformität hinsichtlich des Rechts auf informationelle Selbstbestimmung⁵. Dem vorangestellt sind dem Grundverständnis dienende Ausführungen das „System eGK“ betreffend. Abschließend widmet sich der Beitrag in einem Ausblick der ab dem 1. 1. 2024 ergänzend zur eGK verfügbaren sicheren digitalen Identität im Gesundheitswesen. Vorbehaltlich spezifischer Nennung der privaten Krankenversicherung (PKV), nehmen sämtliche Ausführungen die gesetzliche Krankenversicherung (GKV) in Bezug.

I. Technisch-strukturell-konzeptionelle Einführung

Um datenschutzrechtliche Fragestellungen spezifisch zum Lichtbilderfordernnis der eGK aufwerfen, gewichten und

beantworten zu können, bedarf es des technisch-strukturell-konzeptionellen Verständnisses des eGK-Systems. Gleichwohl sei der Vollständigkeit halber erwähnt, dass das Erfordernis eines Lichtbildes vor dem Hintergrund der drohenden Identitätstäuschung bereits bei der alten Krankenversicherungskarte diskutiert wurde.

1. Grundsätzliches

Mit der Gesundheitsreform 2004 beschloss der Gesetzgeber die Einführung der eGK (einer „personenbezogenen Smartcard“⁶ „zur Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung“⁷) und zugleich die Ablösung der seit dem 1. 1. 1995 gültigen Krankenversicherungskarte. Nach der schließlich stufenweisen Einführung ab dem 1. 10. 2011⁸, besitzt seit dem 1. 1. 2015 nur noch die eGK Gültigkeit⁹.

Die Ergänzung der – damals noch – Krankenversicherungskarte um ein Lichtbild (nunmehr in § 291a Abs. 5

*) Die Autorin dankt Herrn Prof. Hornung, LL.M. für die wertvolle Unterstützung bei der Erstellung dieses Beitrags.

- 1) Grundlegend BSG, Urt. v. 18. 11. 2014 – B 1 KR 35/13 R –, BSGE 117, 224. Ein Versicherter, der sich durch die Lichtbildpflicht in seinem Recht auf informationelle Selbstbestimmung verletzt sah, blieb damals mit seinem Begehren – die Ausstellung einer Nachweisberechtigung der bestehenden GKV gänzlich ohne Lichtbild – erfolglos. Ein derartiger Anspruch bestehe nicht. Vielmehr hätten Versicherte eine dem Allgemeininteresse geschuldete Mitwirkungspflicht, den Missbrauch von Krankenkassenleistungen zu verhindern. Grundrechte würden dadurch nicht verletzt.
- 2) Dazu Lorenz, jurisPR-ITR 1/2022, Anm. 6. Weiterhin wurde die Beschwerde der Klägerin gegen die Nichtzulassung der Revision in einem weiteren Urteil des LSG Bayern (Urt. v. 22. 6. 2021 – L 20 KR 397/18) inzwischen vom BSG als unzulässig verworfen (Beschl. v. 21. 2. 2022 – B 12 KR 47/21 B).
- 3) VO 2016/679/EU.
- 4) Zum Erfordernis der eigenständigen Unterschrift nach (nunmehr) § 291a Abs. 7 SGB V für die Sicherstellung der Identifikationsfunktion s. LSG Bad.-Würt., Urt. v. 24. 1. 2017 – L 11 KR 3562/16 –, juris und SG Berlin, Beschl. v. 7. 11. 2013 – S 81 KR 2176/13 ER –, juris. Die Verpflichtung zur Unterschriftsleistung verstoße grundsätzlich nicht gegen das Recht auf informationelle Selbstbestimmung. Bei Minderjährigen (bis zur Vollendung des 15. Lebensjahres) sind die §§ 11 und 36 SGB I zu beachten (sozialrechtliche Handlungsfähigkeit).
- 5) Praktisch Kritik am Lichtbilderfordernnis wurde dahingehend geäußert, dass die Krankenkassen nicht überprüfen, ob es sich bei dem eingereichten Lichtbild tatsächlich um ein solches des Versicherten handelt.
- 6) So die Bezeichnung der gematik, s. <https://fachportal.gematik.de/karten-und-identitaeten/elektronische-gesundheitskarte>.
- 7) BT-Dr. 15/1525, 46.
- 8) Der jahrelange Streit über Kosten und Datenschutz bedingte die wiederholte Verschiebung der Kartenausgabe, die bereits spätestens zum 1. 1. 2006 erfolgen sollte, s. § 291a Abs. 1 SGB V a. F. (nach GKV-Modernisierungsgesetz).
- 9) Dem Antrag der FDP, ein Moratorium für die eGK herbeizuführen, gab der Bundestag nicht statt. Ebenfalls abschlägig beschieden wurde ein Antrag von Bündnis 90/Die Grünen, der das Freiwilligkeitsprinzip sowohl für Patienten als auch für Leistungserbringer forderte.

SGB V geregelt) sah erstmals der Entwurf des GKV-Modernisierungsgesetzes aus dem Jahr 2003 vor¹⁰. Zugleich wurden die administrativen Daten um die Angabe des Geschlechts erweitert. Ziel der zum 1. 1. 2004 erfolgten Änderung der Sicherheitsmerkmale war es, durch Verbesserung der eindeutigen Zuordnung zum jeweiligen Karteninhaber, (Identitäts-)Missbrauch zu verhindern¹¹.

Legt der Versicherte seine eGK beim Leistungserbringer vor, ist dieser verpflichtet, die Identität des Versicherten anhand der auf der eGK aufgetragenen Identitätsdaten, u. a. dem Lichtbild, zu prüfen¹². Im Zweifelsfall kann sich der Leistungserbringer zusätzlich den Personalausweis oder ein anderes Ausweisdokument zeigen lassen (dies wird derzeit gerade mit Blick auf die Pflicht zum Tragen von Masken in Gesundheitseinrichtungen praxisrelevant sein).

Am 20. 10. 2020 erfuhr die eGK durch das Gesetz zum Schutz elektronischer Patientendaten in der TI (Patientendaten-Schutz-Gesetz, PDSG, BGBl. I 2020, S. 2115) zahlreiche (strukturelle) Änderungen (v. a. eigenständiger Zugriff von Versicherten auf die elektronische Patientenakte [ePA], Einführung des E-Rezepts); das Fotoerfordernis war indes nicht tangiert. Betroffen waren alle in der GKV Versicherten, mithin von den mehr als 83 Millionen Menschen in Deutschland ca. 74 Millionen in 97 Kassen der GKV (Stand Juli 2022)¹³.

Verschlüsselt auf dem Mikrochip der Chipkarte, – die mittlerweile nicht nur Versicherungsnachweis, sondern zugleich Schlüssel zu digitalen Anwendungen im Gesundheitswesen ist¹⁴ –, für alle Versicherten verpflichtend gespeichert sind die Versichertenstammdaten (Name, Geburtsdatum, Adresse, Versichertennummer/-status¹⁵, vgl. § 291a Abs. 2 SGB V); die Europäische Krankenversicherungskarte (European Health Insurance Card, EHIC) befindet sich auf der Rückseite jeder eGK (Hintergrund dessen ist, dass sich § 291a Abs. 4 ausdrücklich nicht auf § 291a Abs. 3 Nr. 5 SGB V bezieht, d. h. keine Pflicht zur Speicherung in für maschinelle Übertragung geeigneter Form besteht). Die Notfalldaten und der elektronische Medikationsplan (eMP) (dazu § 358 SGB V) werden nur auf ausdrücklichen Wunsch des Versicherten gespeichert. Einige Funktionen der eGK sind ebenfalls nur verfügbar, wenn der Versicherte das wünscht; zusätzlich bedarf es hierbei der Eingabe einer sechsstelligen PIN. Daneben speichert die eGK digitale Schlüssel, d. h. die digitale Identität des Versicherten, mit denen sich dieser in der TI technisch ausweisen (authentifizieren) kann, v. a. um die durch das PDSG eingeführten Neuerungen in Anspruch zu nehmen (wie z. B. auf seine ePA zuzugreifen).

Nur auf der eGK abgebildet, d. h. gerade nicht auf dieser gespeichert, ist das zur Ausstellung vorausgesetzte Lichtbild. Dies bestätigt der Blick in § 291a SGB V, der dem Lichtbilderfordernis einen eignen Absatz 5 widmet und dieses gerade nicht in den Absätzen 2 und 3 regelt.

2. Gewährleistung von Datenschutz und Informationssicherheit

Gesundheitsdaten sind in besonders hohem Maße schutzbedürftig (vgl. Art. 2 Nr. 15, Art. 9 Abs. 1 DSGVO, § 22 BDSG)¹⁶. Beim Aufbau des nationalen digitalen Gesundheitsnetzes – Teil dessen auch die eGK ist –, hat daher die Gewährleistung maximaler Daten- und Informationssicherheit sowie die Wahrung der informationellen Selbstbestimmung der Versicherten bei jedem Datenabruf und -austausch oberste Priorität.

Die Verfahren, die die Funktionen der eGK absichern, werden in regelmäßigen Abständen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet. Zur Gewährleistung eines konstant hohen Sicherheitsniveaus wird die eGK fortwährend weiterentwickelt und in einer neuen eGK-Kartengeneration ausgegeben (die Aufdrucke G2 und G2.1 kennzeichnen die aktuelle zweite Generation)¹⁷. Entsprechend der Einschätzung des BSI im

Hinblick auf die Sicherheit der Nutzung der eGK erster Generation erfolgte am 31. 12. 2018 deren Ungültigkeitserklärung. Die aktuelle eGK bedient sich einer anders gearteten Verschlüsselungstechnik, kann die Online-Überprüfung der Versichertenstammdaten protokollieren, ist mit einer kontaktlosen Schnittstelle (NFC, Near-Field-Communication) ausgestattet (§ 291 Abs. 3 S. 1 SGB V) sowie unterstützt neben neueren kryptographischen Verfahren auch medizinische Fachanwendungen.

Die TI-Plattform ist in eine zentrale und eine dezentrale Zone unterteilt. Die eGK ist Teil der dezentralen Zone, da sie von den Nutzern der TI eingesetzt wird¹⁸. Um zu gewährleisten, dass Versicherte (auch bei Verlust oder Diebstahl ihrer eGK vorab deren Sperrung) die Datenhoheit behalten, gilt bei der Nutzung der eGK grundsätzlich das Zwei-Schlüssel-Prinzip: ein Lesen der sensiblen Daten (d. h. aller Nicht-Verwaltungsdaten) auf der eGK ist genauso wie die Nutzung der digitalen Schlüssel nur möglich, authentifiziert sich der Heilberufler (in seiner Rolle als Arzt etc.) mit seinem elektronischen Heilberufsausweis (eHBA) direkt gegenüber der eGK des Versicherten (sog. Card-to-Card-Authentifizierung) (s. § 339 SGB V zu den Voraussetzungen für den Zugriff von Leistungserbringern und anderen zugriffsberechtigten Personen)¹⁹. Um – falls eingerichtet – die medizinischen Daten des Notfalldatenmanagement (NFDm) und des eMP auszulesen, ist – vorbehaltlich eines Notfalls oder des Abrufs einer Organspendeerklärung – darüber hinaus die Eingabe der Heilberufler- bzw. Versicherten-PIN erforderlich. Da jeder Datenzugriff inzwischen automatisch protokolliert wird, ist im Nachhinein nachzuvollziehen, wer wann auf welche Daten Zugriff hatte.

Vorgaben zum Einzug, der Sperrung und der weiteren Nutzung der eGK nach Krankenkassenwechsel sowie zu deren eGK enthält § 291c SGB V (zur Löschung von Daten siehe v. a. Abs. 3 i. V. mit § 334 Abs. 1 S. 1 Nr. 2–5 SGB V).

II. Maßgeblicher Ordnungsrahmen

Für die eGK und das für diese erforderliche Lichtbild gelten zuvorderst die Bestimmungen des SGB. Darüber hinaus ist – besonders bei der Auslegung und praktischen Anwen-

10) Entwurf eines Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GMG), BT-Dr. 15/1525, 46: § 291 Abs. 2 S. 1 SGB V-E.

11) Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz, GMG) v. 14. 11. 2003, BGBl. 2003 I, S. 2190; BT-Dr. 15/1525, 143.

12) Die Verwendung der eGK ist in Anhang 1 zu Anlage 4a BMV-Ä geregelt. In 1.2 heißt es: Der Arzt ist verpflichtet, die Identität des Versicherten [...] anhand der auf der [eGK] aufgetragenen Identitätsdaten (Lichtbild [...]) zu prüfen.

13) https://www.vdek.com/presse/daten/b_versicherte.html.

14) Trotz des Lichtbildes gilt die eGK nicht als amtlich gültiger Lichtbildausweis.

15) Zur Rechtmäßigkeit der Speicherung der Versicherungsnummer s. nur BSG, Urt. v. 20. 1. 2021 – B 1 KR 7/20 R –, juris, insb. Rdnr. 50; zum Versicherungsstammdatenmanagement *Schüttler*, jurisPR-MedizinR 8/2021, Anm. 3.

16) Das Lichtbild ist kein solches Gesundheitsdatum, wird also von den folgenden IT-sicherheitsrechtlichen Vorgaben nicht unmittelbar erfasst.

17) Zum Konformitätsnachweis bzw. Zertifizierungskonzept für die Karten der Generation G2 vgl. TR BSI TR-03106 und TR BSI TR-03144.

18) Ausführlich zur Sicherheitsarchitektur: gematik, Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur, Stand: Juni 2021, S. 12 ff.

19) Der eHBA enthält – als digitales Pendant zur handschriftlichen Unterschrift – eine qualifizierte elektronische Signatur, mit der der Heilberufler rechtsverbindlich versichert, Urheber der signierten Daten zu sein. Die Beantragung des HBA setzt den Nachweis der Berufsgruppenzugehörigkeit voraus.

der Normen durch die GKV – die Rechtsprechung der Gerichte der Sozialgerichtsbarkeit, bei Grundrechtsbezug zusätzlich die der Verfassungsgerichte, zu beachten.

Sowohl die kodifizierten Regelungen zur eGK als auch ihre praktische Anwendung stehen im Spannungsverhältnis zwischen den Interessen der Allgemeinheit an einer ausreichenden, zweckmäßigen und wirtschaftlichen sowie finanziell stabilen Versorgung der Versicherten einerseits und dem informationellen Selbstbestimmungsrecht derselben andererseits²⁰. Speziell die gesetzlich vorgesehenen Datenspeicherungen und –übermittlungen, die sich in der einzelnen Speicherungs- oder Übermittlungsmaßnahme aktualisieren, werfen in Anbetracht der tangierten datenschutzrechtlichen Belange „gewichtige verfassungsrechtliche Fragen“ auf²¹.

1. Datenverarbeitungsvorgänge im Zusammenhang mit der eGK

a. Datenverarbeitungen im Anwendungsbereich des SGB

Allgemeine Vorgaben die Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten betreffend sind in § 67b SGB X normiert. Für die Erhebung von Sozialdaten relevant ist § 67a SGB X. Absatz 1 der Norm erklärt die Erhebung von Sozialdaten durch die in § 35 SGB I genannten Stellen für zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem SGB erforderlich ist. Dasselbe gilt für die Erhebung der besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO.

Gemäß Erwägungsgrund (ErwG) 51 S. 3 DSGVO soll die Verarbeitung von Lichtbildern indes nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. An dieser Stelle sei vorweggenommen, dass das Lichtbild auf der eGK bereits nicht der Biometrie bedarf, jedenfalls aber mit Blick auf Größe und Qualität regelmäßig wohl nicht allein die eindeutige Identifizierung oder Authentifizierung des Karteninhabers erlaubt und zumindest unter diesen Voraussetzungen nicht Art. 9 Abs. 1 DSGVO unterfällt (auch nicht als Gesundheitsdatum, vgl. ErwG 35 DSGVO)²².

Ausweislich § 67a Abs. 1 S. 3 SGB X gilt § 22 Abs. 2 BDSG entsprechend (angemessene und spezifische Maßnahmen zur Wahrung der Betroffeneninteressen). Gemäß § 67c Abs. 1 SGB X ist die Speicherung, Veränderung oder Nutzung von Sozialdaten o. g. genannten Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden gesetzlichen Aufgaben nach dem SGB erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

In § 284 Abs. 1 S. 1 Nr. 2 SGB V (für das Lichtbild i. V. mit § 291a Abs. 5 SGB V) ist explizit geregelt, dass die Krankenkasse berechtigt ist, Sozialdaten zu erheben und zu speichern, soweit diese für die Ausstellung des Berechtigungsscheines und der eGK erforderlich sind. Gemäß der Legaldefinition in § 67 Abs. 2 S. 1 SGB X (Absatz 2 ergänzt gem. § 67 Abs. 1 SGB X die Begriffsbestimmungen der DSGVO) sind Sozialdaten personenbezogene Daten (i. S. d. Art. 4 Nr. 1 DSGVO), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB verarbeitet werden. Lichtbilder stellen Sozialdaten im Sinne der Norm dar, sodass die GKV zu ihrer Erhebung und Speicherung ausdrücklich ermächtigt wird.

b. Bereichsspezifische Regelungen nach §§ 284 ff. SGB V

Die Verarbeitung personenbezogener Daten im System der gesetzlichen Krankenversicherung ist detailliert in den

§§ 284 ff. SGB V geregelt. Mit der Einfügung des Kapitel 10 des SGB V intendierte der Gesetzgeber die Transparenz des Leistungsgeschehens zu verbessern sowie die Arbeit der Krankenkassen dank des Einsatzes elektronischer Datenverarbeitung zu erleichtern²³. Die bereichsspezifischen Regeln sollen ferner verhindern, dass durch das Sammeln und Auswerten personenbezogener Daten, namentlich aus der Datenzusammenführung von ärztlichen Abrechnungen, Leistungs- und Gesundheitsprofile (Stichwort „gläserner Patient“) erstellt werden²⁴. Besonders die normenklare Ausgestaltung der bereichsspezifischen Normen der §§ 291 ff. SGB V belegen, dass der Gesetzgeber im Falle der eGK und der TI (seit dem PDSG eigens geregelt in Kapitel 5 [§§ 306 ff. SGB V]) dem Sozialdatenschutz einschließlich der Datensicherheit in ganz besonderem Maße hohe Bedeutung beimisst²⁵.

Die eGK ist v. a. Gegenstand der § 15 und §§ 291–291c SGB V. Speziell § 291a SGB V enthält zentrale Zweckbestimmungen sowie datenschutzrechtliche Vorgaben zum Inhalt obligatorisch (Abs. 2) bzw. fakultativ (Abs. 3) zu speichernden Daten. Ebenfalls kodifiziert ist hier der Umgang mit den verpflichtenden Lichtbildern und die Art der Speicherung auf der Karte. Die Norm vereint somit Organisationsrecht und Datenschutzrecht.

Die Ausgabe der eGK ist in § 291 Abs. 1 SGB V normiert. Sie dient dem Versicherungsnachweis und der Abrechnung mit den Leistungserbringern, vgl. § 15 Abs. 2 S. 1, Abs. 6 SGB V. Eine Befreiungsmöglichkeit sieht § 15 Abs. 2 SGB V nicht vor. Mit der Nutzungspflicht korrespondiert laut SG Berlin ein Verweigerungsrecht der Krankenversicherung, einen anderen Berechtigungsnachweis auszustellen²⁶. Die in § 15 Abs. 2 SGB V statuierte Nutzungspflicht beschränke zwar die allgemeine Handlungsfreiheit der Versicherten. Dies sei aber durch das Interesse der Solidargemeinschaft (§ 1 SGB V) an der einheitlichen und effektiven Zusammenarbeit von Versicherten, Krankenkassen und Leistungserbringern sowie der wirtschaftlichen Abrechnung der Behandlungskosten gerechtfertigt.

c. Verhältnis von SGB, DSGVO und BDSG

Die Vorgaben der §§ 291 ff. SGB V liegen an der Schnittstelle bzw. im Regelungsgefüge des bereichsspezifischen Sozialdatenschutzes nach § 35 Abs. 1 SGB I und dem allgemeinem Datenschutzrecht nach der DSGVO bzw. dem BDSG.

Datenschutzrechtliche Grundlagen finden sich in der seit dem 25.5.2018 (Art. 99 Abs. 2 DSGVO) unmittelbar und auch im Bereich des Gesundheitsdatenschutz vorrangig geltenden DSGVO. So regelt etwa Art. 9 Abs. 2 lit. a DSGVO die Einwilligung in die Verarbeitung von Gesundheitsdaten. Regelungen zu Pflichtenwendungen der TI, d. h. solche, die der Verwaltung des Gesundheitssystems dienen und die Verarbeitung besonders geschützter Gesundheitsdaten unabhängig von der Einwilligung des betroffenen Versicherten erlauben, unterfallen Art. 9 Abs. 2 lit. h oder i DSGVO; Regeln zu freiwilligen Anwendungen sind hingegen unter Art. 9 Abs. 2 lit. a i. V. mit Abs. 4 DSGVO zu fassen²⁷.

20) *Schifferdecker*, in: KassKomm, 118. EL März 2022, § 291 SGB V, Rdnr. 10.

21) BVerfG, Beschl. v. 13.2.2006 – 1 BvR 1184/04 –, juris, Rdnr. 61.

22) Dazu, wann Lichtbilder biometrische Daten (Art. 4 Nr. 14 DSGVO) und damit gem. Art. 9 Abs. 1 DS-GVO zu den besonderen Kategorien personenbezogener Daten zählen s. ErwG 51 DSGVO. Weiterführend etwa *Schindler/Schneider*, ZD 2018, 463 zu Videodaten.

23) Vgl. BT-Dr. 11/2237, 235 f. und BT-Dr. 11/3480, S. 42 f.

24) BT-Dr. 11/2237, S. 235.

25) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 97 m. w. N., vgl. insb. BT-Dr. 19/18793, S. 2.

26) SG Berlin, Beschl. v. 7.11.2013 – S 81 KR 2176/13 ER –, juris, Rdnrn. 19 f.

27) *Schifferdecker*, in: KassKomm, 118. EL März 2022, § 291 SGB V, Rdnr. 18.

Ob die DSGVO im Rahmen der GKV unmittelbar Anwendung findet oder lediglich über die Auffangregelung des § 35 Abs. 2 S. 2 SGB I gilt, ließ das BSG dahinstehen²⁸. Fraglich ist es gleichwohl deshalb, weil die Festlegung der Gesundheitspolitik sowie die Organisation des Gesundheitswesens und die medizinische Versorgung Sache der Mitgliedstaaten ist (vgl. Art 168 Abs. 7 S. 1 und 2 AEUV) und die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt (vgl. Art 2 Abs. 2 lit. a DSGVO)²⁹.

Vorliegend bedurfte dies aus Sicht des BSG jedoch keiner Entscheidung. Denn die gesetzlichen Regelungen zur eGK und ihrer Einbeziehung in die TI stünden mit den Vorgaben der DSGVO auch dann in Einklang, wenn letztere unmittelbar anwendbar und damit als höherrangiges Recht anzusehen wäre: die Verarbeitung personenbezogener Daten im Zusammenhang mit der eGK nach Maßgabe der einschlägigen Vorschriften des SGB V sei durch die Ermächtigungen in Art. 6 Abs. 1 lit. c und e i. V. mit Abs. 3 DSGVO und – soweit besondere Kategorien von Daten i. S. v. Art. 9 Abs. 1 DSGVO betroffen sind – Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO gedeckt. Diese Regelungen seien auch mit den Vorgaben zur Gewährleistung von Datensicherheit (Art. 5 Abs. 1 lit. f, Art. 32, 35, 25 DSGVO) konform.

Im Verhältnis zum BDSG sind die Vorschriften der §§ 291 ff. SGB V jedenfalls *lex specialis*³⁰.

d. Exkurs: Datenschutzrechtliche Verantwortlichkeit

Werden Sozialdaten von einem Leistungsträger i. S. d. § 12 SGB I verarbeitet, ist der i. S. d. Art. 4 Nr. 7 DSGVO Verantwortliche – und damit der primäre Normadressat der datenschutzrechtlichen Regelung – der Leistungsträger (§ 67 Abs. 4 S. 1 SGB X). Ihm obliegt es dafür Sorge zu tragen, dass alle datenschutzrechtlichen Pflichten eingehalten werden, insbesondere, dass sämtliche Sozialdaten rechtskonform verarbeitet werden; ferner hat er die Pflicht, alle erforderlichen Maßnahmen zur Wahrung des in § 35 Abs. 1 SGB I statuierten Sozialgeheimnisses zu ergreifen. Die gesetzlichen Krankenkassen sind Leistungsträger und damit Verantwortliche in diesem Sinne (s. § 21 Abs. 2 SGB I)³¹.

Dasselbe ergibt sich mit Blick auf das verbindliche Sicherheitskonzept (als Dokumentation der Anwendung der einheitlichen Methoden der Informationssicherheit der TI) der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)³², wonach den Krankenkassen als Herausgeber der eGK die Einhaltung der gesetzlichen (nationaler und europäischer) Vorgaben, der Spezifikationen der gematik³³ sowie die Berücksichtigung der Anforderungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in eigener Verantwortung obliegt³⁴.

III. Datenschutz- und Verfassungskonformität der einschlägigen Regelungen der §§ 284 ff. SGB V

Bevor auf sich im Rahmen der Anwendung der §§ 284 ff. bzw. 291 ff. SGB V auftretende Detailfragen eingegangen werden kann, sind die insoweit einschlägigen Vorgaben der §§ 284 ff. SGB V auf ihre Vereinbarkeit mit höherrangigem Recht hin zu prüfen (auf die ggf. ebenfalls einschlägigen §§ 334 ff. SGB V wird nachstehend nicht eingegangen).

Ob auf Sachverhalte wie die vorliegend diskutierten die Grundrechte des Grundgesetzes oder diejenigen der GRCh Anwendung finden, kann – so das BSG mit Urteil vom 20.1.2021 – dahingestellt bleiben, denn der in der Obliegenheit zur Nutzung der eGK und der Verarbeitung der damit zusammenhängenden personenbezogenen Daten der Versicherten liegende Grundrechtseingriff sei sowohl am Maßstab des nationalen Grundrechts auf informationelle

Selbstbestimmung als auch am Maßstab der Art. 7 und 8 GRCh gerechtfertigt³⁵.

Nach gefestigter Rechtsprechung des BSG³⁶ begegnen die §§ 284 ff. SGB V keinen datenschutzrechtlichen Bedenken. Die durch das PDSG neu gefassten Regelungen des SGB V zur eGK (und zur TI) verfügten über ausreichende Vorkehrungen zur Gewährleistung einer angemessenen Datensicherheit. Die mit dem PDSG neu gefassten und inhaltlich überarbeiteten §§ 291 ff. SGB V enthielten ein hinreichend normdichtes und klares Regelungsgefüge, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiellrechtlicher, organisatorischer und prozeduraler Maßnahmen der Datensicherheit diene, der der Gesetzgeber beim Auf- und Ausbau der TI eine „herausragende Rolle“ beimessen³⁷. Der Gesetzgeber sei sich bewusst gewesen, dass im Rahmen der TI besonders sensible Gesundheitsdaten verarbeitet werden, die im Interesse der Versicherten und der Leistungserbringer als Berufsgeheimnisträger besonders schutzbedürftig sind³⁸.

Die nachstehenden Erwägungen des BSG beziehen sich im Wesentlichen auf die eGK als solche (teils i. V. mit der TI), für das Fotoerfordernis sind die Ausführungen – ob dessen mittelbarer Betroffenheit – indes nicht minder relevant.

1. Grundrecht auf informationelle Selbstbestimmung

a. Verpflichtende Datenverarbeitung

§§ 291 ff. SGB V sehen eine einverständnisunabhängige Datenverarbeitung und damit grundsätzlich einen Eingriff in das Recht auf informationelle Selbstbestimmung als eine Ausprägung des allgemeinen Persönlichkeitsrechts vor.

Das BSG führte eingehend aus, dass die bestehende gesetzliche Obliegenheit zur Nutzung der eGK gemäß § 15 Abs. 2, §§ 291 bis 291b SGB V und die Verarbeitung der damit im Zusammenhang stehenden personenbezogenen Daten zwar einen Eingriff in das Grundrecht der Versicherten auf informationelle Selbstbestimmung begründe, diese jedoch nicht in ihren Grundrechten verletze, denn der in der Obliegenheit zur Nutzung der eGK liegende Grundrechtseingriff sei sowohl am Maßstab des nationalen Grundrechts auf informationelle Selbstbestimmung, als auch am Maßstab der durch die Art. 7 und 8 GRCh garan-

28) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnrn. 25 ff.

29) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnrn. 28 ff. Vgl. BSG, Urt. v. 18.12.2018 – B 1 KR 31/17 R –, BSG, Urt. v. 18.12.2018 – B 1 KR 40/17 R –.

30) BSG, Urt. v. 18.11.2014 – B 1 KR 35/13 R –, juris, Rdnr. 15 (noch vor Geltung der DS-GVO).

31) S. ebenfalls § 341 Abs. 4, 358 Abs. 5 und § 307 SGB V. Zum Ganzen *Hornung*, in: *Hänlein/Schuler*, SGB V, 6. Aufl. 2022, § 307, Rdnrn. 1 ff.

32) Diese ist gesetzlich für die Einführung und den Betrieb der TI sowie die Sicherstellung von Datenschutz und Datensicherheit in der TI zuständig.

33) Insb. gematik, Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter, Version 1.3.0., Stand: 12.11.2020 (dort v. a. S. 11).

34) Vgl. gematik, Übergreifendes Sicherheitskonzept der Telematikinfrastruktur, Anhang E, Version 2.4.0., 5.9.2008, S. 15.

35) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 90. Zustimmung *Beyer*, *WzS* 2022, 57. Zu den Konsequenzen hieraus für die Nutzung digitaler Anwendungsmöglichkeiten im Gesundheitswesen *Bieresborn*, *JM* 2022, 113.

36) Zuletzt BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R und B 1 KR 15/20 R –, jew., juris. Dazu *Müller*, *NZS* 2022, 591.

37) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 1004. s. bereits BSG, Urt. v. 18.11.2014 – B 1 KR 35/13 R –, juris, Rdnr. 34. *Kühling/Seidel* in: *Kingreen/Kühling*, *Gesundheitsdatenschutzrecht*, 2015, S. 181.

38) Vgl. BT-Dr. 19/18793, 2.

tierten Grundrechte auf Achtung des Privatlebens und auf Schutz der personenbezogenen Daten gerechtfertigt³⁹.

Die gesetzliche Konzeption gewährte auch die von Verfassungen wegen gebotene (faktische) Datensicherheit⁴⁰. Versicherte würden nicht in ihren Grundrechten dadurch verletzt, dass ihnen kein anderer Weg eröffnet werde, als durch Nutzung der eGK ihre Berechtigung zur Inanspruchnahme von Leistungen nachzuweisen und die Abrechnung der Krankenkassen mit den Leistungserbringern zu ermöglichen⁴¹.

Aus § 15 Abs. 2 und §§ 284, 291, 291a, 291b SGB V i. V. mit § 25 Abs. 2 S. 1 SGB I, § 67a Abs. 1 und § 67b Abs. 1 SGB X, die die Beschränkungen des Rechts auf informationelle Selbstbestimmung einfachgesetzlich für die eGK regeln, ergäben sich Voraussetzungen und Umfang der Beschränkungen klar erkennbar⁴². Die Regelungen entsprechen daher dem rechtsstaatlichen Gebot der Normenklarheit. Zweifel, welche Angaben von wem zu welchem Zweck verarbeitet werden dürften, bestünden nicht.

Dasselbe gelte für § 291a Abs. 3 Nr. 4 SGB V, der die Speicherung weiterer Angaben auf der eGK erlaube, soweit deren Verarbeitung zur Erfüllung von Aufgaben erforderlich ist, die den Krankenkassen gesetzlich zugewiesen sind⁴³. Insoweit habe der Gesetzgeber die Regelungsbefugnis unter klarer Begrenzung von Inhalt, Zweck und Ausmaß der Ermächtigung (zur bundesweiten Verwendung der eGK „als Versicherungsnachweis“ und soweit die Verarbeitung der Daten zur Erfüllung der den Kassen gesetzlich zugewiesenen Aufgaben erforderlich ist) verfassungskonform gem. § 291b Abs. 6 SGB V auf die Vertragspartner der gemeinsamen Selbstverwaltung auf Bundesebene übertragen, § 87 Abs. 1 SGB V. Diese seien bei der Ausübung ihrer Regelungskompetenz ihrerseits den Geboten der Normenklarheit, der Bestimmtheit und der Verhältnismäßigkeit verpflichtet.

Im Ergebnis sei der auf hinreichende Rechtsgrundlagen gestützte Grundrechtseingriff in Form der Beschränkungen des Rechts auf informationelle Selbstbestimmung durch die Regelungen über die eGK durch überwiegende Allgemeininteressen gerechtfertigt⁴⁴. Denn diese seien zur Verhinderung von Missbrauch und zur Kosteneinsparung zwecks Erhalts der finanziellen Stabilität der gesetzlichen Krankenversicherung geeignet, erforderlich und angemessen. Durch die speziellen datenschutzrechtlichen Rechtsbehelfe nach Art. 77 ff. DSGVO i. V. mit §§ 81 ff. SGB X sei auch die effektive Kontrolle der Einhaltung des Datenschutzrechts durch die Gerichte gewährleistet.

b. Freiwillige Anwendungen der TI

Weil die Nutzung der freiwilligen Anwendungen der TI die (jederzeit zu widerrufende) Einwilligung des Versicherten voraussetzt (§ 291a Abs. 3 S. 3 und 4 SGB V), liegt kein Eingriff in das informationelle Selbstbestimmungsrecht vor. Allein die eröffnete Möglichkeit zur Nutzung freiwilliger Anwendungen nach Einwilligung, bedeutet keine Beschwer von Versicherten, die nicht einwilligen⁴⁵. Anhaltspunkte, dass der Versicherte trotz Fehlens seiner Einwilligung zum „gläsernen Patienten“ wird, sieht das LSG Baden-Württemberg mit überzeugender Begründung nicht⁴⁶.

Die Frage nach einem faktischen Einwilligungszwang aus einem Konformitätsdruck und grundrechtsrelevanten Auswirkungen eines solchen, stellt sich noch nicht⁴⁷.

2. Art. 7 und 8 GRCh

Als Beurteilungsmaßstab zu erwägen sind ferner Art. 7 und 8 GRCh, da der Anwendungsbereich der DSGVO eröffnet ist, mithin die Durchführung von Unionsrecht durch die Mitgliedstaaten in Rede steht. Das BSG sprach sich für die Vereinbarkeit des Fotoerfordernisses mit Art. 7 und 8 GRCh aus⁴⁸.

Insoweit führte es aus, dass Art. 6 Abs. 1 lit. c und e DSGVO, die selbst noch keine Rechtsgrundlage für die Verarbeitung darstellen (vgl. Art. 6 Abs. 3 S. 1 DSGVO), sondern eine den Anforderungen des Abs. 3 genügende Rechtsvorschrift im Unionsrecht oder Recht des Mitgliedstaats voraussetzen, die eine rechtliche Verarbeitungspflicht bzw. die hoheitliche Verarbeitungsbefugnis auslöst, mit dem in Art. 8 Abs. 2 S. 1 und Art. 52 Abs. 1 S. 1 GRCh sowie Art. 8 Abs. 2 EMRK verankerten Grundsatz, dass es für jede Beschränkung des Grundrechts auf Datenschutz einer gesetzlichen Grundlage bedarf, vereinbar sind⁴⁹. Der nationale Gesetzgeber, der hinsichtlich der mit der eGK verbundenen Datenverarbeitung insoweit § 35 Abs. 2 S. 1 SGB I, § 67a Abs. 1 und § 67b Abs. 1 SGB X, § 15 Abs. 2 und §§ 284, 291, 291a, 291b SGB V geschaffen hat, wahrt damit aus Sicht des BSG – wie von Art. 52 Abs. 1 S. 2 GRCh gefordert (vgl. Art. 6 Abs. 3 S. 4 DSGVO) – den Grundsatz der Verhältnismäßigkeit, nachdem ihnen ein „ausgewogenes Konzept“ zugrunde liegt, das die Verarbeitung personenbezogener Daten auf das zur Erreichung der verfolgten (legitimen) Ziele – wie vom EuGH gefordert⁵⁰ – zwingend erforderliche Maß beschränkt und die Persönlichkeitsrechte der Versicherten schützt⁵¹. Die frühere Krankenversicherungskarte ohne Lichtbild (als zu erwägendes milderes Mittel) wies ein erhebliches Missbrauchspotential auf, das deutlich höher war als jenes der eGK; die flankierende Vorlage des Personalausweises scheidet als gleich geeignetes milderes Mittel zur Missbrauchsverhinderung aus⁵². Auch beschränke das Lichtbilderfordernis die Versicherten in ihrem Recht aus Art. 8 GRCh nur relativ geringfügig, zumal diese auch die alleinige Verfügungsgewalt über das auf der eGK aufgebrachte – nicht im Chip gespeicherte – Lichtbild haben⁵³. Dagegen würden die zu erwartenden Vorteile für die Missbrauchsabwehr und Wirtschaftlichkeit der vertragsärztlichen Versorgung schwer wiegen. Die mit den genannten Funktionen zu erwartende Sicherung der finanziellen Stabilität der GKV sei ein überragend wichtiges Gemeinschaftsgut, ein Gemeinwohlbelang von derart hoher Bedeutung, dass Maßnahmen, die ihr zu dienen bestimmt sind, auch dann gerechtfertigt sein können, wenn sie für die Betroffenen zu fühlbaren Einschränkungen führen⁵⁴.

39) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnrn. 90 ff.

40) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 92.

41) BSG, Urt. v. 18.11.2014 – B 1 KR 35/13 R –, juris, Rdnrn. 23 ff.; zustimmend *Schifferdecker*, in: KassKomm, 118. EL März 2022, § 291a, Rdnrn. 14 ff.

42) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 95 m. w. N.

43) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 96 m. w. N.

44) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnrn. 98 f.

45) LSG Bad.-Württ., Beschl. v. 30.11.2012 – L 11 KR 4746/12 ER-B –, juris; Hess. LSG, Urt. v. 26.9.2013 – L 1 KR 50/13 –, juris.

46) LSG Bad.-Württ., Urt. v. 21.6.2016 – L 11 KR 2510/15 –, juris, Rdnr. 38.

47) *Schifferdecker*, in: KassKomm, 118. EL März 2022, § 291 SGB V, Rdnr. 16. *Dochow*, WzS 2015, 137, 140 f.

48) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 50 m. w. N.

49) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 32 m. w. N.

50) Vgl. nur EuGH, Urt. v. 16.12.2008 – C-73/07 –, juris, Rdnr. 56 – *Satakunnan Markkinapörssi und Satamedia*.

51) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnrn. 47 ff. m. w. N.

52) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 51 m. w. N.

53) BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R –, juris, Rdnr. 52 m. w. N. Abgesehen davon, dass dieses bei den Kassen gespeichert wird, § 291a Abs. 6 SGB V.

54) Vgl. nur BVerfG, Beschl. v. 14.5.1985 – 1 BvR 449/82 – BVerfGE 70, 1, 30.

3. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Jedenfalls für das Lichtbild ist – schon mangels Eröffnung des Schutzbereichs – eine Verletzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht)⁵⁵ abzulehnen, denn dieses wird lediglich auf die eGK abgedruckt, nicht aber auf dieser elektronisch gespeichert (die Speicherung erfolgt (de-)zentral bei der jeweiligen Krankenkasse).

Hingegen fällt der Chip der Karte – hierauf sei an dieser Stelle kurz hingewiesen – technisch zwar in den Anwendungsbereich des IT-Grundrechts. Damit der Schutzbereich eröffnet ist, müsste auf Seiten der Versicherten jedoch eine begründete Vertraulichkeitserwartung vorherrschen. Denn eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht nach dem BVerfG nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt⁵⁶. Ob und inwieweit dies bei der eGK der Fall ist, muss mit Rücksicht auf das gesetzlich statuierte Verarbeitungsrecht der Krankenkassen beurteilt werden, wobei auch die ausgeweiteten selbständigen Zugriffsbefugnisse des Versicherten nicht unberücksichtigt bleiben dürfen.

Der Beitrag wird mit Teil II in Heft 12 fortgesetzt.

Open Access. Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Open Access funding enabled and organized by Projekt DEAL.

55) Grundlegend BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07 –, BVerfGE 120, 274 – Online-Durchsuchung.

56) BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07 –, juris, Rdnr. 206.

Enhancement mit Gehirnorganoiden – Ethische und rechtliche Probleme einer *terra nova*

Hannes Wolff und Jana Pecikiewicz*

Enhancement – ein Begriff, der zwar im Alltag noch nicht in aller Munde ist, aber dennoch seit geraumer Zeit große Beachtung in der Wissenschaft findet. Übersetzt bedeutet Enhancement „Steigerung“ oder „Verbesserung“ und setzt dort an, wo Behandlungen über das medizinisch Notwendige hinausgehen.

Enhancement ist umstritten, denn so sehr es in das Zeitalter der Selbstoptimierung passt, so sehr stellt es die Grenzen dessen, was (wissenschaftlich-technisch) möglich ist und was (ethisch-rechtlich) möglich sein darf, in Frage und hat damit das Potential, die Gesellschaft zu spalten. Noch kontroverser wird die Lage, wenn Enhancement zukünftig mit Hilfe sog. Gehirnorganoiden stattfindet, was jedenfalls denkbar ist.

Wo neue Grenzen ausgelotet werden, ist es umso wichtiger, einen rechtlich verbindlichen Rahmen unter Beachtung ethischer Gesichtspunkte zu schaffen. Dafür soll der vorliegende Aufsatz Impulse geben.

Nach einer Definition der wichtigsten Begriffe (I.) zeigt der Beitrag den naturwissenschaftlichen Forschungs- und

Entwicklungsstand von Gehirnorganoiden und einem Enhancement mit diesen auf (II.). Danach werden die ethischen Probleme diskutiert, die sich hinsichtlich Gehirnorganoiden und deren Nutzung ergeben (III.). Zuletzt werden solche Behandlungseingriffe mit Gehirnorganoiden, die neben einer therapeutischen auch eine enhancende Wirkung haben, aus rechtlicher Sicht betrachtet. Dafür wird u. a. auf Fragen der rechtlichen Einordnung von Gehirnorganoiden, arzneimittelzulassungsrechtliche Fragen, Einwilligungsfragen und sozialversicherungsrechtliche Aspekte eingegangen (IV.).

I. Begriffliche Grundlagen

1. Gehirnorganoid

Organoid sind aus Stammzellen¹ *in vitro* geschaffene Zellgebilde, die durch ihre räumliche Organisation ein *in vivo*

Hannes Wolff, wissenschaftlicher Mitarbeiter und Doktorand, Lehrstuhl für Staats- und Verwaltungsrecht, Völkerrecht, Internationales und Europäisches Wirtschaftsrecht von Prof. Dr. iur. Hans-Georg Dederer, Universität Passau, Passau, Deutschland

Jana Pecikiewicz, studentische Hilfskraft, Lehrstuhl für Staats- und Verwaltungsrecht, Völkerrecht, Internationales und Europäisches Wirtschaftsrecht von Prof. Dr. iur. Hans-Georg Dederer, Universität Passau, Passau, Deutschland

*) Gefördert vom Bayerischen Staatsministerium für Wissenschaft und Kunst im Rahmen des Bayerischen Forschungsverbundes „ForInter – Interaktion humaner Gehirnzellen“. Wir bedanken uns bei Prof. Dederer für hilfreiche Kommentare und Anregungen und bei Gregor Frenken für nicht nur eine erhellende Diskussion über die Feinheiten des Arzneimittelrechts.

1) Für die Herstellung von Gehirnorganoiden wird auf induziert pluripotente Stammzellen (iPSZ) zurückgegriffen. Sie unterscheiden sich von den früher nur verfügbaren humanen embryonalen Stammzellen (hESZ) dadurch, dass sie ohne Rückgriff auf Embryonen durch Entdifferenzierung menschlicher somatischer Körperzellen gewonnen werden können. Zur historischen Entwicklung von iPSZ ausführlich *Faltus*, Stammzellenreprogrammierung, 2016, 130 ff.