AUFSÄTZE

https://doi.org/10.1007/s00350-020-5725-6

Das Patienten-Datenschutz-Gesetz (Teil 1): Die elektronische Gesundheitskarte und Telematikinfrastruktur

Carsten Dochow*

Der Beitrag gibt einen Überblick über die Neustrukturierung der Regelungen zur Telematikinfrastruktur des Gesundheitswesens (I.) und geht auf die elektronische Gesundheitskarte (II.), die rechtlichen Bestimmungen zur Telematikinfrastruktur im Allgemeinen (III.) und der elektronischen Patientenakte im Besonderen (IV.) ein, bevor die erweiterten Datenverarbeitungsbefugnisse der Krankenkassen (V.), die Datenspende (VI.) und weitere Änderungen (VII.) betrachtet werden. Intensiver setzt sich der Beitrag mit dem datenschutzrechtlichen Verantwortlichkeitskonzept (III., 2.) und der Datenspende auseinander.

I. Einführung und Überblick

Am 15.10.2020 ist das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, kurz: Patienten-Datenschutz-Gesetz (PDSG) in Kraft getreten[1]. Dem Referentenentwurf v. 4.2.2020 folgte der Gesetzentwurf der Bundesregierung v. 27.4.2020[2], dessen Anhörung am 27.5.2020 im Bundestag[3] stattfand. Das PDSG wurde am 3.7.2020 vom Deutschen Bundestag verabschiedet. Der Bundesrat befasste sich am 18.9.2020 mit dem Gesetz und hat den Vermittlungsausschuss nicht angerufen, obwohl der Bundesbeauftragte für den Datenschutz (BfDI) im Vorfeld erhebliche Kritik am Gesetz äußerte[4]. Ungeachtet dessen verfolgt das Gesetz ein gesellschaftlich und wirtschaftlich bedeutsames Anliegen: Mehr als 15 Jahre nach dem ersten Vorstoß mit dem GMG[5], die papierbasierte Kommunikation durch elektronische Verfahren abzulösen, versucht das Artikel-Gesetz der Digitalisierung im Gesundheitswesen[6] neuen Schub zu verleihen. Zwar urteilte kürzlich das OLG Karlsruhe noch, dass die postalische Übersendung eines Arztbriefs das gängige Mittel zur Aufrechterhaltung des Informationsflusses zwischen den an der Behandlung beteiligten Ärzten sei[7]. Zudem ist Deutschland im Bereich der Digitalisierung des Gesundheitswesens in internationalen Vergleichen stets auf die hinteren Plätze verwiesen[8]. Generell bedürfen Abläufe in der Gesundheitsversorgung aus Gründen der Effizienz und im Interesse der Verbesserung der Versorgung daher schnellstmöglich einer digitalen Durchdringung. Gerade die Pandemie mit dem neuartigen Coronavirus SARS-CoV-2 hatte jüngst noch einmal eindrücklich aufgezeigt, welche Bedeutung telematischen Verfahren zukommen kann, wenn direkte menschliche Kontakte nur eingeschränkt möglich sind. Dabei ist es sogar gelungen, in kurzer Zeit eine funktionierende Corona-Warn-App zur Kontaktverfolgung zur Verfügung zu stellen[9].

Das Ziel des PDSG ist einerseits eine verbesserte Nutzung der Ressourcen durch Einsparungen mithilfe der elektronischen Patientenakte, z.B. durch eine Vermeidung von Doppeluntersuchungen und Fehlverordnungen aufgrund einer verbesserten Kommunikation. Es will andererseits den Wandel der Strukturen der Gesundheitsversorgung in Ansehung der digitalen Transformation einleiten[10] und ist bestrebt, die Voraussetzungen für eine sichere und vertrauensvolle Kommunikation im Gesundheitswesen mit der Telematikinfrastruktur (TI) als „Datenautobahn des Gesundheitswesens“[11] fortzuschreiben.

Eine umfassende Neuregelung ist damit nicht verbunden. Ohne hier eine vollständige Gegenüberstellung der alten und neuen Vorschriften abzubilden, fällt auf, dass ein größerer Teil der bisherigen Regelungen (§§ 291 ff. SGB V a.F.) in den neuen Normenbestand übernommen, neu sortiert und punktuell modifiziert wird. Es findet sich etwa das wichtige Verlangens- und Benachteiligungsverbot[12] wieder. Eine gänzlich neue Regelung ist auch das nun umfassend ausgestaltete „Zugriffsrecht“ des Versicherten[13] nicht. Insoweit ist keine grundlegend neue Ausrichtung des Rechtskonzepts zu verzeichnen, sondern weiterhin werden, wie schon durch ehealth-Gesetz[14], TSVG[15], GSAV[16] und DVG[17], vereinzelte Anpassungen vorgenommen.

1. Neustrukturierung der Regelungen zur Gesundheitstelematik

Die bisherigen Vorschriften zur Gesundheitstelematik, die vor allem in den §§ 291a bis 291h SGB V a.F. zu finden waren[18], werden neu strukturiert. Die Regelungen zur

Dr. iur. Carsten Dochow,
Referent in der Rechtsabteilung der Bundesärztekammer, Berlin, Deutschland

*) Es wird hier ausschließlich die persönliche Auffassung des Verfassers wiedergegeben.
1) Verkündet am 14.10.2020, BGBl. I S. 2115.
2) BT-Dr. 19/18793.
3) S. bundestag.de/ausschuesse/a14/anhoerungen/27-05-2020-pdsg-693222 (alle Links im Beitrag abgerufen am 30.9.2020).
4) S. Pressemitteilung BfDI, DuD 2020, 640.
5) Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) v. 14.11.2003 (BGBl. I S. 2190).
6) S.z.B. *Katzenmeier*, MedR 2019, 259 ff.
7) OLG Karlsruhe, Urt. v. 11.3.2020 – 7 U 10/19.
8) *Bertelsmann Stiftung*, #SmartHealthSystems, Digitalisierungsstrategien im internationalen Vergleich, 2018; s.a. Digital-Health-Index, s.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2018/november/digitale-gesundheit-deutschland-hinkt-hinterher.
9) Lobend *Gottberg*, E-HealthCOM 5/2020, S. 33; s. dazu auch *Dochow*, GuP 2020, 129 ff. m.w.N.
10) BT-Dr. 19/18793, S. 1, 5; BT-Dr. 19/20708, S. 6.
11) BT-Dr. 19/18793, S. 1, 80.
12) S. dazu III., 6.
13) S. § 336 SGB V, s. dazu III., 7.
14) Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) v. 21.12.2015 (BGBl. I S. 2408), s. dazu *Buchner*, MedR 2016, 660 ff.
15) Terminservice- und Versorgungsgesetz (TSVG) v. 6.5.2019 (BGBl. I S. 646).
16) Gesetz für mehr Sicherheit in der Arzneimittelversorgung v. 9.8.2019 (BGBl. I S. 1202).
17) Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) v. 9.12.2019 (BGBl. I S. 2562), BT-Dr. 19/13438.
18) Ausf. *Dochow*, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen (im Folgenden: Telematik im Gesundheitswesen), 2017, S. 987 ff.

elektronischen Gesundheitskarte[19] (eGK) als Berechtigungsnachweis und als Mittel zur Abrechnung im Rahmen der vertragsärztlichen Versorgung (§§ 291a – 291c SGB V) verbleiben im 10. Kapitel des SGB V.

Es wird hingegen ein vollständig neues 11. Kapitel für die Telematikinfrastruktur (TI) eingefügt (§§ 306 –383 SGB V). Dieses enthält einen 1. Abschnitt zu den Anforderungen an die TI (§§ 306–309 SGB V), wobei u. a. die TI definiert und datenschutzrechtliche Verantwortlichkeiten festgelegt werden. Im 2. Abschnitt zur Gesellschaft für Telematik (§§ 310–322 SGB V)[20] werden u. a. deren Aufgaben, Verfassung, die Finanzierung[21] sowie weitere organisatorische Aspekte[22] geregelt. Ferner findet sich ein 3. Abschnitt zum Betrieb der TI (§§ 323–328 SGB V) und ein 4. Abschnitt zur Überwachung von Funktionsfähigkeit und Sicherheit (§§ 329–333 SGB V).

Zentral für die Funktionalitäten der TI ist der 5. Abschnitt zu den Anwendungen der TI (§§ 334–363 SGB V), der neben allgemeinen Vorschriften zu Anwendungen, einem Diskriminierungsverbot und Zugriffsrechten der Versicherten (§§ 334–340 SGB V) unter anderem die maßgeblichen Regelungen für die elektronische Patientenakte (ePA) enthält (§§ 341–355 SGB V). Ferner sind in diesem Abschnitt die Zugriffsrechte auf weitere Anwendungen für persönliche Erklärungen (§§ 356 f. SGB V), Bestimmungen zum elektronischen Medikationsplan (eMP) und zu den elektronischen Notfalldaten (NFD) (§§ 358 f. SGB V) sowie Regelungen für elektronische Verordnungen (§§ 360 f. SGB V) enthalten. Zuletzt unterfallen diesem Abschnitt Regelungen zur Nutzung der Anwendungen der TI in der privaten Krankenversicherung (§ 362 SGB V) und zur Verfügbarkeit von Daten aus Anwendungen der TI für Forschungszwecke (§ 363 SGB V).

In einem 6. Abschnitt werden ohne inhaltliche Änderungen die Vorgaben für Vereinbarungen zu „Telemedizinischen Verfahren" (z. B. Telekonsile oder Videosprechstunden)[23] geregelt (§§ 364–370 SGB V)[24], der 7. Abschnitt regelt die Anforderungen an Schnittstellen in informationstechnischen Systemen (§§ 371–375 SGB V) und die Bestimmungen zur Finanzierung und Kostenerstattung befinden sich im letzten 8. Abschnitt (§§ 376–383 SGB V). Das 12. Kapitel enthält die bekannten Bestimmungen für die Interoperabilität (§§ 384–393 SGB V)[25]. Die bisherigen Straf- und Bußgeldvorschriften[26], die sich teilweise auf Regelungen zur TI beziehen, werden nun in §§ 394–397 SGB V geregelt.

Die neue Struktur löst die bisherige bloße Aneinanderreihung und bisherige Fortschreibung der §§ 291a ff. SGB V a. F. ab und verleiht eine übersichtlichere Struktur. Die neue Sortierung stellt noch deutlicher die hohe Komplexität heraus, welche das Vorhaben der Gesundheitstelematik mit sich bringt. Der Umfang des Normbestandes wird noch einmal erhöht, was z. B. mit der differenzierten Festlegung der Zugriffsrechte je Anwendung zusammenhängt. Inwieweit künftige Gesetzesänderungen die alte Unübersichtlichkeit wiederherstellen, bleibt abzuwarten.

2. Rechtssystematische Einordnung: Neues Datenschutzgesetz im Gesundheitsbereich?

Das Artikelgesetz mit dem aus Datenschutzsicht vielversprechenden Kurztitel „Patienten-Datenschutz-Gesetz" (PSDG) führt auch nicht zu grundlegenden Neuregelungen des Patientendatenschutzes. Es bleibt bei dem Regelungsgefüge im Bereich des Gesundheitsdatenschutzrechts, das durch die DSGVO, Regelungen im BDSG oder in Landesdatenschutzgesetzen sowie bereichsspezifischen Gesetzen gekennzeichnet ist. Vorschriften, die durch das PDSG erlassen werden und datenschutzrechtlichen Regelungsgehalt aufweisen, gehören überwiegend zu den bereichsspezifischen Datenschutznormen. Soweit Anwendungen der TI als Pflichtanwendungen dezidiert der Verwaltung des Gesundheitssystems dienen und insoweit unabhängig von der Einwilligung des Versicherten eine Datenverarbeitung erlauben, können die Regelungen auf Art. 9 Abs. 2 lit. h oder lit. i DSGVO gestützt werden[27]. Die Regelungen zu den freiwilligen Anwendungen werden unter Art. 9 Abs. 2 lit. a i. V. mit Abs. 4 DSGVO zu fassen sein[28].

Nach hier vertretener Auffassung handelt es sich bei den Regelungen nicht durchweg um solche des Sozialdatenschutzrechts[29]. Verpflichtet auf das Sozialgeheimnis sind gem. § 35 Abs. 1 SGB V vor allem die Leistungsträger (z. B. Krankenkassen) und deren Auftragsverarbeiter[30]. Das greift § 67 Abs. 2 SGB X auf, der definiert, dass Sozialdaten personenbezogene Daten sind, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB V verarbeitet werden. Leistungserbringer werden nach überwiegender Auffassung nicht zur Wahrung des Sozialgeheimnisses verpflichtet[31]. Soweit mit den Regelungen zur eGK und TI Datenverarbeitungsvorschriften konstituiert werden, welche Leistungserbringer (z. B. Vertragsärzte) oder andere Personen adressieren, handelt es sich um bereichsspezifisches Gesundheitsdatenschutzrecht, das im entsprechenden „Fachgesetz" geregelt wird. Im Übrigen unterliegen viele Leistungserbringer daneben der Pflicht zur Wahrung des Berufsgeheimnisses[32]. Ein umfassender Rechtsrahmen der Gesundheitstelematik ist mit dem PDSG ebenfalls nicht geschaffen[33]. Es bestehen z. B. noch Unklarheiten, wenn jenseits des GKV-Systems zum Beispiel eine Einbindung von Behandelnden erfolgen soll (z. B. ausschließlich privatärztlich tätige Ärzte), auch wenn die Nutzung der eGK für Versicherte von Unternehmen der privaten Krankenversicherung weiterhin möglich ist (§ 362 SGB V[34]).

Im Übrigen ist das PDSG kein reines „Datenschutzgesetz", soweit es in weiten Teilen im Interesse einer zügigen Digitalisierung Vorschriften zur Vergütung von Leistungen und organisatorische Regelungen zur TI enthält[35]. Als Anreize sind etwa Vergütungen für die Unterstützung der Versicherten bei der Nutzung der ePA, bei deren Befüllung im aktuellen Behandlungskontext sowie für weitere Datenverarbeitungstätigkeiten von Leistungserbringern zur Aktualisierung von

19) S. *Dochow/Kreitz*, ZfmE 2018, 147 ff.; *Dochow*, WzS 2015, 104 ff. und 137 ff.
20) Bisher v. a. § 291b SGB V a. F.
21) §§ 310–316 SGB V.
22) Beirat (§§ 317 f. SGB V), Schlichtungsstelle (§§ 319 ff. SGB V).
23) Zu Änderungen mit dem DVG s. *Weyd*, MedR 2020, 183, 192; s. a. *Dochow*, MedR 2019, 636 ff.; zu Videosprechstunden *Hahn*, NZS 2020, 281 ff.
24) Bisher teilw. in § 291g SGB V a. F.
25) Bisher z. B. § 291e SGB V a. F.
26) §§ 306–307b SGB V a. F.
27) Art. 9 Abs. 2 lit. h DSGVO i. V. mit § 291, § 291a Abs. 2 und Abs. 3 SGB V n. F. bzgl. Versichertenstammdaten.
28) So zu den Vorgängernormen *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1195, 1312, 1327.
29) Zu §§ 291a ff. SGB V a. F. *Dochow*, WzS 2015, 104, 107; *Dochow/Kreitz*, ZfmE 2018, 147, 152; zust. *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, § 291a SGB V, Rdnr. 18; a. A. BSG, Urt. v. 18. 11. 2014 – B 1 KR 35/13 R = ZD 2015, 441, 443; *Bales/Schwanenflügel*, NJW 2012, 2475 f.; *Pitschas*, NZS 2009, 177 f.
30) S. a. die in § 35 Abs. 1 S. 4 u. Abs. 6 SGB I genannten Stellen; näher *Gutzler*, in: BeckOK SozR, 58. Ed, Stand: 1. 9. 2020, § 35 SGB I, Rdnrn. 8 ff.
31) *Schifferdecker*, in: KassKomm, 103. EL, März 2019, § 35 SGB I, Rdnr. 48; *Gutzler*, in: BeckOK SozR, 58. Ed, Stand: 1. 9. 2020, § 35 SGB I, Rdnrn. 10, 34.
32) Zum Verhältnis von Datenschutz und Schweigepflicht s. *Dochow*, MedR 2019, 276 ff. und 363 ff.
33) S. zu Lösungsoptionen *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1275 ff.
34) Vgl. bisher § 291a Abs. 1a SGB V a. F.
35) Vgl. zu § 291a SGB V a. F. *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, § 291a SGB V, Rdnr. 18 m. w. N.

eMP und NFD vorgesehen und zum Teil erhöht worden[36]. Demgegenüber werden weiterhin Fristen[37] und Sanktionen[38] (z.B. Honorarkürzungen) geregelt und zum Teil angepasst. Fernerhin sind zahlreiche informationssicherheitsrechtliche Regelungen enthalten, welche dem Schutz der Infrastruktur bzw. IT-Systeme dienen. Sie stehen aber in engem Zusammenhang mit dem Datenschutzrecht[39], das auf den Schutz personenbezogener Daten abzielt.

Kritisiert wurde die Bezeichnung als „Datenschutzgesetz" schon bezogen auf den Referentenentwurf, weil datenschutzrechtliche Maßgaben eher außer Acht gelassen werden und das Gesetz der Bezeichnung damit nicht gerecht werde[40]. Ungeachtet dessen bewirkt das PDSG wohl eher ein „Informationsnutzungsrecht"[41], das dem legitimen Anliegen der Verarbeitung von Gesundheitsdaten zur verbesserten Gesundheitsversorgung dient. Damit steht es in Kontinuität zu vergangenen Änderungen an den §§ 291a ff. SGB V a.F., die seit dem GMG zunehmend zu einer Ausweitung der Verarbeitungsbereiche und -befugnisse führen sollten. Das PDSG will nun z.B. „Spenden" zur Sekundärnutzung von Daten ermöglichen und die Anbindung von neuen Zugriffsberechtigten und Zugriffsverfahren erleichtern.

II. Elektronische Gesundheitskarte

1. Überblick und rechtssystematische Einordnung

Die Regelungen der §§ 291 ff. werden grundlegend neu strukturiert und die neuen Regelungen zur eGK sind fortan in den §§ 291 bis 291c SGB V enthalten. Die neuen Bestimmungen, die viele der bekannten Regelungen enthalten, sind nun übersichtlicher gestaltet, weil insbesondere die Regelungen zur TI herausgelöst worden sind. Überzeugend ist der Standort im 10. Kapitel (Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz) im ersten Abschnitt (Informationsgrundlagen, §§ 284 ff. SGB V), weil die eGK und die darauf enthaltenen und damit verarbeiteten Daten zu den Sozialdaten zählen, welche durch die Krankenkassen als Stellen i.S.v. § 35 SGB I verarbeitet werden.

2. Abgrenzung zu Anwendungen der Telematikinfrastruktur

Durch die Neugestaltung kann dem landläufigen Missverständnis entgegengewirkt werden, die vorgesehenen Anwendungen des § 291a Abs. 3 S. 1 SGB V a.F. seien „auf der Karte" enthalten. Das bisherige Gesetz hatte den Speicherort immer offengelassen und nur bezüglich bestimmter Angaben (z.B. Versichertenstammdaten) den Speicherort festgelegt[42]. Auch hinsichtlich des NFD – wie nunmehr § 291 Abs. 2 Nr. 3 i.V. mit § 358 Abs. 4 SGB V – ist weiterhin angeordnet, dass dessen Daten auch auf der Karte ohne Netzzugang verarbeitet werden können müssen[43].

Insgesamt werden Anwendungen der TI jetzt noch deutlicher von der eGK entkoppelt. Die Anwendungen werden jetzt in § 334 SGB V aufgeführt und sind darüber hinaus zugleich optionaler Teil der ePA gem. § 341 SGB V. Die Fokussierung auf die ePA als zentralem „Silo" für andere telematische Anwendungen im SGB V ist allerdings nicht ganz neu, da bereits durch e-health-Gesetz[44] und TSVG[45] verstärkt die Regelungen zur TI und ePA weiterentwickelt wurden und die eGK mehr in ihrer Rolle als Schlüsselwerkzeug[46] verstanden wurde.

3. Funktionen als Zugriffswerkzeug, Berechtigungsnachweis und Speicherort

Hervorzuheben ist nach wie vor die Funktion der eGK als Zugangsschlüssel des Versicherten zur TI, auch wenn künftig alternativ „mittels einer Benutzeroberfläche eines geeigneten Endgeräts"[47] auf die Daten zugegriffen werden kann. Soweit mit Hilfe der eGK der Zugriff erfolgt, unterstützt sie gem. § 291 Abs. 2 Nr. 2 SGB V die Anwendungen der TI[48]. Weitere auch hierfür bedeutsame technische Regelungen sind nicht neu[49]: Die eGK muss die Authentifizierung, Verschlüsselung und elektronische Signatur für den Versicherten ermöglichen[50]. Außerdem muss sie mit einer kontaktlosen Schnittstelle ausgestattet sein[51]. Die Regelung ist bereits durch das TSVG aufgenommen worden und dient dazu, dass die eGK mit einem mobilen Gerät mit Near Field Communication (NFC)-Schnittstelle genutzt werden kann, ohne dass ein zusätzliches Kartenlesegerät erforderlich ist[52]. Dies ist Voraussetzung für die Authentifizierung bei einem mobilen Zugriff auf medizinische Daten oder bei Nutzung von (telemedizinischen) Anwendungen in der TI.

Wie nach den bisherigen Regelungen in §§ 291, 291a SGB V a.F. werden der eGK noch weitere Funktionen zugewiesen, die überwiegend verwaltungstechnische Bedeutung haben. Zum einen ist die eGK, welche gem. § 291 Abs. 1 SGB V von den Krankenkassen auszustellen ist, vor allem Berechtigungsnachweis für die Inanspruchnahme von Leistungen im Rahmen der GKV (§ 291a Abs. 1 SGB V). Zusätzlich ist hier weiterhin § 15 Abs. 2 SGB V zu beachten[53], der nur redaktionelle Änderungen erfährt. Als Versicherungsnachweis enthält die eGK die in § 291a Abs. 2 und Abs. 3 SGB V aufgelisteten Daten, die neben Stammdaten wie bisher auch Angaben zu Wahltarifen und zusätzlichen Vertragsverhältnissen enthalten[54]. Daten des Europäischen Versicherungsnachweises sind nun auch explizit elektronisch auf der Karte zu speichern[55]. Die eGK ist also zum anderen auch Speicherort für die Versichertenstammdaten gem. § 291a Abs. 2 und 3 SGB V[56], aber – wie erwähnt – auch für den NFD gem. § 334 Abs. 1 S. 2 Nr. 5 SGB V[57]. Zum anderen dient sie gem. § 291a Abs. 1 SGB V der Abrechnung der Leistungen.

4. Versichertenstammdatenmanagement

Das Verfahren zur Nutzung der eGK als Versicherungsnachweis regelt nun § 291b SGB V. Dabei ist das ebenfalls nicht neue Versichertenstammdatenmanagement (VSDM)

36) § 87 Abs. 1 S. 13 ff., Abs. 2a S. 22 u. S. 27 ff., § 346 Abs. 4, Abs. 5, § 358 Abs. 3 SGB V.
37) S. zur ePA z.B. § 342 Abs. 2 SGB V; zum eRezept § 360 Abs. Abs. 2 SGB V.
38) S. z.B. § 291b Abs. 5, § 341 Abs. 6, Abs. 7, § 342 Abs. 5 SGB V.
39) S. *Voskamp*, in: *Kipker*, Cybersecurity, Rechtshandbuch, 2020, Kap. 5, Rdnrn. 1 f., 4 ff., s.a. Vorwort; *Wischmeyer*, Die Verwaltung 50 (2017), 155 ff.
40) LfDI BaWü, Pressemitteilung v. 27.2.2020.
41) Zum Begriff s. bei *Veil*, NVwZ 2018, 686, 696 m.w.N.
42) Bisher § 291 Abs. 2 SGB V a.F.; s. nun § 291 Abs. 4 SGB V.
43) § 291a Abs. 3 S. 1 Halbs. 2 SGB V a.F.; s. nun § 291a Abs. 4 SGB V.
44) S. z.B. die Anpassung der Normüberschrift und Abs. 1 in § 291a SGB V a.F.
45) S. § 291a Abs. 5c S. 4 ff. SGB V a.F.
46) S. dazu näher *Dochow/Kreitz*, ZfmE 2018, 147 ff.
47) S. z.B. § 336 Abs. 2, § 339 Abs. 4 SGB V; zuvor schon wegbereitend in § 291a Abs. 5 S. 8 SGB V a.F.
48) Abweichend davon werden gem. § 334 Abs. 2 SGB V nur die Anwendungen gem. § 334 Abs. 1 S. 2 Nr. 1 bis 5 SGB V unterstützt.
49) Bisher § 291 Abs. 2a SGB V a.F.
50) § 291 Abs. 2 Nr. 1 SGB V.
51) § 291 Abs. 3 SGB V.
52) BT-Dr. 19/8361, S. 106, 213.
53) Zu § 15 Abs. 2 SGB V s. *Dochow*, WzS 2015, 104, 108 f.
54) Krit. zu den „*statusergänzenden Merkmalen*" *Scholz*, in: BeckOK SozR, 58. Ed, Stand: 1.9.2020, § 291 SGB V, Rdnr. 5 m.w.N.
55) § 291a Abs. 3 Nr. 5 SGB V; bisher § 291a Abs. 2 Nr. 2 SGB V a.F. und als Sichtausweis, s. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1005 f.; *Dochow*, WzS 2015, 137, 138 m.w.N.
56) S. § 291 Abs. 4 SGB V.
57) § 291 Abs. 2 Nr. 3 i.V. mit § 358 Abs. 4 SGB V.

nun in § 291b Abs. 2 i. V. mit § 291a Abs. 2 und Abs. 3 SGB V geregelt[58]. Es verlangt von Leistungserbringern den Online-Abgleich der auf der Karte gespeicherten Versichertendaten mit den bei der Krankenkasse vorliegenden Daten. Es handelt sich um einen administrativen Dienst ohne medizinischen Nutzen. Die Überprüfung der Daten als auch die Aktualisierung erfolgen automatisiert beim Einlesen der eGK. Der Onlineabgleich ist der erste Dienst, der in der TI als Pflichtanwendung in Betrieb genommen werden konnte[59], auch wenn zuletzt Störungen durch Konfigurationsfehler in der zentralen TI auftraten[60].

5. Schutz vor Identitätsmissbrauch

Neu ist in § 291 Abs. 6 SGB V klarstellend geregelt, dass die Krankenkassen bei der Ausstellung der eGK die in der Richtlinie gemäß § 217f Abs. 4b SGB V vorgesehenen Maßnahmen und Vorgaben zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme umzusetzen haben[61]. Im Interesse der Erhöhung der Sicherheit der Ausgabeprozesse der eGK schreibt § 217f Abs. 4b S. 4 SGB V nun vor, dass vor dem Versand der eGK und deren persönlicher Identifikationsnummer (PIN) an die Versicherten ein Abgleich der Anschrift der Versicherten mit den Daten aus dem Melderegister erfolgen muss. § 291 Abs. 6 S. 3 SGB V ermächtigt die Krankenkassen hierzu die Daten gem. § 34 Abs. 1 S. 1 Nr. 1 bis 6 und Nr. 10 BMG abzurufen. Dies dient dem Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme. Weitere Verfahrensvorgaben zur Zustellung der eGK und zur Authentifizierung des Versicherten (z. B. über PostIdent[62], elektronischer Personalausweis) sind in § 336 Abs. 5 SGB V enthalten. Krankenkassen müssen also sicherstellen, dass die eGK und die PIN als Authentifizierungsmittel nur den berechtigten Versicherten zugeht.

Hintergrund für die Änderungen und höheren Anforderungen ist wohl, dass es dem *Chaos Computer Club* Ende 2019 gelungen war, Zugangsberechtigungen für die TI zu erlangen, indem er sich u. a. gültige Heilberufsausweise und Gesundheitskarten unter der Identität Dritter an eine Wunschadresse liefern lassen hat[63]. Es habe dazu lediglich der Online-Meldung einer einfachen Adressänderung bedurft[64]. Demzufolge bestanden beim Identitätsmanagement für den Zugang zur TI und bei der Herausgabe der Chipkarten erhebliche strukturelle Sicherheits- und Organisationsmängel[65]. Vor dem Hintergrund der Risiken eines Identitätsmissbrauchs für die in der TI verarbeiteten Gesundheitsdaten ist der Datenabgleich gem. § 217f Abs. 4b S. 4 SGB V sachgemäß.

6. Befugnis zur Speicherung des Lichtbildes, weitere Regelungen

Nach § 291a Abs. 6 S. 1 SGB V dürfen Krankenkassen das Lichtbild zur Ausstellung einer eGK für die Dauer des Versicherungsverhältnisses des Versicherten, jedoch längstens für zehn Jahre, für Ersatz- und Folgeausstellungen der eGK speichern. Das Lichtbild ist damit nicht mehr nach Übermittlung der eGK zu löschen. Die neu geschaffene Aufbewahrungsregelung i. S. d. Art. 17 Abs. 3 lit. b DSGVO ist Folge eines Urteils des BSG, wonach eine dauerhafte Speicherung des Lichtbildes durch die Krankenkassen für unzulässig erklärt wurde, weil es hierfür an einer Rechtsgrundlage mangelte[66].

Ferner wird mit § 291a Abs. 6 S. 2 SGB V geregelt, dass die bisherige Krankenkasse das Lichtbild nach dem Ende des Versicherungsverhältnisses unverzüglich, spätestens aber nach drei Monaten, zu löschen hat. Die Verarbeitung der Daten ist dann nicht mehr erforderlich (vgl. auch Art. 5 Abs. 1 lit. c, Art. 17 Abs. 1 lit. a DSGVO). Die weiteren Aspekte zu Einzug, Sperrung oder weiterer Nutzung der eGK nach einem Krankenkassenwechsel sowie zum Austausch der eGK regelt in weitgehender Übereinstimmung mit dem bisherigen Recht § 291c SGB V.

III. Telematikinfrastruktur

1. Definition und Merkmale

Mit dem PDSG wird im SGB V nunmehr eine klarere Struktur für Regelungen zur TI und ihrer Anwendungen angelegt, die in einem eigenen 11. Kapitel näher ausgestaltet wird. Die Telematikinfrastruktur wird in § 306 Abs. 1 S. 2 SGB V definiert als „*die interoperable und kompatible Informations-, Kommunikations-und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens sowie der Rehabilitation und der Pflege dient*". Sie soll dem besonderen Schutzbedarf von Gesundheitsdaten i. S. v. Art. 9 Abs. 1, Art. 4 Nr. 15 DSGVO Rechnung tragen (vgl. § 306 Abs. 3 SGB V). Die Infrastruktur ist erforderlich für die Nutzung der eGK und die gesetzlich vorgesehenen Anwendungen[67]. Sie soll ferner für die Nutzung weiterer Anwendungen der TI (§ 327 SGB V) auch ohne Einsatz der eGK[68] sowie für Verarbeitungszwecke im Kontext der Gesundheits- und pflegerischen Forschung[69] geeignet sein.

Die Gesamtarchitektur der TI umfasst gem. § 306 Abs. 2 Nr. 1 SGB V eine „*dezentrale Infrastruktur*" bestehend aus Komponenten zur Authentifizierung (z. B. eGK, eHBA[70], SMC-B[71]) und zur sicheren Übermittlung von Daten in die zentrale Infrastruktur (z. B. sicherheitszertifizierte Konnektoren[72], Kartenleseterminals). Dies ermöglicht registrierten Nutzern den sicheren Zugang zum geschlossenen Netz der zentralen Infrastruktur[73]. Diese Komponenten, die von der *gematik* zugelassen werden (§ 325 SGB V), kommen in den Umgebungen der Leistungserbringer (Arztpraxen und Krankenhäuser) zum Einsatz[74]. Komponenten werden in § 306 Abs. 4 S. 3 SGB V allgemein definiert als „dezentrale technische Systeme oder deren Bestandteile", womit sowohl Computerprogramme (Software) als auch Geräte (Hardware) gemeint sind[75]. Ferner umfasst die TI

58) Bisher § 291 Abs. 2b SGB V a. F., s. dazu *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1001 ff.; zum Ablauf zusf. *Scholz*, in: BeckOK SozR, 58. Ed, Stand: 1. 9. 2020, § 291 SGB V, Rdnrn. 4a.1 ff.; zur Rspr. s. *Dochow*, WzS 2015, 104, 105 ff. und WzS 2015, 137, 138 f.

59) Näher *Dochow/Kreitz*, ZfmE 2018, 147, 150 f.

60) Ärzteblatt.de v. 29. 5. 2020, aerzteblatt.de/nachrichten/113298/Stoerung-beim-Versichertenstammdatendienst.

61) So auch § 336 Abs. 7 SGB V.

62) Dag. zum VideoIdent-Verfahren krit. BfDI, Stellungnahme zum PDSG v. 25. 5. 2020, S. 10 f.

63) Chaos Computer Club v. 27. 12. 2019, ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk; näher auch *Schmedt*, DÄBl. 2020, A-7.

64) *Schmedt*, DÄBl. 2020, A-7.

65) Spiegel.de v. 27. 12. 2019, spiegel.de/netzwelt/netzpolitik/ccc-hacker-finden-sicherheitsluecken-in-der-telematikinfrastruktur-a-1302902.html; ärztezeitung.de v. 3. 1. 2020, aerztezeitung.de/Wirtschaft/Chaos-Computer-Club-fordert-neue-Prozesse-fuer-Kartenausgabe-405406.html; *Schmedt*, DÄBl. 2020, A-7.

66) BSG, Urt. v. 18. 12. 2018 – B1 KR 31/17 R = NZS 2019, 670 ff.; zum Lichtbild auf der eGK s. a. *Dochow*, WzS 2015, 137 f.

67) § 306 Abs. 1 S. 2 Nr. 1 SGB V.

68) § 306 Abs. 1 S. 2 Nr. 2 lit. a SGB V.

69) § 306 Abs. 1 S. 2 Nr. 2 lit. b SGB V.

70) Elektronischer Heilberufsausweis (für Ärzte auch „elektronischer Arztausweis"), zur Ausgabe s. § 340, § 312 Abs. 1 Nr. 9 SGB V. Er muss über eine Möglichkeit zur sicheren Authentifizierung und zur Erstellung qualifizierter elektronischer Signaturen verfügen, § 339 Abs. 6 SGB V, s. a. § 361 Abs. 4 SGB V.

71) Sog. Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (auch „elektronischer Praxisausweis"), s. a. § 340 SGB V.

72) Künftig soll es weitere (mobile) Zugangsmöglichkeiten geben, vgl. BReg., BT-Dr. 19/10731, S. 2, 4.

73) BT-Dr. 19/18793, S. 99.

74) BT-Dr. 19/18793, S. 99.

75) BT-Dr. 19/18793, S. 100.

gem. §306 Abs. 2 Nr. 2 SGB V eine „*zentrale Infrastruktur*" bestehend aus sicheren Zugangsdiensten als Schnittstelle zur dezentralen Infrastruktur und einem gesicherten Netz einschließlich der für den Betrieb notwendigen Dienste. In §306 Abs. 4 S. 2 SGB V werden Dienste allgemein definiert als „zentral bereitgestellte und in der TI betriebene technische Systeme, die einzelne Funktionalitäten der TI umsetzen." In der zentralen Infrastruktur sind dies zum einen konkret VPN-Dienste, die dazu dienen, die Nutzer an das geschlossene gesicherte Netz der TI anzubinden[76]. Zum anderen gehören dazu die für den Betrieb der TI notwendigen Dienste, wie zum Beispiel Verzeichnis- und Identifikationsdienste (§313 SGB V)[77]. Bestandteil der TI ist gem. §306 Abs. 2 Nr. 3 SGB V schließlich eine „*Anwendungsinfrastruktur*" bestehend aus Diensten für die telematischen Anwendungen, die den Nutzern zur digitalen Gesundheitsversorgung zur Verfügung stehen[78]. Anwendungen werden in §306 Abs. 4 S. 1 SGB V definiert als „nutzerbezogene Funktionalitäten auf der Basis von zugelassenen Diensten und Komponenten[79] zur Verarbeitung von Gesundheitsdaten in der Telematikinfrastruktur". Das umfasst weitere nutzerbezogene Funktionalitäten[80]. Neben dem Versichertenstammdatenmanagement gem. §291b Abs. 2 SGB V und sicheren Übermittlungsverfahren für die Kommunikation der Leistungserbringer gem. §311 Abs. 1 Nr. 5 SGB V gehören dazu auch die Anwendungen gem. §334 Abs. 1 S. 2 SGB V[81]. Diese technikneutral beschriebene Struktur ist maßgebend für die Zuteilung der datenschutzrechtlichen Verantwortlichkeit und für die Konkretisierung der Mittel der Datenverarbeitung.

2. Datenschutzrechtliche Verantwortlichkeiten

Hervorzuheben sind die Regelungen zur datenschutzrechtlichen Verantwortlichkeit in §307 SGB V. Etwa 15 Jahre nach Erlass der einschlägigen Regelungen kam die Frage auf, wer Verantwortlicher im Sinne des Datenschutzrechts in der TI ist[82]. Die *gematik* sah sich nicht in der datenschutzrechtlichen Verantwortlichkeit[83] und (Zahn)Ärzte wirkten darauf hin, dass deren Verantwortlichkeit am technischen Konnektor, also in der Regel an der Grenze ihrer Einflusssphäre in der Praxis, enden solle[84]. Bedeutsam ist die Festlegung einer Verantwortlichkeit u. a. für die Frage, wer für „Datenpannen" einsteht (Art. 33 f. DSGVO), für Verstöße haftet (Art. 82 DSGVO), Bußgeldforderungen oder Maßnahmen der Aufsichtsbehörden für den Datenschutz ausgesetzt ist oder wer bestimmte Pflichten zu erfüllen hat, wie etwa die Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO). Aus Gründen der Transparenz ist bedeutsam, wer Informationspflichten zu erfüllen hat und wem gegenüber der Betroffene seine Rechte geltend machen kann (Art. 12 ff. DSGVO)[85].

a) Auffassung der DSK vor dem PDSG

Die *Datenschutzkonferenz (DSK)* vertrat zu §291a Abs. 7 SGB V a. F. die Auffassung, dass die *gematik* für die zentrale Zone datenschutzrechtlich alleinverantwortlich und für die dezentrale Zone datenschutzrechtlich mitverantwortlich i. S. v. Art. 26 DSGVO ist, wobei der Umfang der Verantwortung der *gematik* für die dezentrale Zone der Telematik-Infrastruktur einer gesetzlichen Regelung[86] bedürfe. Die *gematik* sei für die Verarbeitung insbesondere verantwortlich, soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist[87].

b) Zuteilung der Verantwortlichkeiten mit dem PDSG

Mit dem PDSG wird von der Einschätzung der *DSK* abgewichen. Eine gemeinsame Verantwortlichkeit i. S. v. Art. 26 DSGVO ist nicht vorgesehen. Vielmehr sollen die Verantwortlichkeiten in der TI getrennt voneinander, „differenziert" und „lückenlos" festgelegt werden[88]. Verantwortlich im Sinne des Art. 4 Nr. 7 DSGVO für die Verarbeitung von Gesundheitsdaten innerhalb der TI sind mehrere Stellen. Die Zuweisung der jeweiligen Verantwortlichkeit orientiert sich laut Gesetzesbegründung an den für die jeweilige Stelle überblickbaren und beherrschbaren Strukturen, wie sie sich aus den einzelnen Bausteinen der TI ergeben sollen. Jeder Verantwortliche soll für den Bereich zuständig sein, in dem er über die konkrete Datenverarbeitung entscheidet[89].

Nach §307 Abs. 1 SGB V sind „*Leistungserbringer*", z. B. Ärzte und Praxen, welche Anwendungen der TI nutzen und Patientendaten z. B. in die ePA einstellen oder darüber abrufen, für die Verarbeitung personenbezogener Daten mittels der in ihrer Umgebung genutzten Komponenten der *dezentralen Infrastruktur* verantwortlich[90]. Die Pflicht zur Nutzung bestimmter Dienste, Anwendungen und Komponenten entbinde nicht von der mit der Verantwortlichkeit einhergehenden Pflichten[91]. Dies gilt für die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten. Es wird hierbei auf die Nutzereigenschaft[92] abgestellt. Einschränkend sollen die Nutzer aber nur verantwortlich sein, soweit sie über die Mittel der Datenverarbeitung „mit entscheiden". Daraus wird jedoch nicht die Konsequenz der gemeinsamen Verantwortlichkeit gezogen, wohl weil sich die Verantwortlichkeit „schwerpunktmäßig auf die Sicherstellung der bestimmungsgemäßen Nutzung der Komponenten, deren ordnungsgemäßen Anschluss und die Durchführung der erforderlichen fortlaufenden Software-Updates" erstrecken soll[93].

„*Anbieter des Zugangsdienstes*" sind gem. §307 Abs. 2 SGB V datenschutzrechtlich verantwortlich für den Betrieb des durch die *gematik* spezifizierten und zugelassenen Zugangsdienstes in der *zentralen Infrastruktur.* Die Anbieter des gesicherten Netzes in der zentralen Infrastruktur sind gem. §307 Abs. 3 SGB V verantwortlich für die Übertragung insbesondere von Gesundheitsdaten zwischen Leistungserbringern, Kostenträgern sowie Versicherten und für die Übertragung im Rahmen der Anwendungen der eGK. Unter die Regelungen fallen Hersteller und Anbieter von Sicherheitsroutern (Konnektoren) und Software-Programmen, VPN-Anbieter für den alleinverantwortlichen Betrieb des gesicherten Netzes sowie für die Praxen tätige IT-Dienstleister[94]. Die *gematik* selbst ist nicht Anbieter des Netzes[95].

76) BT-Dr. 19/18793, S. 99.
77) Vgl. BT-Dr. 19/18793, S. 99.
78) Vgl. BT-Dr. 19/18793, S. 99.
79) §325 SGB V.
80) §327 SGB V.
81) BT-Dr. 19/18793, S. 99.
82) *Gerlof*, Ärzte Zeitung online v. 18. 9. 2019.
83) S. ärzteblatt.de v. 18. 7. 2019.
84) BZÄK, Pressemitteilung v. 28. 6. 2019; 122; Deutscher Ärztetag 2019, Beschluss Ib-01.
85) Zu den Pflichten s. zusf. z. B. *Conrad*, DuD 2019, 563, 565 f.
86) Art. 26 Abs. 1 S. 2 DSGVO.
87) Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) v. 12. 9. 2019; s. a. BfDI, 28. TB., BT-Dr. 19/19900, S. 24 f.
88) BT-Dr. 19/18793, S. 2, 4, 81, 83; BT-Dr. 19/20708, S. 4.
89) BT-Dr. 19/18793, S. 100.
90) BT-Dr. 19/18793, S. 100.
91) Vgl. BT-Dr. 19/18793, S. 100.
92) Der Begriff „Nutzer" findet sich auch in §313 und §355 SGB V wieder, wird i. Ü. aber in Bezug auf den Versicherten verstanden, wenn von „nutzerbezogenen Funktionalitäten" und „Nutzerfreundlichkeit" die Rede ist, vgl. BT-Dr. 19/18793, S. 1, 101.
93) BT-Dr. 19/18793, S. 100 f.
94) Vgl. *Gieselmann*, c't 19/2020, S. 32. Für diese gelten besondere Anforderungen im Hinblick auf Sorgfalt und notwendige Fachkunde: s. §332 SGB V (bisher §291b Abs. 6a SGB V a. F.).
95) BT-Dr. 19/18793, S. 101.

Der Betrieb der Dienste der *Anwendungsinfrastruktur* erfolgt durch den jeweiligen *Dienstanbieter*, der gem. § 307 Abs. 4 SGB V für die Verarbeitung insbesondere von Gesundheitsdaten zum Zweck der Nutzung des jeweiligen Dienstes verantwortlich ist. So sind gem. § 341 Abs. 4 i. V. mit § 307 Abs. 4 SGB V die Krankenkassen für die Datenverarbeitung in der ePA datenschutzrechtlich verantwortlich. Ebenfalls sind sie für die Anwendungen eMP und NFD gem. § 358 Abs. 5 SGB V datenschutzrechtlich verantwortlich.

Die *gematik* wird damit, trotz der ihr gesetzlich zugewiesenen zentralen Aufgaben (§§ 311 ff. SGB V), aus der Gesamtverantwortlichkeit für die TI entlassen. Sie ist datenschutzrechtlich nur verantwortlich, soweit sie im Rahmen ihrer Aufgaben nach § 311 Abs. 1 SGB V die Mittel der Datenverarbeitung bestimmt. Ausdrücklich ist sie gem. § 307 Abs. 5 i. V. mit § 311 Abs. 1 Nr. 3 i. V. mit § 313 SGB V datenschutzrechtlich Verantwortliche für den Verzeichnisdienst der TI und für die eRezept-App[96]. Sie soll aber nicht verantwortlich sein, soweit schon eine Verantwortlichkeit nach § 307 Abs. 1–4 SGB V begründet ist. Inwieweit daneben noch Raum bleibt für die Auffangregelung des § 307 Abs. 5 SGB V, die eine lückenlose Zuweisung der Verantwortlichkeit erreichen soll[97], ist fraglich, weil die Verantwortlichkeiten nach § 307 Abs. 1–4 SGB V schon recht pauschal zugewiesen werden.

d) Bewertung

Dem nationalen Gesetzgeber ist mit Art. 4 Nr. 7, Halbs. 2 DSGVO eine Möglichkeit eröffnet, den Verantwortlichen gesetzlich zu bestimmen, wenn die Zwecke und Mittel der Verarbeitung durch das Recht der Mitgliedstaaten „vorgegeben" sind. Letzteres ist bei der TI der Fall, denn die Zwecke (u. a. „Versorgung der Versicherten") und wesentlichen Mittel der Verarbeitung, wie die Infrastruktur, bestimmte telematische Anwendungen sowie bestimmte (zulässige) Dienste und Komponenten, sind gesetzlich festgelegt[98]. Somit kann der zuständige Gesetzgeber, da er die Entscheidungshoheit über die Zwecke und Mittel selbst ausübt, einer Stelle die Position als Verantwortlichen zuweisen[99], wobei eine Anknüpfung an eine entsprechende Aufgabenverteilung sinnvoll erscheint[100]. Allerdings soll die Möglichkeit nur bestehen, wo für den Gesetzgeber überhaupt Öffnungsklauseln für die Bestimmung der Mittel und Zwecke bestehen[101]. Soweit in der TI für viele Anwendungen ein Freiwilligkeit- bzw. Einwilligungsmodell zugrunde gelegt wird, sind Öffnungsklauseln hierfür nur vorzufinden, soweit „zusätzliche Bedingungen" i. S. v. Art. 9 Abs. 4 DSGVO geregelt werden[102]. Fraglich ist zudem, ob mit Art. 4 Nr. 7 Halbs. 2 DSGVO Regelungsspielräume eröffnet sind, welche es zulassen, die Verantwortlichkeit abweichend von Maßstäben der DSGVO und der Rechtsprechung des EuGH festzulegen. Die „klare Zuteilung der Verantwortlichkeiten" soll im Interesse des Schutzes der Betroffenen im Grundsatz durch die DSGVO erfolgen[103]. Das ist wegen der angestrebten Harmonisierung des europäischen Datenschutzrechts nachvollziehbar. Im Hinblick auf die datenschutzrechtlichen Vorgaben, die auch der Gesetzgeber des PDSG im Rahmen seiner „Klarstellung" betont[104], sind die Legaldefinitionen in Art. 4 Nr. 7 und 8 DSGVO, die Bestimmungen der Art. 24, 26, 28 DSGVO und die Erwägungsgründe 74, 79 maßgeblich. Im Ausgangspunkt ist anhand objektiver Kriterien[105] zu ermitteln, wer über die Zwecke und wesentlichen Mittel der Verarbeitung von personenbezogenen Daten (mit-)entscheidet[106]. Dabei sind funktionelle und tatsächliche Gegebenheiten entscheidend[107]. Dem Rechtsgedanken des Art. 26 Abs. 2 S. 1 DSGVO entsprechend dürften Regelungen i. S. v. Art. 4 Nr. 7 Halbs. 2 DSGVO nur im Einklang mit der DSGVO stehen, wenn die Festlegungen die jeweiligen tatsächlichen Funktionen und Beziehungen der verarbeitenden Stellen gebührend widerspiegeln[108]. Die Betroffenen sollen nicht der Möglichkeit beraubt werden, ihre Rechte gegenüber denjenigen Stellen geltend zu machen, die den faktisch größten Einfluss auf die Datenverarbeitung haben[109]. Nach dem auf einen umfassenden Schutz der Betroffenen abzielenden weiten Verständnis des EuGH[110] genügt es für die Begründung einer (Mit)Verantwortlichkeit schon, wenn ein Beteiligter einem anderen eine Datenverarbeitung ermöglicht[111]. Eine Mitwirkung an der Entscheidung über Zwecke und Mittel kommt durch ein Veranlassen, Ermuntern und Beenden der Datenverarbeitung eines anderen in Betracht: Es genügt das Festlegen von Auswahlbedingungen[112] oder das Organisieren und Koordinieren der Datenverarbeitung eines anderen[113]. Das ist charakteristisch in Netzwerken oder bei Plattformen, sodass die Errichtung einer gemeinsamen Infrastruktur oder Internetplattform auf eine gemeinsame Verantwortlichkeit hinweist[114]. Die Akteure können dabei durchaus in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein[115]. Insoweit nicht mitverantwortlich sind dann nur Personen, die vor- oder nachgelagerte Vorgänge in einer Verarbeitungskette ausführen, ohne dabei einen tatsächlichen Einfluss auf die Zwecke und Mittel zu haben[116].

Für Leistungserbringer ist eine Verantwortung für die Verarbeitung von Patientendaten in der von ihnen tatsächlich beherrschbaren Sphäre sachgerecht. Das betrifft also die Komponenten, über welche sie eigenständig verfügen können (z. B. Praxisverwaltungssysteme) und für welche die einschlägigen Datenschutzregelungen[117] zu beachten sind. Auf

96) S. § 311 Abs. 1 Nr. 10, § 360 Abs. 5 SGB V; s. a. III., 3., d).
97) BT-Dr. 19/18793, S. 101.
98) Vgl. BT-Dr. 19/18793, S. 100; zu den entspr. Anforderungen s. *Petri*, in: *Simitis* et al., Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO, Rdnr. 23.
99) Vgl. *Kühling/Martini et al.,* Die DSGVO und das nationale Recht, S. 25.
100) *Raschauer*, in: *Sydow*, EU-DSGVO, 2. Aufl. 2018, Art. 4, Rdnr. 141; vgl. *Hartung*, in: *Kühling/Buchner*, DS-GVO BDSG, 3. Aufl. 2020, Art. 4, Nr. 7, Rdnr. 14.
101) *Kühling/Martini et al.,* Die DSGVO und das nationale Recht, S. 26.
102) S. für die Pflichtanwendungen Art. 9 Abs. 2 lit. h, i DSGVO; s. a. o. bei I., 2.
103) ErwG 79, vgl. zum Prinzip der Verantwortlichkeit *Artikel-29-Datenschutzgruppe*, WP 169 v. 16. 2. 2010, S. 2.
104) BT-Dr. 19/18793, S. 2, 81, 100.
105) Vgl. *Conrad*, DuD 2019, 563, 564 f. m. w. N.; zu den Kriterien s. *Artikel-29-Datenschutzgruppe*, WP 169 v. 16. 2. 2010, S. 34 ff., 40.
106) Art. 4 Nr. 7 Halbs. 1 DSGVO; *Conrad*, DuD 2019, 563, 564.
107) *Artikel-29-Datenschutzgruppe*, WP 169 v. 16. 2. 2010, S. 1, 11 ff., 22 f., 38 und passim; vgl. *Conrad*, DuD 2019, 563, 564 m. w. N.
108) *Petri*, in: *Simitis* et al., Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO, Rdnr. 26.
109) *Petri*, in: *Simitis* et al., Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO, Rdnr. 26.
110) S. EuGH, Urt. v. 5. 6. 2018, Rs. C-210/16 –, (ULD/Wirtschaftsakademie Schleswig-Holstein) = JZ 2018, 1154 ff., Rdnr. 28 (unter Hinweis auf EuGH, Urt. v. 13. 5. 2014, Rs. C-131/12 – (Google Spain), Rdnr. 34); bestätigt in EuGH, Urt. v. 10. 7. 2018, Rs. C-25/17 – (Zeugen Jehovas) = NJW 2019, 285 ff. und EuGH, Urt. v. 29. 7. 2019, Rs. C-40/17 – (Fashion-ID) = MMR 2019, 579, 581, Rdnr. 66 m. w. N.; *Conrad*, DuD 2019, 563, 563; zusf. *Jung/Hansch*, ZD 2019, 143, 147 m. w. N.; s. a. krit. *Dochow,* MedR 2019, 636, 640 ff. m. w. N.
111) Vgl. EuGH, JZ 2018, 1154, 1156, Rdnr. 35.
112) EuGH, JZ 2018, 1154, 1156, Rdnrn. 36, 39.
113) EuGH, NJW 2019, 285, 290, Rdnrn. 70 ff. (erforderlich ist ein „Eigeninteresse", Rdnr. 68).
114) S. *Artikel-29-Datenschutzgruppe*, WP 169 v. 16. 2. 2010, S. 24, 29; *Jung/Hansch*, ZD 2019, 143, 145 m. w. N.
115) EuGH, NJW 2019, 285, 290, Rdnr. 66; MMR 2019, 579, 581 f., Rdnrn. 70, 72.
116) Vgl. EuGH, MMR 2019, 579, 582, Rdnrn. 74, 85.
117) S. dazu *Dochow et al.*, Datenschutz in der ärztlichen Praxis, 2019.

eine tatsächliche Sachherrschaft über einen Konnektor oder andere Komponenten kann es darüber hinaus aber nicht ankommen, denn dingliche oder ortsbezogene Kriterien trügen dem Charakter einer digital-vernetzten Infrastruktur nicht hinreichend Rechnung. Ferner sind Leistungserbringer freilich mitverantwortlich, soweit sie für Anwendungen die Zwecke der Verarbeitung konkretisieren[118]. Aus tatsächlichen Überlegungen heraus ist aber fraglich, ob Leistungserbringern[119] i. S. v. § 307 Abs. 1 SGB V eine Alleinverantwortlichkeit für bestimmte Elemente einer staatlich implementierten Infrastruktur zugewiesen werden kann, auch wenn die Festlegung der Mittel betont „technikneutral“[120] durch ein Gesetz, die detaillierte konkretisierende Ausgestaltung aber durch die *gematik* sowie andere Akteure und gerade nicht durch die Leistungserbringer, erfolgt. In der Gesetzesbegründung wird ausgeführt, dass die Mittel der Verarbeitung „bereichsspezifisch gesetzlich vorgeprägt“ werden, so dass die Art und Weise einer Datenverarbeitung nicht mehr durch einzelne Datenverarbeiter bestimmt werde[121]. Das steht im Widerspruch zur Regelung des § 307 Abs. 1 SGB V, wo wegen der Entscheidung zur Nutzung der Komponenten trotzdem Verantwortlichkeiten begründet werden sollen und zum Teil von einer Mitentscheidung die Rede ist. Mit wem zusammenentschieden wird, bleibt offen.

Maßgeblich für die Frage der (Mit)Verantwortlichkeit ist, welche Rolle den Akteuren, insbesondere der *gematik*, zugewiesen wird. Das Gesetz gibt für die Aufgaben und Rollen genügend Anhaltspunkte: Eine Besonderheit ist, dass eine staatlich implementierte Infrastruktur nicht durch zuständige Behörden betrieben wird. Nach § 306 Abs. 1 S. 1 SGB V schafft die Bundesrepublik Deutschland, vertreten durch das BMG[122], gemeinsam mit den Verbänden des Gesundheitswesens die TI, wobei sie diese Aufgabe gem. § 306 Abs. 1 S. 3 SGB V durch eine Gesellschaft, die *gematik,* wahrnimmt. Bisher war in § 291a Abs. 7 S. 2 SGB V a. F. noch geregelt, dass die *gematik* „die Regelungen zur TI trifft sowie deren Aufbau und Betrieb übernimmt“. Nunmehr lassen sich die Aufgaben der *gematik* aus §§ 311 ff. SGB V entnehmen, die aber nicht weniger auf zentrale Handlungen zur Ermöglichung einer Datenverarbeitung durch Leistungserbringer und Anbieter von Diensten hindeuten. Dazu gehören als wesentliche Mittel der Datenverarbeitung z. B. die konkrete Festlegung von Inhalt und Struktur der Datensätze, die Festlegung von Verfahren zur Verwaltung der Zugriffsberechtigungen, der Aufbau der TI und insoweit die Festlegung der Rahmenbedingungen für Betriebsleistungen[123]. Die gesetzlich vorgeprägten Anwendungen werden von der *gematik* spezifiziert und bestimmte Komponenten und Dienste, welche die Basis für diese Funktionalitäten bieten, dürfen erst an die TI angebunden werden[124], wenn sie von der *gematik* zugelassen wurden[125]. Auch weitere Anwendungen bedürfen erst der Bestätigung durch die *gematik*, die hierfür Festlegungen der Voraussetzungen für die Nutzung der TI trifft[126]. Sie legt jeweils das nähere zu Kriterien, Voraussetzungen und Verfahren fest[127] und ermöglicht damit erst eine Datenverarbeitung eines Dritten bzw. schafft dafür die wesentlichen Voraussetzungen, was der EuGH, wie dargelegt, als maßgebliches Kriterium für die Begründung einer gemeinsamen Verantwortlichkeit angesehen hat. Genauso liegt es hinsichtlich der „Verfahren zur Übermittlung medizinischer Daten über die Telematikinfrastruktur“, welche die *gematik* gem. § 311 Abs. 6 SGB V festlegt. Diese Verfahren dienen der Erreichung des Zwecks, einen Datenaustausch zwischen Leistungserbringern zu bewirken. Insoweit wird das Verfahren als „Mittel zur Zweckerreichung“[128] maßgeblich von der *gematik* bestimmt.

Auch Betriebsleistungen der TI sind auf der Grundlage der von der *gematik* festzulegenden Rahmenbedingungen zu erbringen und dazu vergibt sie unter bestimmten Voraussetzungen an Anbieter von Betriebsleistungen Zulassungen und kann die Zulassungen sogar beschränken[129]. Zwar erfolgt die Zulassung im Rahmen der gesetzlichen Vorgaben. Dennoch hat die *gematik* eine maßgebliche Steuerungsrolle wegen der konkreten Festlegung der verbindlichen Rahmenbedingungen[130], sodass auch hiernach mit Blick auf die Rechtsprechung des EuGH von einer Mitverantwortlichkeit auszugehen ist.

Schließlich soll die *gematik* ein Sicherheitskonzept samt Vorgaben für den sicheren Betrieb der TI erstellen und deren Umsetzung überwachen[131]. Sie hat die Gesamtverantwortung für die Sicherheit des Betriebs der TI[132]. Im Rahmen der Maßnahmen zur Abwehr von Gefahren für die Funktionsfähigkeit und Sicherheit der TI durch Komponenten und Dienste ist sie nicht nur verpflichtet, unverzüglich die erforderlichen technischen und organisatorischen Maßnahmen zur Abwehr dieser Gefahr entsprechend dem Stand der Technik zu treffen[133], sondern kann sie zur Gefahrenabwehr ferner Komponenten und Dienste sperren[134]. Damit erhält sie eine wesentliche Steuerungsmacht über die Komponenten zum Beenden der Verarbeitung und verarbeitet im Rahmen der Erkennung von Störungen und Angriffen sogar selbst Daten[135]. Die Entbindung der *gematik* von der datenschutzrechtlichen Verantwortung ist nach alledem nicht nur „nicht sachgerecht“[136], sondern wegen der tatsächlichen Funktionen infolge der umfänglichen Aufgabenzuweisungen zur detaillierten verbindlichen Festlegung der wesentlichen Mittel der Datenverarbeitung und der Entscheidung über Zulassungen und Sperrungen von Komponenten und Diensten auch datenschutzrechtlich fragwürdig, da die *gematik* einen maßgeblichen Einfluss auf den Aufbau und Betrieb der TI hat[137]. Dass sie keinerlei Ursache für die Datenverarbeitung setzt, ist zu bezweifeln. Vor diesen Hintergrund liegt es näher, im Sinne der *DSK* von einer gemeinsamen Verantwortlichkeit auszugehen, deren Merkmal gem. Art. 26 Abs. 1 S. 1 DSGVO gerade ist, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Obwohl er selbst die „arbeitsteiligen Datenverarbeitungsprozesse“[138] anerkennt, lässt der Gesetzgeber des PDSG die

118) Diese sind keineswegs durch den Gesetzgeber vorgegeben, sondern konkretisieren sich in Abhängigkeit von Indikation und Patientenwillen hin zur Nutzung einer bestimmten Anwendung in einem bestimmten Umfang, ggf. mit bestimmten Akteuren zu z. B. einem bestimmten Therapiezweck. A. A. wohl BT-Dr. 19/18793, S. 100.

119) Leistungserbringer, deren personenbezogene Daten verarbeitet werden (s. § 313 SGB V), sind als „Nutzer“ der TI zugleich Betroffene i. S. v. Art. 4 Nr. 1 DSGVO. Allg. zum Problem, dass Nutzer in die Verantwortlichkeit gedrängt werden s. a. *Conrad*, DuD 2019, 563, 566 f.

120) BT-Dr. 19/18793, S. 98.

121) BT-Dr. 19/18793, S. 99.

122) S. BT-Dr. 19/18793, S. 106; vgl. § 322 SGB V.

123) § 311 Abs. 1 S. 1 Nr. 1 lit. b und e, Nr. 2 SGB V; vgl. für die ePA auch § 354 SGB V.

124) S. § 326 SGB V.

125) § 311 Abs. 1 S. 1 Nr. 4, § 325 SGB V. S. a. das bußgeldbewehrte Verbot: § 326 i. V. mit § 395 Abs. 2a Nr. 1 SGB V.

126) § 311 Abs. 1 S. 1 Nr. 6, § 327 SGB V.

127) S. § 325 Abs. 3 S. 5. § 327 Abs. 2 S. 2 SGB V; für die ePA s. a. § 341 Abs. 3 sowie § 355 SGB V, wonach die KBV die Inhalte definiert.

128) So die Eigendefinition in BT-Dr. 19/18793, S. 99.

129) § 323 Abs. 2, § 324 Abs. 1, Abs. 2 SGB V.

130) Vgl. auch BT-Dr. 19/18793, S. 101.

131) § 311 Abs. 1 S. 1 Nr. 1 lit. a SGB V; vgl. ferner § 330 SGB V.

132) BT-Dr. 19/20708, S. 183.

133) § 329 Abs. 1 SGB V.

134) § 329 Abs. 3 SGB V.

135) S. § 331 Abs. 4 SGB V.

136) Zit. nach *Gieselmann*, c't 19/2020, S. 32.

137) Wie hier BR, BT-Dr. 19/19365, S. 4 ff.; a. A. *Heckmann*, Stellungnahme zum PDSG v. 25. 5. 2020, Ausschuss-Dr. 19(14)165(25), S. 5, der das „Eigeninteresse“ der *gematik* an der Erfüllung ihrer gesetzlich übertragenden Aufgaben verneint.

138) BT-Dr. 19/18793, S. 100.

im Rahmen von Art. 4 Nr. 7 Halbs. 2 DSGVO zu beachtenden, oben skizzierten Maßstäbe der Verantwortlichkeit der DSGVO und des EuGH außer Acht, wenn er die Rechtsfigur der gemeinsamen Verantwortlichkeit ignoriert und die Alleinverantwortlichkeit den Leistungserbringern sowie Dienst- oder Anwendungsanbietern zuweisen will, die aber ohne die *gematik* de facto nicht vollständig allein insbesondere die wesentlichen Mittel der Datenverarbeitung bestimmen können. Die Festlegung in § 306 Abs. 2 i. V. mit § 307 SGB V ist auf eine artifizielle Trennung der Bereiche angelegt und spiegelt nicht die faktischen Umstände wieder, die sich mit einer Gesamtbetrachtung der Verarbeitungsvorgänge in einer vernetzten Infrastruktur erschließen dürften.

Es überzeugt auch nicht, wenn in der Gesetzesbegründung darauf abgestellt wird, wann eine Anwendung auf einer „operativen Ebene" durch Zusammenführung der Komponenten zur „Wirkung gebracht" wird[139]. Nach der Rechtsprechung des EuGH kommt es gerade nicht auf die Durchführung des „konkreten Datenverarbeitungsvorgangs" an. Er verlangt weder eine gleichwertige Verteilung der Einflussnahme auf Entscheidung über die Zwecke und Mittel[140] noch überhaupt Zugangs- bzw. Zugriffsmöglichkeiten auf Daten[141]. Dass letztlich nicht mehr von *gematik* gänzlich beherrschbare[142] Verarbeitungsprozesse in einer der informationstechnischen Teilsphären der TI ablaufen, kann sie jedoch nicht von der Verantwortung befreien[143]. Schon durch die „Festlegung von konzeptionellen und regulatorischen Vorgaben"[144] gemäß ihrer gesetzlichen Aufgabenzuweisung legt sie Funktionen und Steuerungen der verwendeten Programme näher fest und schafft damit die grundlegenden Strukturen für die Datenverarbeitung in der TI, welche durch andere Verantwortliche, wie Leistungserbringer und Anbieter von Diensten und Anwendungen, letztlich genutzt werden. Durch ihre Tätigkeit trägt die *gematik* maßgeblich zur Organisation und Kontrolle der Datenverarbeitung in allen Zonen der TI bei. Dieser überwiegend vorgelagerte Beitrag wirkt sich maßgeblich auf sämtliche späteren Verarbeitungsvorgänge aus. Die Übertragung einer Alleinverantwortlichkeit durch das PDSG auf Leistungserbringer und Anbieter von Diensten, die über die Zwecke und wesentliche Mittel tatsächlich nicht allein entscheiden kann, stellt hingegen das Verantwortlichkeitskonzept der DSGVO und letztlich einen effektiven Grundrechtsschutz in Frage. Die Nutzer der Komponenten sind hinsichtlich der wesentlichen Mittel auf die Unterstützung fachkundiger Stellen angewiesen, welche dafür die notwendigen Festlegungen getroffen haben. Aufgrund der Spezifikationen der *gematik* und damit beschränkter Beherrschbarkeit sowie Handlungsspielräume könnten die vermeintlich Verantwortlichen technisch nicht in der Lage sein, datenschutzrechtliche Pflichten zu erfüllen (z. B. „Datenpannen" abhelfen) oder Betroffenenrechten zu entsprechen. Das hat der Gesetzgeber durchaus erkannt[145]. Über eine stattdessen nach vorstehenden Maßstäben zu bestimmende gemeinsame Verantwortlichkeit muss auch im Verhältnis der Leistungserbringer zu Anbietern von Diensten und der weiteren Akteure zueinander[146] nachgedacht werden, weil die einzelnen Zonen der TI nicht losgelöst voneinander betrieben werden. Insoweit oblag es dem Gesetzgeber gem. Art. 26 Abs. 1 S. 2 DSGVO durch nationale Rechtsvorschriften festzulegen, wer von den gemeinsam Verantwortlichen welche konkrete Verpflichtung gemäß der DSGVO übernimmt.

An einer solchen transparenten Festlegung fehlt es nach wie vor. Soweit die Möglichkeit zur Benennung eines Verantwortlichen gem. Art. 4 Nr. 7, Halbs. 2 DSGVO der Komplexität der Verarbeitungsvorgänge und deren Umsetzung in der Praxis Rechnung tragen soll[147], ist § 307 SGB V misslungen. Zwar ist eine Kategorisierung nach „bestimmten Kriterien" zulässig. Die neuen Regelungen sind aber derart deutlich vom Bestreben getragen, die *gematik* aus der Verantwortung zu entlassen, dass dies zulasten der Klarheit geht. Erst unter Heranziehung der Gesetzesmaterialien, weiterer Vorschriften sowie von Kenntnissen zur TI wird eine Bestimmung des Verantwortlichen möglich. Nach Ansicht von Fachleuten lassen sich die technischen Details kaum von IT-Dienstleistern, geschweige denn von Ärzten und Patienten durchschauen[148]. Erst Recht mangelt es für die Betroffenen im Ergebnis an Transparenz, weil sie von außen nicht erkennen können, welchem Infrastrukturbaustein oder welchen Komponenten welcher Verantwortliche zuzuordnen ist. Die artifizielle Dezentralisierung der Verantwortlichkeit bedingt eine Verantwortungszerfaserung. Es ist durch die Aufsplittung nicht nur unklar, wer erster Ansprechpartner für Betroffenenrechte ist[149], sondern auch wer für Datenpannen[150], Schadensersatzansprüche und Maßnahmen der Aufsichtsbehörden für den Datenschutz verantwortlich ist. Immerhin ist von der *gematik* gem. § 307 Abs. 5 SGB V eine „koordinierende Stelle" zum Zweck der Erteilung von Auskünften über die Zuständigkeiten innerhalb der TI einzurichten. Das Instrument der „Anlaufstelle" ist nicht nur der gemeinsamen Verantwortlichkeit entlehnt[151], sondern die Notwendigkeit einer solchen Lotsenfunktion zeigt zugleich, von welcher Komplexität seiner Zuteilung der Gesetzgeber selbst ausgeht.

e) Datenschutz-Folgenabschätzung

Offen geblieben ist, wer etwa eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO durchzuführen hat[152]. Es kann wohl nicht angenommen werden, dass im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlagen für die TI eine DSFA erfolgte (Art. 35 Abs. 10 DSGVO). Den Gesetzesmaterialien ist dazu nichts zu entnehmen und die Technikoffenheit der Regelungen spricht eher dafür, dass eine DSFA nach konkreter Festlegung der gesetzlich vorgeprägten Mittel der Datenverarbeitung erfolgen muss. Dabei ist die DSFA isoliert für einzelne Zonen oder Komponenten der TI entsprechend der Aufteilung gem. § 306 Abs. 2 i. V. mit § 307 Abs. 1–4 DSGVO kaum sinnvoll durchführbar.

139) BT-Dr. 19/18793, S. 101; ähnl. wohl *Heckmann*, Stellungnahme zum PDSG v. 25. 5. 2020, Ausschuss-Dr. 19(14)165(25), S. 4, 6.
140) EuGH, JZ 2018, 1154, 1157, Rdnr. 43; NJW 2019, 285, 290, Rdnr. 66; MMR 2019, 579, 581, Rdnr. 70.
141) Vgl. EuGH, JZ 2018, 1154, 1156, Rdnr. 38; NJW 2019, 285, 290, Rdnr. 69; MMR 2019, 579, 581, Rdnr. 69.
142) Beachte aber die Befugnis zur Sperrung von Komponenten und Diensten gem. § 329 Abs. 3 SGB V.
143) Vgl. EuGH, JZ 2018, 1154, 1156, Rdnr. 40.
144) BT-Dr. 19/18793, S. 101.
145) Vgl. BT-Dr. 19/18793, S. 102.
146) Für Leistungserbringer und andere Nutzer der TI, die unabhängig voneinander Daten in Anwendungen dieses Netzwerkes übermitteln, liegt dagegen in der Regel eine getrennte Verantwortlichkeit nahe; vgl. *Artikel-29-Datenschutzgruppe*, WP 169 v. 16. 2. 2010, S. 22.
147) *Kühling/Martini et al.,* Die DSGVO und das nationale Recht, S. 25 m. w. N.
148) *Gieselmann*, c't 19/2020, S. 32.
149) S. schon die Krit. zum RefE des LfDI BaWü, Pressemitteilung v. 27. 2. 2020; BR, BT-Dr. 19/19365, S. 7.
150) Zum Ausfall der TI von Mai bis Juli 2020 s. *Gieselmann*, c't 19/2020, S. 32 m. w. N.
151) Art. 26 Abs. 1 S. 3 DSGVO; a. A. *Heckmann*, Stellungnahme zum PDSG v. 25. 5. 2020, Ausschuss-Dr. 19(14)165(25), S. 6 f: Art. 9 Abs. 4 DSGVO.
152) Die Ausführungen in BT-Dr. 19/18793, S. 100, die sich isoliert auf die Arztpraxis und nicht auf die (Anwendungen und Dienste der) Infrastruktur konzentrieren, sind für diese Frage nicht weiterführend. Näher zur DSFA s. *Dochow,* MedR 2019, 646 ff.; *Dochow*, in: *Dochow* et al., Datenschutz in der ärztlichen Praxis, 2019, S. 99 ff.

Denn sie ist für einzelne Komponenten der TI faktisch nicht möglich, wenn keine geeigneten Abhilfemaßnahmen gegen festgestellte Risiken ergriffen werden könnten, weil eine Dispositionsmöglichkeit für Leistungserbringer oder Anbieter von Diensten nicht besteht[153]. Es bedarf mithin einer Betrachtung des gesamten Systems[154].

3. Anwendungen der Telematikinfrastruktur

a) Verpflichtende und freiwillige Anwendungen

Die Anwendungen der TI werden in weiten Teilen übernommen und weiterentwickelt. Trotz der neuen Gliederung lässt sich die Unterteilung in Pflichtanwendungen und freiwilligen Anwendungen aufrechterhalten. Zu den *Pflichtanwendungen* gehören weiterhin das VSDM gem. §291b Abs. 2 SGB V[155], der Auslandsversicherungsnachweis (EHIC) gem. §291a Abs. 3 Nr. 5 SGB V und, nach zwischenzeitlicher Streichung, wieder das früher sog. eRezept[156], also elektronische Verordnungen i. S. v. §334 Abs. 1 S. 2 Nr. 6, §360 SGB V. Ebenfalls hierzu zählen wohl elektronische Überweisungen (§86a SGB V), die perspektivisch über die TI abgewickelt werden sollen.

Zu den *freiwilligen Anwendungen* gem. §334 Abs. 1 S. 2 SGB V zählen die elektronische Patientenakte (Nr. 1, §§341–355 SGB V), elektronische Erklärungen zu Organ- und Gewebespende bzw. Hinweise zu Vorhandensein und deren Aufbewahrungsort (Nr. 2), Hinweise zu Vorhandensein und Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen (Nr. 3), der eMP (Nr. 4, §31a Abs. 3 S. 3 i. V. m. §358 SGB V) und die NFD (Nr. 5, §358 SGB V). Der elektronische Arztbrief[157] wird Teil der ePA[158]. Für die ePA, die NFD und den eMP wird die Freiwilligkeit im Gesetz nochmals ausdrücklich hervorgehoben[159]. Wie für die anderen freiwilligen Anwendungen ergibt sich das bereits aus dem Einwilligungserfordernis.

b) Offenheit für neue Anwendungen

Die Anwendungen sind in §334 Abs. 1 S. 2 SGB V jetzt abschließend aufgeführt[160]. Das Gesetz ist gleichwohl entwicklungsoffen[161] und sieht perspektivisch weitere Anwendungen ohne Einsatz der eGK und zur Verwendung bei der Forschung nach §306 Abs. 1 S. 2 Nr. 2 SGB V vor. Die *gematik* kann gem. §334 Abs. 3 SGB V Festlegungen und Maßnahmen für zusätzliche Anwendungen der TI treffen, die insbesondere dem weiteren Ausbau des elektronischen Austausches von Befunden, Diagnosen, Therapieempfehlungen, Behandlungsberichten, Formularen, Erklärungen und Unterlagen dienen. Eine Zulassung gem. §325 Abs. 1 SGB V darf aber erst erfolgen, wenn die erforderlichen gesetzlichen Rahmenbedingungen (u. a. Zugriffsregelungen) erlassen worden sind. Weitere Anwendungen können gem. §327 SGB V zugelassen werden oder sollen entwickelt werden. Dazu zählen sichere Übermittlungsverfahren für die Kommunikation der Leistungserbringer gem. §311 Abs. 1 Nr. 5; Abs. 6 SGB V. Damit sind auch moderne Kommunikationsformen wie Messenger Dienste[162] angesprochen.

c) Anspruch auf Notfalldatensatz

Die Bereitstellung der Notfalldaten gehört zu den ersten nutzbringenden Anwendungen der TI für die medizinische Gesundheitsversorgung[163]. Sie können Daten zu Befunden, Daten zur Medikation oder Zusatzinformationen über den Versicherten enthalten[164]. Um die Anwendung zu fördern, erhalten Patienten nun dezidierte Ansprüche gegenüber Ärzten zur Anlage und Aktualisierung[165].

d) Fortentwicklung elektronischer Verordnungen, Empfehlungen und Überweisungen

Die Regelungen für Verordnungen in elektronischer Form sind bereits maßgeblich durch das GSAV und DVG geändert worden, wobei das eRezept insbesondere von der eGK entkoppelt wurde[166]. Die Regelungen werden mit dem PDSG fortgeschrieben (§334 Abs. 1 S. 2 Nr. 6, §360 SGB V)[167]. Die Einführung der eVerordnung erfolgt gem. §360 Abs. 2, Abs. 3 SGB V ab dem 1.1.2022. Es ist die erste patientenbezogene digitale Pflichtanwendung[168]. §360 Abs. 2 S. 2 und Abs. 3 S. 2 SGB V regeln Ausnahmen von der Verpflichtung für den Fall der technischen Unmöglichkeit. Perspektivisch sollen auch Verordnungen von Heil- und Hilfsmitteln, sonstiger Medizinprodukte sowie von häuslicher Krankenpflege elektronisch über die TI erfolgen[169]. Um verschiedene eVerordnungen, z. B. für apothekenpflichtige Arzneimittel, für Betäubungsmittel und Arzneimittel nach §3a Abs. 1 S. 1 AMVV (sog. T-Rezept), häuslicher Krankenpflege oder Soziotherapien, medienbruchfrei zu ermöglichen, muss die *gematik* zu bestimmten Zeitpunkten entsprechende Vorgaben erarbeitet haben (§312 Abs. 1 SGB V)[170]. Ferner soll gem. §86 Abs. 3 SGB V ein elektronischer Vordruck für das „Grüne Rezept" festgelegt werden, um bei Empfehlungen von apothekenpflichtigen, nicht verschreibungspflichtigen Arzneimitteln im Wege der Selbstmedikation Medienbrüche zu vermeiden und die elektronische Übermittlungsform über Anwendungen der TI gem. §334 Abs. 1 S. 2 SGB V vorzubereiten. Entsprechendes wird zur Fortentwicklung der „Digitalisierung des Formularwesens"[171] im Vertrags(zahn)arztrecht für elektronische Überweisungen in §86a SGB V geregelt[172].

Ferner soll eine eRezept-App für die Übermittlung von eVerordnungen über mobile Endgeräte der Versicherten entwickelt werden. Den Auftrag zur Entwicklung und Zurverfügungstellung bis zum 30.6.2021 erhält die *gematik*[173]. Die App kann Schnittstellen zu „Mehrwertangeboten von Drittanbietern" enthalten, sodass auch Apps anderer Anbieter in Betracht kommen[174]. Dies wirft natürlich datenschutzrechtliche Folgefragen für die Verarbeitung in den Drittanbieter-Apps auf.

153) Vgl. Bundesärztekammer, Stellungnahme zum DVG v. 9.10.2020, S. 15.
154) Vgl. FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.), Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-App, Version 1.0 v. 29.6.2020, S. 9f.
155) Zur verfassungsrechtlichen Rechtfertigung s. nur *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, §291a SGB V, Rdnrn. 14ff. m. w. N. aus der Rspr.
156) S. dazu *Dochow*, Telematik im Gesundheitswesen, 2017, S. 134ff., 1006ff. (auch zu §291a Abs. 2 Nr. 1 a. F. vor dem 19.12.2019); *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, §291a SGB V, Rdnrn. 40ff.
157) §291a Abs. 3 S. 1 Nr. 2 SGB V a. F.
158) §341 Abs. 2 Nr. 1 lit. d, §349 SGB V; s. a. §383 SGB V (§291f SGB V a. F.).
159) §341 Abs. 1 S. 2, §358 Abs. 1 S. 2, Abs. 2 S. 2 SGB V.
160) Zur bisher offenen Konzeption des §291a SGB V s. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1280ff.
161) Vgl. BT-Dr. 19/18793, S. 108.
162) BT-Dr. 19/18793, S. 103.
163) BT-Dr. 19/18793, S. 103.
164) §358 Abs. 1 S. 2 SGB V.
165) §358 Abs. 3 SGB V.
166) S. dazu *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, §291a SGB V, Rdnr. 42; *Weyd*, MedR 2020, 183, 191.
167) Näher *Braun*, PharmR 2020, 315, 318ff.
168) Vgl. auch BT-Dr. 19/18793, S. 127.
169) BT-Dr. 19/18793, S. 127; BReg., BT-Dr. 19/21743, S. 3.
170) BT-Dr. 19/18793, S. 103f., BT-Dr. 19/20708, S. 182; näher *Braun*, PharmR 2020, 315, 318f.
171) BT-Dr. 19/18793, S. 93.
172) S. a. §312 Abs. 5 SGB V.
173) §311 Abs. 1 Nr. 10, §360 Abs. 5, §312 Abs. 4 SGB V, s. a. BT-Dr. 19/18793, S. 103.
174) BT-Dr. 19/18793, S. 103; s. a. *Braun*, PharmR 2020, 315, 319.

4. Datenverarbeitungszwecke

Wie bisher ist die Datenverarbeitung innerhalb der TI auf einen bestimmten Zweck angelegt: Nach § 335 SGB V und den Bestimmungen zu den Zugriffsregelungen (§§ 352, 357, 359 und 361 SGB V) ist einem Berechtigten jeweils ein Zugriff erlaubt, soweit dies für die „Versorgung des Versicherten" erforderlich ist. Das umfasst die medizinische und pflegerische Versorgung. Für die Anwendungen zu Erklärungen zur Organ- und Gewebespende besteht nachvollziehbar keine solche Begrenzung[175]. Ferner konkretisieren die einzelnen Anwendungen die Verarbeitungszwecke.

Daneben sind schon seit dem eHealth-Gesetz vereinzelt Erweiterungen vorgenommen worden, wie z. B. die Verarbeitung von Daten zu Forschungszwecken[176], die nun fortgeschrieben werden (zur Datenspende s. VI.). Ansonsten werden Verarbeitungszwecke durch die Aufnahme weiterer, neuer Anwendungen statuiert. Unabhängig davon gehen aber auch mit der Einführung von neuen Zugriffsberechtigungen einige Zweckerweiterungen einher: Ein neuer Zugriffszweck ist die „Erfüllung von Aufgaben, die der für den Öffentlichen Gesundheitsdienst (ÖGD) zuständigen Behörde nach dem Infektionsschutzgesetz zugewiesen sind" (§ 352 Nr. 16, 17 SGB V). Für welche Zwecke Betriebsärzte sich unter Zugriff auf die Gesundheitsdaten einen besseren Überblick über den Gesamtzustand eines Arbeitnehmers verschaffen sollen (§ 352 Nr. 18 SGB V), bleibt offen. Die hintergründigen Verarbeitungsbefugnisse der Krankenkassen erweitern ebenfalls die bisherigen Zwecke (z. B. Versorgungsplanung und strategische Entscheidungen, s. dazu V.).

5. Zugriffskonzept

Das Zugriffskonzept in der TI ist weiterhin gekennzeichnet von normativen Vorgaben insbesondere zu Zweckbeschreibungen (s. o.), eines Einwilligungsvorbehaltes und der abstrakten Bestimmung des Kreises der Zugriffsberechtigten. Zusammen mit dem Verzeichnisdienst sind damit die wesentlichen Voraussetzungen dafür gegeben, dass auf Anwendungen und Inhalte differenziert zugegriffen werden kann. Flankiert wird dies durch technische Zugriffserfordernisse. Die Regelungen basieren in weiten Teilen auf den bisherigen Grundsätzen[177].

a) Freiwilligkeitsprinzip: Einwilligung und technische Zugriffsfreigabe

Grundlegende Voraussetzung für den Datenzugriff ist die Einwilligung des Versicherten gem. § 339 Abs. 1 S. 1 SGB V[178]. Hierauf nehmen weitere Vorschriften Bezug, wie etwa § 352 SGB V[179]. Es ist schon seit dem TSVG für die meisten Anwendungen kein zweistufiges Einwilligungskonzept[180] mehr vorgesehen, da das Erfordernis der Einwilligung zur Initialisierung freiwilliger Anwendungen entfallen ist. Anders ist dies jetzt wieder für die ePA, weil diese Anwendung erst auf Antrag des Versicherten eingerichtet wird (§ 341 Abs. 1 S. 1 SGB V). Die informationelle Selbstbestimmung des Versicherten wird dort also doppelt abgesichert.

Hinsichtlich der Einwilligung bestehen keine Regelungsmöglichkeiten für den nationalen Gesetzgeber. Es gelten die Voraussetzungen gem. Art. 7, Art. 4 Nr. 11 DSGVO und, da es sich um Gesundheitsdaten handelt, nach Art. 9 Abs. 2 lit. a DSGVO. Wie § 339 Abs. 1 S. 2 SGB V in Wiederholung von Art. 4 Nr. 11 DSGVO jetzt klarstellt, wird die Erklärung im Wege einer „eindeutigen bestätigenden Handlung" durch technische Zugriffsfreigabe zugelassen. Dadurch soll gewährleistet sein, dass ein aktives Tätigwerden des Versicherten erforderlich ist[181]. Was sich hinter dem Rechtsbegriff verbirgt, wird nicht erläutert. Bisher war eine „Autorisierung"[182], z. B. durch die Eingabe eines PINs[183] oder mittels Fingerprint möglich, wovon Ausnahmen z. B. für den NFD statuiert waren[184]. Für die ePA soll die Freigabe auch mittels der Benutzeroberfläche eines geeigneten Endgeräts möglich sein[185]. Die „technische Zugriffsfreigabe" dürfte diese Formen umfassen. Soweit die technische Zugriffsfreigabe nicht für einzelne Anwendungen ganz entbehrlich ist[186], erfolgt sie im Übrigen über die dezentrale Infrastruktur der Leistungserbringer im Praxisverwaltungssystem, also wohl durch PIN-Eingabe.

Die Einwilligung gem. § 339 Abs. 1 SGB V weicht daher von den Voraussetzungen gem. Art. 9 Abs. 2 lit. a DSGVO ab, weil das Ausdrücklichkeitsgebot nicht gewahrt werden kann, wenn die Zustimmung zum Datenzugriff mittels der eGK oder durch eine andere „technische Zugriffsfreigabe" erfolgt. Es handelt sich um einen schlüssigen Akt der Erklärungsabgabe, der konkludent und gerade nicht ausdrücklich vollzogen wird[187]. Diese Modifikation der Einwilligungsvoraussetzungen[188] sind gem. Art. 9 Abs. 4 DSGVO und ErwG 53, S. 4 DSGVO zulässig, denn danach sind nicht nur zusätzliche Beschränkungen, sondern ebenfalls Erleichterungen im nationalen Recht möglich[189], wenn diese als „zusätzliche Bedingungen" für die jeweiligen Schutzzwecke geeignet, erforderlich und angemessen sind[190]. Die vorgesehene Unterstützung der Erklärungsabgabe durch ein technisches Verfahren gem. § 339 SGB V bewirkt den Schutz der Gesundheitsdaten gleichermaßen wie eine ausdrückliche Einwilligung. Im Vergleich zu konventionellen Einwilligungsverfahren, die vor einer Datenverarbeitung meist in Schriftform und mittels umfangreicher Einwilli-

175) S. dazu § 356 SGB V, bisher nicht so klar in § 291a Abs. 5a S. 1 SGB V a. F.
176) Bisher § 291a Abs. 7 S. 3 SGB V a. F.
177) S. zu den bisherigen Regelungen *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1049 ff.
178) Unverständlich ist BT-Dr. 19/18793, S. 127, wonach es sich um eine „gesetzliche Befugnisnorm" handeln soll. Dafür fehlt im Gesetz und der Begründung jeder Anhaltspunkt (z. B. zur einschlägigen Öffnungsklausel).
179) Teilweise wird das Einwilligungserfordernis wiederholt, § 356 Abs. 2, § 357 Abs. 2 S. 1 SGB V.
180) Dazu *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1117 ff.; *Schifferdecker*, in: KassKomm, 110. EL, Juli 2020, § 291a SGB V, Rdnr. 71.
181) S. zu § 352 SGB V in BT-Dr. 19/18793, S. 122.
182) § 291a Abs. 5 S. 2 SGB V a. F.
183) Die eGK wird weiterhin mit einer PIN ausgestattet sein, vgl. § 336 Abs. 5 SGB V.
184) § 291a Abs. 5 S. 3 SGB V a. F.
185) § 354 Abs. 2 Nr. 2 SGB V; s. a. unter IV.
186) § 356 Abs. 2, § 357 Abs. 2, § 359 Abs. 2, Abs. 3 S. 2 SGB V.
187) Zum bisherigen Recht *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1066 f., 1068 f.
188) Trotz des Bezugs auf die Einwilligung in § 339 Abs. 1 S. 2 SGB V („hierzu"), könnte auch vertreten werden, dass die technische Zugriffsfreigabe zusätzlich zur ausdrücklichen Einwilligung erfolgen muss, vgl. zu § 352 SGB V in BT-Dr. 19/18793, S. 122 („darüber hinaus").
189) *Weichert*, in: *Kühling/Buchner*, DS-GVO BDSG, 3. Aufl. 2020, Art. 9, Rdnr. 150; *Dochow*, GesR 2016, 401, 407; *Dochow*, Telematik im Gesundheitswesen, 2017, S. 434. Entgegen *Schiff*, in: *Ehmann/Selmayr*, DS-GVO, 2. Aufl. 2018, Art. 9, Rdnr. 64 geht es dabei nicht darum, die Grenzen von Art. 9 Abs. 2 DSGVO zu verlassen und „weitere Ausnahmen zum Verbotsgrundsatz" zuzulassen, sondern in dem vorgegebenen Rahmen bei der Ausgestaltung der nationalen Normen strengere oder mildere Bedingungen zu statuieren, insoweit auch „*zusätzliche*" Bedingungen, *einschließlich*" Beschränkungen".
190) *Weichert*, in: *Kühling/Buchner*, DS-GVO BDSG, 3. Aufl. 2020, Art. 9, Rdnr. 150. Nach einer anderen Auffassung sind zusätzliche Bedingungen und Formerfordernisse als „Minus" zur Untersagung der Einwilligung durch mitgliedstaatliches Recht nach Art. 9 Abs. 1 lit. a DSGVO zulässig, so *Kühling/Martini et al.,* Die DSGVO und das nationale Recht, S. 50, die damit aber Art. 9 Abs. 4 DSGVO außer Acht lassen.

gungserklärungen erfolgen, wird der Grad der informationellen Einflussnahme auf die Datenverarbeitung durch das technisch-intuitive Einwilligungskonzept sogar erhöht. Der sinnvolle Einsatz technischer Steuerungsinstrumente macht die Einwilligung mehr zum Werkzeug der Mitwirkung bei der Informationsverarbeitung. Informationelle Selbstbestimmung kann auf diese Weise noch effektiver sichergestellt werden. Das rechtfertigt eine Abweichung vom Ausdrücklichkeitsgebot. Die übrigen zusätzlichen Bedingungen, welche zu weiteren Beschränkungen führen, wie der gesetzliche Einwilligungsvorbehalt[191], die konturierenden Regelungen u. a. zum Zweck der Datenverarbeitung mit einer Limitierung des Kreises der zur Datenverarbeitung generell Zugriffsberechtigten[192] dürften ebenfalls von Art. 9 Abs. 4 DSGVO gedeckt sein.

Auf Erklärungen zur Organ- und Gewebespende kann, wie bisher, nach dem Tod des Versicherten auch ohne Einwilligung zugegriffen werden (§ 356 Abs. 3 SGB V). Auf Hinweise zu Vorsorgevollmachten und Patientenverfügungen kann ohne Einwilligung des Versicherten zugegriffen werden, wenn eine ärztlich indizierte Maßnahme unmittelbar bevorsteht und der Versicherte nicht fähig ist, in die Maßnahme einzuwilligen (§ 357 Abs. 3 SGB V). Ebenfalls wie nach bisherigem Recht kann gem. § 359 Abs. 3 S. 1 Nr. 1 SGB V auf die Notfalldaten ohne Einwilligung zugegriffen werden, soweit das für die Versorgung des Versicherten in einem Notfall erforderlich ist. Soll der NFD als „kleine Patientenakte" außerhalb eines Notfalls verwendet werden, ist dies mit der Einwilligung des Versicherten unter den Voraussetzungen von § 359 Abs. 3 S. 1 Nr. 1 SGB V zulässig. Auch für die Freigabe von Gesundheitsdaten aus der ePA für Forschungszwecke besteht ein vorgeschaltetes Einwilligungserfordernis (§ 363 SGB V)[193].

b) Drei-Karten-Prinzip

Die Einwilligung wird flankiert von einem technischen Zugriffsverfahren, das neben der erforderlichen technischen Zugriffsfreigabe jetzt grundsätzlich auf einem Drei-Karten-Prinzip basiert[194]. Nach den Vorgaben zu den Zugriffsvoraussetzungen dürfen auf die freiwilligen Anwendungen gem. § 334 Abs. 1 S. 2 Nr. 1–5 SGB V generell Zugriffsberechtigte im Einzelfall im Grundsatz nur mittels eGK und eHBA[195] in Verbindung mit einer SMC-B[196] zugreifen (§ 339 Abs. 3 SGB V). Die Komponente zur Authentifizierung von Leistungserbringerinstitutionen (Institutionskarte, SMC-B), die an den eHBA bzw. Berufsausweis gekoppelt ist[197], ist nun zusätzlich erforderlich[198]. Sie weist eine Einheit oder Organisation des Gesundheitswesens, z. B. Praxis, Apotheke, Krankenhaus oder Organisationseinheit eines Krankenhauses, aus[199] (daher auch Praxisausweis). Von dem Drei-Karten-Prinzip werden in § 339 Abs. 4 SGB V Ausnahmen statuiert[200].

c) Keine „Datenhoheit" bei elektronischen Verordnungen?

Der Zugriff auf eVerordnungen i. S. v. § 334 Abs. 1 S. 2 Nr. 6, § 360 SGB V ist nach §§ 361, 339 Abs. 2 SGB V – wie bisher nach altem Recht – ohne eGK und ohne Einwilligung des Versicherten zulässig. Zwar soll die Legitimation der Datenverarbeitung nach der Gesetzesbegründung auf eine Einwilligung des Versicherten und eine gesetzliche Grundlage des § 339 Abs. 2 SGB V gestützt sein, obwohl an anderer Stellen von der Verpflichtung die Rede ist[201]. Im Gesetzestext findet sich indes kein Einwilligungserfordernis. § 361 SGB V wird weder von § 339 Abs. 1 SGB V in Bezug genommen noch statuiert die Vorschrift selbst ein Einwilligungserfordernis. Im Umkehrschluss aus § 339 Abs. 1 SGB V ergibt sich daher, dass für Zugriff auf eVerordnungen kein Einwilligungserfordernis besteht[202]. Die freie Entscheidung des Versicherten liegt hier aber in dem Umstand der Entscheidung über die Einlösung des Rezepts begründet[203]. Nach dem vorgesehenen Verfahren soll dies gegenüber zugriffsberechtigten Leistungserbringern erfolgen, beispielsweise mittels einer Erkennungsmarke in einem Kommunikationsnetz, welche die Sendeberechtigung zum Abruf der elektronischen Verordnungsdaten enthält[204]. Der eVerordnung ist eine Erkennungsmarke (Token) zugeordnet, welche die Einsicht, Zuweisung und den Abruf ermöglicht[205]. Das eRezept-Token ist faktisch das elektronische Äquivalent zum Papierrezept und kann wahlweise durch einen Ausdruck in Papierform oder elektronisch bereitgestellt werden (§ 360 Abs. 4 SGB V) sowie in einer eRezept-App direkt elektronisch an eine Apotheke übermittelt werden[206]. Dadurch erhält der Versicherte Auswahl- und Steuerungsmöglichkeiten. Ein Zugriff durch Berechtigte erfordert den Einsatz des eHBA oder eines entsprechenden elektronischen Berufsausweises jeweils in Verbindung mit der SMC-B (§ 361 Abs. 2 S. 1 SGB V)[207]. Im Übrigen mangelt es für die Pflichtanwendung an Ausführungen zur Verhältnismäßigkeit der u. U. verbleibenden Grundrechtseingriffe (z. B. der Speicherung der Verordnungsdaten auf Servern) sowie an datenschutzrechtlich notwendigen und Bestimmungen u. a. zur Zweckbindung oder Speicherdauer[208].

d) Zugriffsregelungen: Kreis der generell Berechtigten

Nach einer wiederkehrenden Grundsystematik sind in § 352 SGB V (ePA), § 356 SGB V (elektronische Erklärungen zur Organ- und Gewebespende), § 357 SGB V (Hinweise zu Vorhandensein und Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen), § 359 SGB V (eMP, NFD) und § 361 Abs. 1 SGB V (eVerordnungen) ausdifferenzierte Zugriffsbefugnisse überwiegend nach Berufsgruppen abstrakt festgelegt. Auf die spezifischen Anforderungen der jeweiligen Anwendung und den damit verbundenen Versorgungsabläufen zugeschnitten[209]

191) S. dazu *Dochow*, Telematik im Gesundheitswesen, 2017, S. 714, 969 ff., 1001, 1167, 1327; *Dochow*, in: *Dochow* et al., Datenschutz in der ärztlichen Praxis, 2019, S. 64 f.; *Dochow*, GuP 2020, 129, 145; s. noch *Schifferdecker*, in: KassKomm, 95. EL, Juli 2017, § 291a SGB V, Rdnrn. 70 ff., dag. allg. zu einer gesetzlichen Verarbeitungsgrundlage mit „Zustimmungsvorbehalt" *Schantz*, in: *Simitis* et al., Datenschutzrecht, 1. Aufl. 2019, Art. 6, Rdnr. 14; vgl. *Sackmann*, PinG 2019, 277, 279.

192) Hierunter werden diejenigen Personen und Institutionen verstanden, denen nach den Zugriffsnormen (z. B. §§ 352, 356, 357 SGB V, s. unter d) ein genereller Zugriff auf Anwendungen eingeräumt wird, auch wenn die Legitimation und Autorisierung im Einzelfall von der Einwilligung des Versicherten abhängt.

193) Dazu näher unter VI.

194) Zum bisherigen Zwei-Karten-Prinzip s. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1059 ff.; *Dochow/Kreitz*, ZfmE 2018, 147, 154.

195) Für Personen, die nicht über einen eHBA verfügen, ist nach § 339 Abs. 5 SGB V auch ein Zugriff ohne eHBA zulässig, wenn hierzu eine Autorisierung durch einen eHBA-Inhaber erfolgt.

196) Zu den Abkürzungen s. III., 1.

197) S. § 340 Abs. 5 SGB V.

198) Bisher nicht rechtlich vorgesehen, s. *Dochow/Kreitz*, ZfmE 2018, 147, 154.

199) BT-Dr. 19/18793, S. 110.

200) Zur ePA s. näher IV.

201) BT-Dr. 19/18793, S. 129 u. S. 127.

202) S. schon zum alten Recht *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1172 ff., 1249.

203) S. a. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1249.

204) BT-Dr. 19/18793, S. 110, 128, 130; zur Kritik am Verfahren, weil der Token nicht mehr der Sicherheit der TI unterliegt, s. *Mand/Meyer*, A&R 2020, S. 147, 163 u. 165.

205) BT-Dr. 19/18793, S. 128.

206) BT-Dr. 19/18793, S. 103.

207) Zu Ausnahmen s. § 360 Abs. 3 SGB V.

208) S. zur Krit. näher BfDI, Stellungnahme zum PDSG v. 25. 5. 2020, S. 16.

209) Vgl. zur bisherigen Regelung *Dochow/Kreitz*, ZfmE 2018, 147, 154 f.

erhalten z. B. Ärzte, Apotheker oder Psychotherapeuten die Zugriffsbefugnis im für den Verarbeitungszweck erforderlichen Umfang. Daneben sind berufsmäßige Gehilfen vorgesehen, die zumeist im Rahmen der von ihnen zulässigerweise zu erledigenden Tätigkeiten zum Zugriff berechtigt sein sollen. Die Zugriffsbestimmungen sind weiterhin strafrechtlich abgesichert (§ 397 SGB V), um unberechtigte Zugriffe auszuschließen.

Im Rahmen der Zugriffsregelungen wird eine Anbindung weiterer Berufsgruppen vollzogen oder perspektivisch angestrebt, damit die digitale Vernetzung aller Akteure des Gesundheitswesens[210] vorangetrieben werden kann. Insoweit sind im Rahmen der ePA (§ 352), des eMP und der NFD (§ 359 SGB V) sowie der eVerordnungen (§ 361 SGB V) nun auch berufsmäßige Gehilfen in Vorsorge- und Rehabilitationseinrichtungen zugriffsberechtigt[211]. Weitere Akteure, wie Amtsärzte, Betriebsärzte, Hebammen, Physiotherapeuten oder – wegen der Anbindung von Pflegeeinrichtungen an die TI[212] – Pflegepersonal, erhalten nun ebenfalls Zugriffsrechte[213] oder sollen schrittweise folgen.

Der Versicherte kann aus dem Kreis der so vorfestgelegten generell Zugriffsberechtigten ausweislich § 337 Abs. 3 SGB V Zugriffsberechtigungen erteilen. Erst dadurch sowie im Zusammenspiel mit der einer Einwilligung und der technischen Zugriffsfreigabe (§ 339 Abs. 1 SGB V), soweit diese nicht entbehrlich sind, verdichtet sich die Erteilung der Zugriffsberechtigung auf eine bestimmte Person.

Für welche Dauer das Zugriffsrecht jeweils eingeräumt wird, lässt weder § 337 SGB V noch § 339 SGB V erkennen. In der Gesetzesbegründung wird ausgeführt, dass Leistungserbringer für die Dauer des eingeräumten Zugriffsrechts auch ohne Einsatz der eGK bzw. in Abwesenheit des Versicherten auf Daten des Versicherten in einer elektronischen Patientenakte zugreifen können.[214]

e) Elektronischer Verzeichnisdienst

§ 313 SGB V enthält die Regelungen zum Verzeichnisdienst der Telematikinfrastruktur (VZD), die überwiegend schon mit dem DVG in § 291h SGB V a. F. eingeführt wurden[215] und nun geringfügig ergänzt werden. Der VZD dient vor allem dazu, Leistungserbringer innerhalb der TI auffinden und sicher identifizieren zu können. Das ist von Bedeutung, damit ihnen im Rahmen von Anwendungen der TI Zugriffsbefugnisse eingeräumt werden können oder sie im Übrigen adressiert werden können. Die Berufskammern, Kassen(zahn)ärztliche Vereinigungen und andere Stellen übermitteln die dafür erforderlichen Daten[216] der „Nutzer" auf der Grundlage von Art. 6 Abs. 1 lit. c DSGVO i. V. mit § 313 Abs. 5 S. 1 SGB V. Identifikationsmerkmale für Ärzte sowie Leistungserbringerinstitutionen sind die Arztnummer und Betriebsstättennummer[217]. Das Verfahren der Datenübermittlung kann die *gematik* als Betreiberin des VZD nach der Neuregelung in § 313 Abs. 4 S. 2 SGB V in einer Richtlinie festlegen. In § 313 Abs. 5 S. 2 SGB V ist seit dem PDSG nun berücksichtigt, dass u. a. die Berufskammern zur Erfüllung ihrer Datenlieferungspflicht ein von ihnen für ihre Mitgliederverwaltung betriebenes standardbasiertes System zur Verwaltung von Identitäten und Zugriffsrechten nutzen können, womit etwa Identity- und Access-Management-Systeme gemeint sein dürften. Anders als die Gesetzesbegründung lässt der Wortsinn der Regelung nicht erkennen, dass nur „vorhandene Systeme"[218] genutzt werden können. Das wäre aus technologischer Sicht auch nicht sinnvoll, sodass die neue Befugnisnorm nach Sinn und Zweck auch die (Fort-)Entwicklung solcher Systeme zulässt.

6. Schutz vor Drucksituationen und Benachteiligung

Das wichtige Verwendungs-, Verlangens- und Diskriminierungsverbot, das bisher in § 291a Abs. 8 SGB V geregelt war und dem Schutz des Karteninhabers vor Zugriffsverlangen durch nicht zugriffsberechtigte Dritte sowie der Absicherung der Freiwilligkeit der Versichertenentscheidung vor unsachgemäßen Kopplungen dienen sollte[219], bleibt in § 335 SGB V mit der Überschrift „Diskriminierungsverbot" im Wesentlichen erhalten. Die neue Vorschrift enthält allerdings mehr als lediglich ein Verbot der Diskriminierung, das nur in § 335 Abs. 3 SGB V geregelt ist.

§ 335 Abs. 2 SGB V dient der Verhinderung zweckwidriger Datenverarbeitungen, was nicht etwa nur ein Unterfall eines Diskriminierungsverbotes, sondern Ausprägung eines zentralen datenschutzrechtlichen Grundsatzes ist (Art. 5 Abs. 1 lit. b DSGVO). Weiterhin wird durch § 335 Abs. 1 und Abs. 2 SGB V ein Schutz vor bestimmten Druck- oder „Nötigungssituationen" in sozialen Abhängigkeitsverhältnissen z. B. durch Arbeitgeber, Versicherungen oder andere Dritte bereits im Vorfeld etwaiger unberechtigter Datenzugriffe intendiert. Die Vorschrift bleibt daher insgesamt eine wichtige Absicherung für das Freiwilligkeitsprinzip. Sie enthält letztlich aber auch eine gesetzliche Beschränkung der Dispositionsfreiheit des Versicherten, denn nicht er allein entscheidet im Sinne informationeller Selbstbestimmung darüber, wem er Informationen aus Anwendungen der TI preisgibt[220]. Das Gesetz statuiert damit Grenzen für die Einwilligungen des Versicherten, was von Art. 9 Abs. 4 DSGVO[221] gedeckt ist.

Es werden entgegen der Gesetzesbegründung vereinzelt Modifikationen vorgenommen, welche einerseits die Lesbarkeit der Norm durchaus verbessern, andererseits aber auch zu materiellen Änderungen führen: Zunächst wird konsequenterweise nicht mehr allein an die Inhaberschaft der eGK angeknüpft. Geschützt werden sollen die Versicherten vielmehr umfassend vor Zugriffsverlangen, Benachteiligungen und zweckwidrigen Datenverarbeitungen bezogen auf alle Anwendungen der TI, die von der eGK lediglich unterstützt[222] oder gar losgelöst[223] zum Einsatz kommen können und zum Teil in die ePA integriert sind. Nicht von § 335 SGB V erfasst sind zwar die Daten der eGK gem. § 291a Abs. 2 und 3 SGB V, die durchaus aufschlussreich und ebenfalls „sensibel" sein könnten. Sie sind aber der Disposition des Versicherten entzogen, sodass jedenfalls ein an ihn gerichtetes Verlangen i. S. v. § 335 Abs. 1 SGB V oder eine mit ihm zu treffende Vereinbarung i. S. v. § 335 Abs. 2 SGB V nicht in Betracht kommen dürfte. Der Schutz von § 335 SGB V bezieht sich demnach nur auf Daten, auf welche der Versicherte einen Zugriff einräumen könnte.

Auffällig ist, dass nunmehr nach § 335 Abs. 1 SGB V prinzipiell ein Zugriff auf Anwendungen der TI – auch durch die generell Zugriffsberechtigten – nicht verlangt

210) BT-Dr. 19/18793, S. 2.
211) S. a. § 312 Abs. 2, § 381 SGB V (perspektivisch verpflichtend, BT-Dr. 19/18793, S. 134); s. a. z. B. die Erweiterung in § 357 Abs. 1 Nr. 3 SGB V mit Angehörigen eines Pflegeberufs, die in einer Pflegeeinrichtung, einem Hospiz oder einer Palliativeinrichtung beschäftigt sind.
212) Vgl. § 312 Abs. 2, § 357 Abs. 1 Nr. 3 SGB V.
213) S. z. B. § 352 Nr. 13, 16, 18 SGB V.
214) BT-Dr. 19/18793, S. 110; für die ePA s. aber die Regelung zur Dauer des Zugriffsrechts in § 342 Abs. 2 Nr. 1 lit. e und f SGB V.
215) BT-Dr. 19/14687, S. 100.
216) S. § 313 Abs. 1 SGB V.
217) Für Eigeneinrichtungen, ausschließlich privat tätige Ärzte sowie Psychotherapeuten vergibt die KBV diese Nummern, § 313 Abs. 6 SGB V.
218) BT-Dr. 19/18793, S. 105.
219) *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1085 ff., 1155 f.
220) Zur Verfassungsmäßigkeit s. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1235 ff.
221) S. a. ErwG 53, S. 4 DSGVO.
222) § 334 Abs. 2 SGB V; bisher § 291a Abs. 3 S. 1 SGB V a. F.
223) § 334 Abs. 1 S. 2 Nr. 6 i. V. mit § 86 Abs. 3 SGB V (eVerordnungen).

werden darf. Bisher war lediglich ausgeschlossen, dass vom Karteninhaber verlangt werden kann, anderen als den gesetzlich Zugriffsberechtigten einen Zugriff zu gestatten. Da generell Zugriffsberechtigte, wie z. B. Ärzte, im Rahmen der Behandlung und im Einklang mit den Mitwirkungsobliegenheiten der Versicherten[224] durchaus den Zugriff auf z. B. die ePA anregen werden, wird maßgeblich sein, was unter dem Begriff des „Verlangens" zu verstehen ist. Bisher wurde darunter die an den Versicherten gerichtete Aufforderung verstanden, eine Zugriffsmöglichkeit einzuräumen[225]. In Ansehung der Sanktionsbewährung durch § 395 Abs. 1 SGB V muss aber jedenfalls im Wege der Auslegung deutlich werden, dass eine z. B. ärztliche Aufforderung, im Behandlungskontext etwaige Informationen aus der ePA zur Verfügung zu stellen, nicht gegen § 335 Abs. 1 SGB V verstößt und damit nicht zu einer Ordnungswidrigkeit führen kann. Ein anderes Ergebnis würde den mit den Anwendungen der TI verfolgten Zweck, nämlich Informationen für Behandlungen bereitzustellen, zuwiderlaufen.

Der ebenfalls wichtige Gedanke, dass nicht vereinbart werden darf, anderen als den gesetzlich Zugriffsberechtigten einen Zugriff zu gestatten, findet sich nunmehr in dem „Gestattungsvereinbarungsverbot" gem. § 335 Abs. 2 SGB V[226]. Damit wird etwa unterbunden, dass der Versicherte bei Abschluss von Versicherungsverträgen einem Dritten einen Datenzugriff einräumt.

Das fernerhin datenschutzrechtlich bedeutsame Verbot einer versorgungszweckwidrigen Datenverarbeitung findet sich so klar wie in der Vorgängervorschrift nicht mehr wieder. Bisher war die Datenverarbeitung auf den Zweck der „Versorgung der Versicherten, einschließlich der Abrechnung der zum Zwecke der Versorgung erbrachten Leistungen" begrenzt. Nunmehr wird in § 335 Abs. 2 SGB V auf die Zugriffsregelungen der einzelnen Anwendungen verwiesen, welche jedoch auch weitere Zwecke zulassen. So sind etwa Datenverarbeitungen zum Zweck der Gefahrenabwehr nach dem IfSG gem. § 352 Nr. 18, 19 SGB V durch Amtsärzte und Personal in Gesundheitsämtern zulässig. Ansonsten findet sich in den in Bezug genommenen Normen aber regelmäßig die Begrenzung auf den Zweck der „Versorgung der Versicherten", sodass nur punktuell von Zweckerweiterungen auszugehen ist. Dass die Vorschrift vollumfänglich das bisher in § 291a Abs. 8 SGB V geregelte Recht zum Verwendungs-, Vereinbarungs- und Diskriminierungsverbot enthält[227], ist aber auch vor diesem Hintergrund nicht zutreffend.

Eine Änderung ist auch die Erweiterung der Datenverarbeitung zu Forschungszwecken, welche die Gesetzesbegründung immerhin erwähnt. Dort heißt es aber, die Verarbeitung von Daten zu Forschungszwecken sei als „Ausnahmetatbestand vom Diskriminierungsverbot" statuiert[228]. Selbstverständlich ist eine Diskriminierung auch im Kontext der Forschung nicht erlaubt und Versicherte dürfen dementsprechend gem. § 335 Abs. 3 SGB V weder bevorzugt oder benachteiligt werden, wenn sie einen Zugriff auf Daten ihrer ePA zu Forschungszwecken verweigern. Das lässt sich entgegen der Begründung aus dem Normtext herauslesen. Gemeint ist in der Begründung wohl vielmehr, dass zu Forschungszwecken eine Abweichung von der bisher strengen Zweckbegrenzung gem. § 335 Abs. 2 SGB V erlaubt ist.

Das Benachteiligungsverbot, das bisher in § 291a Abs. 8 S. 2 SGB V a. F. geregelt war und unterschiedslos generell Zugriffsberechtigte und andere Personen adressiert, ist weiterhin nicht sanktionsbewehrt. Nach § 395 Abs. 1 SGB V handelt nur ordnungswidrig, wer entgegen § 335 Abs. 1 oder Abs. 2 SGB V handelt. Eine Benachteiligung des Versicherten aus sachlichem Grund, die sich etwa im Rahmen von Mitwirkungsobliegenheiten der Versicherten (s. z. B. § 66 SGB I) hält und insoweit sachlich gerechtfertigt sein kann, dürfte daher weiterhin zulässig sein[229].

7. „Patientensouveränität" durch spezifische Betroffenenrechte

Durch die im Rahmen der TI implementierten Werkzeuge zur Ausübung informationeller Selbstbestimmung (im PDSG sog. „Patientensouveränität") können die Interessen des Betroffenen entsprechend Art. 8 GRCh und dem Recht auf informationelle Selbstbestimmung umgesetzt werden. Dem Betroffenen sind viele praktische Möglichkeiten eröffnet, seine Rechte faktisch selbst zu realisieren. Dies wird zum Teil durch eigenständige Zugriffsbefugnisse des Versicherten auf Anwendungen möglich, was Auskünfte gem. Art. 15 DSGVO, Art. 8 Abs. 2 S. 2 GRCh, jedenfalls über die auf diese Weise erreichbaren Daten, entbehrlich macht. Das „Zugriffsrecht" des Versicherten in § 336 SGB V war zuvor schon rudimentär in § 291a Abs. 4 S. 2 SGB V a. F. geregelt und konnte als Einsichtsrecht der Patienten verstanden werden. Neu sind hingegen die umfangreichen Regelungen zur Realisierung des Einsichtsrechts[230] durch sehr umständlich formulierte Zugriffsregelungen, die aber Klarheit für die Versicherten schaffen sollen[231]: Jeder Versicherte ist gem. § 336 Abs. 1 SGB V berechtigt, auf Daten in einer Anwendung nach § 334 Abs. 1 S. 2 Nr. 1 bis 3 und 6 (ePA, persönliche Erklärungen, eVerordnungen) mittels seiner eGK barrierefrei zuzugreifen, wenn er sich für diesen Zugriff jeweils durch ein geeignetes technisches Verfahren authentifiziert hat. Ein Authentifizierungsmittel ist eine PIN[232]. Ein von der eGK unabhängiger Zugriff soll für die ePA gem. § 336 Abs. 2 SGB V zulässig sein[233]. Für die Anwendungen nach § 334 Abs. 1 S. 2 Nr. 4 und Nr. 5 (eMP, NFD) besteht ein Einsichtsrecht bei einem Leistungserbringer, der unter Einsatz der eGK mittels seines eHBA und SMC-B auf die Daten zugreifen kann (§ 336 Abs. 3 i. V. mit § 339 Abs. 3 SGB V). Der Zugriff in Verbindung mit einem eHBA in den Praxen entfällt ansonsten und muss über eine Benutzeroberfläche eines geeigneten Endgeräts durchgeführt werden. Für eVerordnungen kann für den Zugriff ohne eGK auch ein geeignetes technisches Verfahren zum Einsatz kommen, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet (§ 336 Abs. 4 SGB V).

Auch Protokolldaten i. S. v. § 309 SGB V sollen dem Versicherten zur Verfügung gestellt werden[234]. Gem. § 338 Abs. 1 SGB V müssen die Krankenkassen für das Auslesen dieser Daten Komponenten zur Verfügung stellen. Überdies bleiben Auskünfte gem. § 305 SGB V unberührt.

Weil der Versicherte ferner durch § 337 Abs. 1 SGB V Möglichkeiten erhält, Daten aus seiner ePA auszulesen und zu übertragen, kann zum Teil auch der Anspruch auf Datenportabilität (Art. 20 DSGVO) erfüllt sein. Außerdem darf der Versicherte gem. § 337 Abs. 1 SGB V Daten, die er selbst zur Verfügung gestellt hat, ebenso wie seine persönlichen Erklärungen (zur Organspende, Patientenverfügung) verarbeiten, also auch ändern.

Das Recht auf Löschung gem. Art. 17 DSGVO kann in bestimmten Umfang nach Maßgabe von § 337 Abs. 2 SGB V selbstständig durch den Versicherten ausgeübt werden. Davon ausgenommen sind nur NFD und der eMP. Hierfür besteht, wie auch für alle anderen Anwendungen

224) *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1132 ff.
225) *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1085 f.
226) Bisher § 291a Abs. 8 S. 1 Halbs. 2 SGB V a. F.
227) BT-Dr. 19/18793, S. 108.
228) BT-Dr. 19/18793, S. 108.
229) *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1132 ff., 1087.
230) S. dazu *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1216 ff.
231) BT-Dr. 19/18793, S. 108.
232) Zur Autorisierung nach bisherigem Recht s. *Dochow*, Telematik im Gesundheitswesen, 2017, S. 1050 ff.
233) S. dazu IV.
234) S. u. 11.

ein Recht, die Löschung von einem Zugriffsberechtigten zu verlangen.

Darüber hinaus werden spezifische Informationspflichten in § 314 SGB V geregelt. Danach muss die *gematik* in dem dort beschriebenen Umfang zahlreiche Informationen zur Verfügung stellen. Es handelt sich um Informationen, welche u. a. die Struktur und Funktionsweise der TI, die grundlegenden Anwendungsfälle und Funktionalitäten der ePA betreffen. Es soll über die Zwecke der Datenverarbeitung in der ePA und die damit verbundenen Datenverarbeitungsvorgänge informiert werden. Ferner ist der Versicherte über seine Zugriffsrechte und das Recht auf Löschung aufzuklären[235]. Weitere spezifische Informationspflichten zur ePA und zur NFD-Anwendung sowie zum eMP enthalten die §§ 343, 358 Abs. 6 SGB V. Bemerkenswert ist dabei der Hinweis auf die möglichen „versorgungsrelevanten Konsequenzen", die daraus resultieren können, dass Versicherte keine elektronische Patientenakte nutzen oder Daten aus dieser löschen wollen (§ 343 Abs. 1 S. 3 Nr. 20 SGB V). Unter Berücksichtigung der regelmäßigen Macht- und Informationsasymmetrie in Behandlungs- oder Versichertenverhältnissen könnte hieraus, je nach Ausgestaltung der Informationsmaterialien, ein Freiwilligkeitsproblem bezüglich der datenschutzrechtlichen Einwilligung des Versicherten gem. § 339 SGB V erwachsen.

Auch wenn sich die Informationen zum Teil decken, ersetzt diese Verpflichtung der *gematik* nicht die Pflicht der Verantwortlichen zur Information gem. Art. 13, 14 DSGVO, sodass die Pflicht aus der DSGVO weiterhin von den Verantwortlichen, z. B. Leistungserbringern, Krankenkassen und Anbietern von Diensten, zu erfüllen ist. Eine gesetzliche Zuweisung i. S. v. Art. 26 Abs. 1 S. 2 DSGVO wäre im Interesse der Betroffenenrechte zielführend gewesen, damit Informationen, die von verschiedenen Verantwortlichen an Betroffene herangetragen werden, sich nicht überschneiden oder gar widersprechen[236]. Ob die Rechte der Art. 12 ff. DSGVO vollständig erfüllt werden können, müsste noch näher untersucht werden. Hier dürfte aber ohnehin noch Entwicklungsbedarf bestehen, weil einige Fragestellungen (z. B. Berichtigung von medizinischen Daten in der ePA)[237] noch nicht berücksichtigt sind.

8. Einschränkung von Betroffenenrechten aufgrund sicherheitstechnischer Unmöglichkeit

§ 308 SGB V regelt den neuen Vorrang von technischen Schutzmaßnahmen vor der Realisierung von Rechten des Betroffenen gem. Art. 12 ff. DSGVO. Diese Rechte sind gem. § 308 Abs. 1 gegenüber den datenschutzrechtlichen Verantwortlichen ausgeschlossen, soweit sie nicht oder nur unter Umgehung von Schutzmechanismen, wie insbesondere der Verschlüsselung oder der Anonymisierung, gewährleistet werden könnten. Wegen dieser technischen Schutzmaßnahmen innerhalb der TI kann eine Kenntnisnahme oder Identifizierung des Betroffenen unter Umständen, z. B. für Anbieter der Dienste oder für die Krankenkassen als Verantwortliche für die ePA, ausgeschlossen sein. Um nicht dennoch den Schutz aufheben zu müssen, sind die Verantwortlichen also ausnahmsweise von ihrer Pflicht befreit. Zur bloßen Gewährleistung der Betroffenenrechte sollen sie keine (Re)Identifizierung des Anspruchstellers vornehmen müssen, indem sie zusätzliche Informationen aufbewahren, einholen oder verarbeiten sowie Sicherheitsvorkehrungen aufheben würden. Dies sei der Rechtsgedanke aus § 11 Abs. 1 DSGVO[238], der einer Konfliktlage zwischen Betroffenenrechten und Datensparsamkeit und gerade der Sicherung der Betroffenenrechte Rechnung tragen soll[239]. Die in § 11 Abs. 2 DSGVO erwähnte Unterrichtungspflicht wird in diesen Gedanken indes nicht einbezogen. Die Anforderungen gem. Art. 11 DSGVO sind für den Fall der unmöglichen Identifizierbarkeit vorrangig zu berücksichtigen, weil insoweit keine Regelungszuständigkeit für den nationalen Gesetzeber besteht. Zusätzlich können Einschränkungen der Betroffenenrechte nach anderen Vorschriften zum Tragen kommen, denn die §§ 32 ff. BDSG[240] und der §§ 82 ff. SGB X werden durch § 308 SGB V nicht verdrängt.

Nach der Rückausnahme gem. § 308 Abs. 2 SGB V kann das Recht des Betroffenen jedoch nicht beschränkt werden, wenn berechtigte Zweifel an der behaupteten Unmöglichkeit bestehen oder die Datenverarbeitung unrechtmäßig ist. In welcher Qualität Anhaltspunkte dafür vorliegen müssen, ist nicht näher beschrieben.

Die Einschränkungen werden zum Teil als unzulässig kritisiert[241], weil nicht erkennbar sei, aufgrund welchen Ausnahmetatbestandes des Art. 23 DSGVO sich die Einschränkungen rechtfertigen ließen, sodass keine Gesetzgebungskompetenz bestehe[242]. Zwar fehlt es an einer hinreichenden Begründung in den Gesetzesmaterialien. Für § 308 SGB V dürfte aber Art. 23 Abs. 1 lit. e DSGVO[243] zum Tragen kommen. Danach können die Rechte des Betroffenen im Interesse des Schutzes wichtiger Ziele des allgemeinen öffentlichen Interesses im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit beschränkt werden. Der sichere Betrieb der TI stellt ein solches Interesse dar, weil die Effizienzgewinne durch die Digitalisierung, insbesondere durch die sichere Vernetzung aller Akteure, für die Gesundheitsversorgung unverzichtbar seien[244]. Zu nennen seien aber auch Risiken für die Sicherheit der elektronischen Verarbeitungssysteme[245]. Es geht aber nicht um die Sicherheit des Systems um seiner selbst willen. Der Fall der Aufrechterhaltung der Sicherheitsvorkehrungen, der gerade dem Schutz der Rechte des Betroffenen dient, dürfte der maßgebliche Grund für die Beschränkung sein. Stellt der Versicherte hingegen seine Informationen zusätzlich zur Verfügung und könnten damit die Betroffenenrechte realisiert werden, ohne dass Sicherheitsvorkehrungen tangiert werden, sollte der Verantwortliche sich unter Berufung auf § 308 Abs. 1 SGB V nicht weigern, zusätzliche Informationen entgegenzunehmen, um die Betroffenenrechte zu gewährleisten[246]. Sofern diese Variante technisch in Frage kommt, berücksichtigt § 308 SGB V diese Ausnahme nicht.

Generell ist zu beachten, dass die Rechte des Betroffenen durch § 308 SGB V nicht vollständig ausgeschlossen sind, sondern nur für den Fall der sicherheitstechnischen „Unmöglichkeit" beschränkt werden. Eine pauschale Verweigerung von Betroffenenrechten unter Berufung auf § 308 SGB V ist unzulässig. Daher erschließt es sich auch nicht, warum z. B. auch Art. 21 oder Art. 22 DSGVO beschränkt werden sollen und für welche Anwendungsfälle. Ebenso wenig dürfte eine technische Unmöglichkeit der Erfüllung von Informationspflichten gem. Art. 13, 14 DSGVO entgegenstehen.

---

235) BT-Dr. 19/18793, S. 105.
236) Für eine Einheitlichkeit der Informationen sollen § 314 S. 2, § 343 Abs. 2, § 358 Abs. 7 SGB V sorgen, vgl. BT-Dr. 19/20708, S. 117, 126, 183.
237) Davon unabhängig sieht § 305 Abs. 1 S. 6 und 7 SGB V nun einen partiellen Berichtigungsanspruch für Diagnosedaten vor.
238) Vgl. auch BT-Dr. 19/18793, S. 102. Art. 11 Abs. 1 DSGVO benennt den Fall, wenn der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren kann (ErwG 57, S. 1).
239) *Weichert*, in: *Kühling/Buchner*, DS-GVO BDSG, 3. Aufl. 2020, Art. 11, Rdnrn. 1, 8.
240) Zur Krit. z. B. an § 34 BDSG s. *Golla*, in: *Kühling/Buchner*, DS-GVO BDSG, 3. Aufl. 2020, § 34, Rdnrn. 9, 11.
241) Krit. zum RefE des LfDI BaWü, Pressemitteilung v. 27. 2. 2020.
242) BR, BT-Dr. 19/19365, S. 8.
243) S. aber BReg., BT-Dr. 19/19365, S. 26.
244) BT-Dr. 19/18793, S. 101 f.
245) BT-Dr. 19/18793, S. 102.
246) Vgl. ErwG 57, S. 2.

9. Datenverarbeitungsbefugnisse der Anbieter von Diensten und Netzen

Für Zugangsdienstanbieter und Netzanbieter enthalten § 307 Abs. 2 S. 2 und Abs. 3 S. 3 SGB V neue Befugnisgrundlagen zur Datenverarbeitung[247]. Zugleich werden damit Zweckbeschränkungen geregelt. Daher dürfen Anbieter die personenbezogenen Daten nur für den Aufbau und Betrieb des Zugangsdienstes oder zum Zweck der Datenübertragung verarbeiten. Wegen des besonderen Schutzbedarfs der transportierten Inhaltsdaten wird jeweils die entsprechende Geltung des Fernmeldegeheimnisses gem. § 88 TKG angeordnet[248].

10. IT- und Datensicherheit

In der TI werden Gesundheitsdaten der Versicherten verarbeitetet. § 306 Abs. 3 DSGVO betont, dass wegen des „besonderen Schutzbedarfs" dieser Daten ein „hohes Schutzniveau" gilt, was durch entsprechende technische und organisatorische Maßnahmen gem. Art. 32 DSGVO sicherzustellen ist. Wegen der technikneutralen Gesetzgebung werden im Einzelnen keine Maßnahmen vorgegeben[249]. Vielmehr werden in der Gesetzesbegründung allgemein die Schutzziele der Datensicherheit aufgelistet, z. B. Datenminimierung, Nichtverkettbarkeit oder Vertraulichkeit[250]. Weitere Aspekte der IT-Sicherheit werden in §§ 329 ff. SGB V geregelt, wobei aufgrund der Kritikalität der TI eine Anlehnung an § 8a Abs. 1 u. 3 BSIG erfolgt[251]. Flankierend wird in § 395 Abs. 2a SGB V u. a. ein Verbot des In-Verkehr-Bringens und des Zur-Verfügung-Stellens von Komponenten oder Diensten der TI ohne Zulassung statuiert und der Bußgeldrahmen in § 395 Abs. 3 SGB V deutlich erhöht. Damit soll der Abhängigkeit von der Sicherheit der TI und deren Diensten und Komponenten Rechnung getragen werden[252].

11. Zugriffsprotokollierung

Die *Protokollierung* bei (versuchten) Zugriffen auf Anwendungen gem. § 334 Abs. 1 und 327 SGB V zum Zwecke der Datenschutzkontrolle wird nun in modifizierter Form in § 309 SGB V geregelt[253]. Die Protokolldaten, die erst nach drei Jahren zu löschen sind[254], sollen dem Versicherten über die Benutzeroberfläche eines geeigneten Endgeräts gem. § 342 Abs. 2 Nr. 1 lit. d, Nr. 2 lit. g SGB V zur Verfügung gestellt werden[255]. Weitere Regelungen zur Zugriffsprotokollierung enthält für eVerordnungen § 361 Abs. 2 S. 2 SGB V und für Zugriffe auf andere Anwendungen § 339 Abs. 3 S. 2, Abs. 5 S. 2 SGB V. Auch hier gewährleistet die Protokollierungspflicht, dass der Versicherte seine Rechte im Rahmen der Patientensouveränität wahrnehmen und kontrollieren kann[256].

Der Beitrag wird in Heft 1/2021 fortgesetzt.

247) BT-Dr. 19/18793, S. 101.
248) § 307 Abs. 2 S. 3 und Abs. 3 S. 4 SGB V, BT-Dr. 19/18793, S. 101.
249) BT-Dr. 19/18793, S. 99.
250) S. dazu *Sohr/Kemmerich*, in: *Kipker*, Cybersecurity, Rechtshandbuch, 2020, Kap. 2, Rdnrn. 6 ff.; *Dochow*, Telematik im Gesundheitswesen, 2017, S. 789 ff. m. w. N.
251) Vgl. BT-Dr. 19/18793, S. 107.
252) Vgl. BT-Dr. 19/18793, S. 136.
253) Bisher § 291a Abs. 6 S. 3–5 SGB V a. F.
254) § 309 Abs. 1, Abs. 3 SGB V i. V. mit § 195 BGB.
255) S. a. § 312 Abs. 6 SGB V.
256) S. BT-Dr. 19/18793, S. 102, 110, 130.

Intelligente Medizinprodukte: Ist der geltende Rechtsrahmen noch aktuell?

Katrin Helle

Künstliche Intelligenz (nachfolgend auch KI) eröffnet der Medizin völlig neue Möglichkeiten. Die ersten Medizinprodukte, die sich KI bedienen, sind auf dem Markt. Neben die Chancen des Einsatzes von KI in gesamtgesellschaftlicher Hinsicht treten Rechtsfragen der Regulierung einer selbstlernenden, sich ständig entwickelnden und autonom entscheidenden Software sowie der Schadenshaftung, falls sich die Software einmal irren sollte, und angesichts des notwendigen Einsatzes von „Big Data" nicht zuletzt des Datenschutzes. Diesen Rechtsfragen widmet sich der nachfolgende Beitrag.

I. Einführung

Immer mehr Medizinprodukte nutzen KI, um seltene Krankheiten zu erkennen, Diagnosen in Sekundenschnelle zu stellen und Patienten präziser behandeln zu können. Beim Erkennen von Krankheiten ist ihre Trefferquote unter bestimmten Bedingungen sogar besser als die von Ärzten. Die wichtige Frage, ob die heute geltenden, auf statische Produkte und deterministische Software ausgerichteten Rechtsvorschriften den Besonderheiten und Risiken der KI gewachsen oder neue Regelungen erforderlich sind, beschäftigte jüngst die Europäische Kommission in ihrem Weißbuch zur KI und dem Bericht über die Auswirkungen von KI in Hinblick auf Sicherheit und Haftung[1]. Es folgte

Rechtsanwältin Dr. iur. Katrin Helle (née Rübsamen), Dierks+Company Rechtsanwaltsgesellschaft mbH, HELIX HUB, Invalidenstraße 113, 10115 Berlin, Deutschland

1) Europäische Kommission, Weißbuch, Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020)65 (nachfolgend Weißbuch); Bericht über die Auswirkungen Künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, COM(2020)64 (nachfolgend Kommissionsbericht); beide v. 19. 2. 2020. Weißbuch und Kommissionsbericht setzen den Einsatz einer hochrangigen Expertengruppe für KI (HEG-KI) fort, die eine Definition der KI entwickelte (s. Definition der Künstlichen Intelligenz: Wichtigste Fähigkeiten und Wissenschaftsgebiete v. 8. 4. 2019, nachfolgend HEG-KI Definition) und einen Bericht zur Haftung für KI verfasste (s. Liability for Artificial Intelligence and other emerging digital technologies v. 21. 11. 2019, nachfolgend HEG-KI Bericht zur Haftung).