B 1 KR 7/20 R

Land
Bundesrepublik Deutschland
Sozialgericht
Bundessozialgericht
Sachgebiet
Krankenversicherung
1. Instanz
SG Trier (RPF)
Aktenzeichen
S 3 KR 17/17
Datum
19.06.2018
2. Instanz
LSG Rheinland-Pfalz
Aktenzeichen
L 5 KR 303/18
Datum
29.08.2019
3. Instanz
Bundessozialgericht
Aktenzeichen
B 1 KR 7/20 R
Datum
20.01.2021
Kategorie
Urteil
Leitsätze

1. Die gesetzlichen Regelungen zur elektronischen Gesundheitskarte stehen in Einklang mit den Vorgaben der Datenschutz-Grundverordnung (juris: EUV 2016/679), ungeachtet der Frage, ob sie im Rahmen der gesetzlichen Krankenversicherung unmittelbar Anwendung findet, und verletzen die Versicherten weder in ihrem Grundrecht auf informationelle Selbstbestimmung noch in ihren Grundrechten nach der EU-Grundrechte-Charta (juris: EUGrdRCh).

2. Der Gesetzgeber hat mit den durch das Patientendaten-Schutz-Gesetz (PDSG) neu gefassten Regelungen des SGB V zur elektronischen Gesundheitskarte und zur Telematikinfrastruktur ausreichende Vorkehrungen zur Gewährleistung einer angemessenen Datensicherheit getroffen und ist dabei auch seiner Beobachtungs- und Nachbesserungspflicht nachgekommen.

3. Die Einhaltung der datenschutzrechtlichen Vorgaben im Zusammenhang mit der elektronischen Gesundheitskarte und der Telematikinfrastruktur ist durch die zuständigen Aufsichtsbehörden zu überwachen und können die Versicherten im Rahmen der speziellen datenschutzrechtlichen Rechtsbehelfe gerichtlich überprüfen lassen, ohne dass hierdurch die gesetzliche Obliegenheit zur Nutzung der elektronischen Gesundheitskarte und deren Verfassungsmäßigkeit tangiert werden.

Die Revision der Klägerin gegen das Urteil des Landessozialgerichts Rheinland-Pfalz vom 29. August 2019 wird zurückgewiesen.

Kosten des Revisionsverfahrens sind nicht zu erstatten.

G r ü n d e :

I

1

Die Beteiligten streiten über die Obliegenheit, die Berechtigung zur Inanspruchnahme von Leistungen mittels elektronischer Gesundheitskarte (eGK) nachzuweisen.

2

Die bei der beklagten Krankenkasse (KK) gesetzlich versicherte Klägerin lehnte es ab, ein Foto für die eGK zur Verfügung zu stellen, und beantragte die Ausstellung eines Versicherungsnachweises in papiergebundener Form. Sie widerspreche der Einführung der eGK und der Telematikinfrastruktur (TI). Die Beklagte lehnte die Ausstellung einer Ersatzbescheinigung ab *(Bescheid vom 3.7.2015, Widerspruchsbescheid vom 25.1.2017)*.

3

Die hiergegen gerichtete Klage, mit der die Klägerin insbesondere datenschutz- und datensicherheitsrechtliche Einwände geltend gemacht

hat, hat keinen Erfolg gehabt *(Urteil des SG vom 19.6.2018)*. Im Berufungsverfahren hat die Klägerin ihr Vorbringen vertieft und ua die Einholung von Auskünften der Gesellschaft für Telematik (gematik GmbH, im Folgenden: gematik) sowie die Anhörung unabhängiger IT-Experten als Sachverständige beantragt. Die gesetzlichen Regelungen zur eGK und zur TI seien wegen Verstoßes gegen das Recht auf informationelle Selbstbestimmung nicht mit dem GG vereinbar. Durch den Einsatz der Erweiterungssprache XML (Extensible Markup Language, erweiterbare Auszeichnungssprache) und das dazugehörige Regelwerk XSD (XML Schema Definition) könnten die auf der eGK unverschlüsselt und nicht löschbar gespeicherten Daten jederzeit unzulässig erweitert und damit Metadaten produziert werden. Systemadministratoren könnten mit Hilfe von Citrix und IGEL-Client die in zentralen Rechenzentren mit nur mittlerem Schutzbedarf gespeicherten Versichertendaten einsehen und sogar verändern. Mit der lebenslang selben Krankenversichertennummer würden alle ihre Daten für immer auffindbar und ihr zurechenbar, damit würde ihr "Recht auf Vergessen" verletzt. Die Übermittlung von Diagnosen, Behandlungs- und Verordnungsdaten an KKn sei nicht mit dem GG vereinbar, weil es bei den KKn eine nur unzureichende Datensicherheit gebe und die Gefahr von Profilbildungen durch die Weitergabe von personenbeziehbaren Gesundheitsdaten bestehe. Die Schutzeinstellung des Bundesamts für Sicherheit in der Informationstechnik (BSI) entspreche nicht der realen Gefährdung. Zudem seien die Zugriffsprotokollierungen unvereinbar mit den Patientenrechten aus dem europäischen Recht. Es sei europarechtswidrig keine Datenschutz-Folgenabschätzung vorgenommen worden. Beim Anschluss der Arztpraxen an die TI sei es zu diversen Datensicherheitsmängeln gekommen.

4

Das LSG hat die Berufung der Klägerin zurückgewiesen *(Urteil vom 29.8.2019)*. Die Klägerin habe auf der Grundlage der gesetzlichen Regelungen über die eGK keinen Anspruch auf Ausstellung eines anderen Versicherungsnachweises als der eGK. An der Verfassungsmäßigkeit der maßgebenden gesetzlichen Bestimmungen bestünden keine Zweifel. Der Eingriff in das informationelle Selbstbestimmungsrecht sei nach wie vor durch das überwiegende Allgemeininteresse gerechtfertigt. Die Klägerin habe ihre Zweifel an einer ausreichenden Datensicherheit zwar umfangreich begründet, letztlich handele es sich jedoch um Vermutungen und Befürchtungen, die nicht belegt seien. Risiken durch kriminelle Eingriffe könnten nicht gänzlich ausgeschlossen werden. Es seien jedoch ausreichende Vorkehrungen gegen unberechtigte Zugriffe getroffen worden. Der Gesetzgeber bleibe weiterhin verpflichtet, die Daten der Versicherten gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen und auf sich eventuell künftig zeigende Sicherheitslücken zu reagieren.

5

Mit ihrer Revision rügt die Klägerin eine Verletzung von § 103 SGG, Art 103 Abs 1 GG sowie des Rechts auf informationelle Selbstbestimmung aus Art 2 Abs 1 iVm Art 1 Abs 1 GG. Das LSG habe die von ihr gestellten Beweisanträge zu den Datensicherheitsmängeln des eGK/TI-Systems nicht unberücksichtigt lassen dürfen. Soweit es davon ausgehe, die behaupteten Mängel seien nicht hinreichend belegt, erwecke das LSG den Eindruck, ihre diesbezüglichen Ausführungen nicht zur Kenntnis genommen oder in Erwägung gezogen zu haben. Die TI sei zwischenzeitlich hinreichend verfestigt und der durch § 15 Abs 2, § 291 und § 291a Abs 2 SGB V (aF) begründete Eingriff in das Recht auf informationelle Selbstbestimmung aufgrund der unzureichenden Datensicherheit insgesamt nicht verhältnismäßig. Das im tatsächlichen Betrieb von eGK und TI vorhandene Schutzniveau habe jedenfalls zur Zeit noch nicht das für eine zumutbare Grundrechtseinschränkung erforderliche Ausmaß erreicht. Die Neuregelungen durch das Patientendaten-Schutz-Gesetz (PDSG) änderten daran nichts. Allein durch normative Akte könne die erforderliche faktische Datensicherheit nicht hergestellt werden. Die Frage der Datensicherheit der eGK und der TI betreffe generelle Tatsachen, die einer Aufklärung im Revisionsverfahren zugänglich seien.

6

Die Klägerin beantragt,

die Urteile des Landessozialgerichts Rheinland-Pfalz vom 29. August 2019 und des Sozialgerichts Trier vom 19. Juni 2018 sowie den Bescheid der Beklagten vom 3. Juli 2015 in der Gestalt des Widerspruchsbescheides vom 25. Januar 2017 aufzuheben und die Beklagte zu verpflichten, ihr den Nachweis ihrer Berechtigung zur Inanspruchnahme von Leistungen durch ein anderes für die Dauer des Versicherungsverhältnisses geltendes Nachweisdokument als die elektronische Gesundheitskarte ohne Lichtbild und ohne Chip zu ermöglichen,

hilfsweise,

das Urteil des Landessozialgerichts Rheinland-Pfalz vom 29. August 2019 aufzuheben und die Sache zur erneuten Verhandlung und Entscheidung an dieses zurückzuverweisen.

7

Die Beklagte beantragt,
die Revision zurückzuweisen.

8

Sie hält die angefochtene Entscheidung für zutreffend.

II

9

Die Revision der Klägerin ist unbegründet *(§ 170 Abs 1 Satz 1 SGG)*. Das Urteil des LSG erweist sich im Ergebnis als richtig.

10

A. Die von der Klägerin erhobene Klage ist als Anfechtungs- und Verpflichtungsklage zulässig.

11

Die Klägerin begehrt neben der Aufhebung des angefochtenen Bescheides *(vom 3.7.2015 in der Gestalt des Widerspruchsbescheides vom 25.1.2017)* die Verpflichtung der beklagten KK, ihr einen Weg zu eröffnen, ihre Berechtigung zur Inanspruchnahme von vertragsärztlichen Leistungen nachweisen zu können, die dann auch von den Leistungserbringern gegenüber der Beklagten abgerechnet werden können, ohne dabei die eGK verwenden und einen online erfolgenden Abgleich von Versichertenstammdaten dulden zu müssen. Streitgegenstand ist daher die Geltendmachung eines Anspruchs auf Befreiung von der nicht fakultativen Nutzung der eGK und den damit verbundenen Obliegenheiten der Versicherten, auch soweit sie die Anbindung an eine TI betreffen. Ihr Ziel verfolgt die Klägerin in zulässiger Weise mit der Anfechtungs- und Verpflichtungsklage *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 7, 12 f)*.

12

Streitgegenstand ist demgegenüber nicht die Installation einer TI in einem ganz allgemeinen Sinne. Streitgegenständlich sind auch nicht die zu den Pflichtanwendungen im Rahmen der TI gehörende elektronische Arbeitsunfähigkeitsbescheinigung *(§ 295 Abs 1 Satz 1 Nr 1, Satz 10 SGB V in der seit dem 1.1.2021 geltenden Fassung von Art 2 Nr 3 des Terminservice- und Versorgungsgesetzes - TSVG vom 6.5.2019, BGBl I 646)* und ab dem 1.1.2022 die Übermittlung vertragsärztlicher Verordnungen in elektronischer Form *(§ 360 Abs 1 bis 3 SGB V)*. Diese Anwendungen der TI erfolgen ohne den Einsatz der eGK und unabhängig hiervon *(vgl § 334 Abs 2 SGB V, wonach nur die Anwendungen nach Abs 1 Satz 2 Nr 1 bis 5 von der eGK unterstützt werden, während die elektronischen Verordnungen in Nr 6 aufgeführt sind; vgl auch BT-Drucks 19/14867 S 94 zu Nrn 33 und 34; Weyd, MedR 2020, 183, 191; Braun, PharmR 2020, 315, 318 ff)*.

13

B. Die Klage ist unbegründet. Die Beklagte lehnte es rechtmäßig ab, die Klägerin mit einem anderen Versicherungsnachweis als der eGK auszustatten.

14

Die Klägerin trifft die Obliegenheit, die eGK in ihrer gesetzlichen Ausgestaltung bei Inanspruchnahme vertragsärztlicher Leistungen vor Beginn der Behandlung zum Nachweis ihrer Berechtigung den vertragsärztlichen Leistungserbringern auszuhändigen und den (anderen) Leistungserbringern zur Abrechnung ihrer Leistungen zur Verfügung zu stellen *(dazu 1.)*. Die aktuellen gesetzlichen Vorgaben zur eGK und ihrer Einbeziehung in die TI stehen in Einklang mit den Vorgaben der Datenschutz-Grundverordnung *(DSGVO; Verordnung <EU> 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 119 vom 4.5.2016, S 1; berichtigt durch ABl L 314 vom 22.11.2016, S 72; berichtigt durch ABl L 127 vom 23.5.2018, S 2; dazu 2. und 3.)*. Sie verletzen die Klägerin auch nicht in ihren nach dem GG und der Europäischen Grundrechtecharta (GRCh) gewährleisteten Grundrechten *(dazu 4.)*. Auf die von der Klägerin behaupteten Datenschutzverstöße und Sicherheitsmängel kommt es dabei nicht an. Für deren Geltendmachung stehen ihr die speziellen datenschutzrechtlichen Rechtsbehelfe gemäß Art 77 ff DSGVO iVm §§ 81 ff SGB X zur Verfügung *(dazu 5.)*. Eine Vorlage an den EuGH oder das BVerfG ist nicht geboten *(dazu 6.)*.

15

1. Die Obliegenheit der Klägerin zur Nutzung der eGK ergibt sich aus § 15 Abs 2 SGB V idF des Art 1 Nr 1 Buchst b des Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze vom 21.12.2015 *(BGBl I 2408)* iVm §§ 291 bis 291b SGB V idF des Art 1 Nr 24 des Gesetzes zum Schutz elektronischer Patientendaten in der TI vom 14.10.2020 *(PDSG; BGBl I 2115)*. Die während des Revisionsverfahrens durch das PDSG bei den Vorschriften zur eGK *(§§ 291 ff SGB V)* und TI *(§§ 306 ff SGB V)* eingetretenen Rechtsänderungen sind bei kombinierten Anfechtungs- und Verpflichtungsklagen zu berücksichtigen, sofern sie - wie hier - das streitige Rechtsverhältnis erfassen *(stRspr; vgl zB BSG vom 9.2.1956 - 1 RA 5/55 - BSGE 2, 188, 192; BSG vom 2.12.2010 - B 9 SB 3/09 R - SozR 4-3250 § 69 Nr 12 RdNr 24; BSG vom 18.12.2018 - B 1 KR 31/17 R - BSGE 127, 181 = SozR 4-2500 § 284 Nr 4, RdNr 14 mwN)*.

16

a) Die für jeden Versicherten auszustellende eGK *(vgl § 291 Abs 1 SGB V)* umfasst Pflichtdaten und -anwendungen sowie freiwillige Daten und Anwendungen. Die auf der eGK gespeicherten Pflichtdaten zur Person des Versicherten werden in § 291a Abs 2 und 3 SGB V enumerativ aufgeführt. Zu den Pflichtanwendungen gehört das sogenannte Versichertenstammdatenmanagement. Dabei werden die auf der eGK gespeicherten Pflichtdaten nach § 291a Abs 2 und 3 SGB V von den an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringern unter Verwendung der TI online überprüft und bei Bedarf aktualisiert *(vgl § 291b SGB V)*.

17

Zu den für die Versicherten freiwilligen Anwendungen gehören das Notfalldatenmanagement mit der Speicherung elektronischer Notfalldaten auf der eGK *(§ 358 Abs 1, 3 und 4 SGB V)*, die Speicherung von elektronischen Erklärungen zur Organ- und Gewebespende bzw von Hinweisen auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende und von Vorsorgevollmachten oder Patientenverfügungen *(§ 334 Abs 1 Nr 2 und 3, §§ 356 f SGB V)* und der elektronische Medikationsplan *(§ 358 Abs 2 SGB V)*. Ebenfalls freiwillig ist für die Versicherten die Nutzung der elektronischen Patientenakte *(ePA; § 341 SGB V)* einschließlich der Freigabe der darin gespeicherten Daten zu Forschungszwecken *(vgl § 363 Abs 1 SGB V, sog "Datenspende")*.

18

Die Nutzung der eGK und der weiteren Anwendungen erfolgt im Rahmen der TI. Dabei handelt es sich um eine 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 *(vgl § 306 Abs 1 Satz 2 SGB V; vgl dazu auch BT-*

Drucks 19/18793 S 99; Dochow, MedR 2020, 979, 982 f). Für den Aufbau und die Verwaltung der TI ist die gematik zuständig *(§ 311 Abs 1 SGB V)*. Deren Gesellschafter sind die Bundesrepublik Deutschland (51 Prozent), der Spitzenverband Bund der KKn (24,5 Prozent) und die Spitzenorganisationen der Leistungserbringer *(vgl § 306 Abs 1 Satz 1 SGB V, zusammen 24,5 Prozent, § 310 Abs 2 SGB V)*.

19

b) § 15 Abs 2 SGB V iVm §§ 291 bis 291b SGB V erlegen der Klägerin die Obliegenheit auf, an der Herstellung der eGK mit Lichtbild *(§ 291a Abs 5 SGB V)* und den in § 291a Abs 2 und 3 SGB V geregelten obligatorischen Angaben mitzuwirken und diese zu verwenden, um ihre Berechtigung zur Inanspruchnahme vertrags(zahn)ärztlicher Versorgung nachzuweisen und damit zugleich Abrechnungen der Leistungserbringer und den online erfolgenden Abgleich von Versichertenstammdaten *(vgl § 291b Abs 1 und 2 SGB V)* zu ermöglichen*(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 17 ff)*.

20

Hierbei muss die Klägerin dulden, dass die eGK weitere Funktionen im Rahmen der TI unterstützt *(vgl § 291 Abs 2 SGB V)* und dass die darauf gespeicherten obligatorischen Daten im Rahmen des sog Versichertenstammdatenmanagements *(vgl § 291b Abs 2 SGB V)* online abgeglichen und aktualisiert werden. In diesem Zusammenhang muss die Klägerin weiter die Verarbeitung ihrer personenbezogenen Daten im Rahmen der TI einschließlich der zentralen Speicherung der auf der eGK gespeicherten Versichertenstammdaten bei der Beklagten dulden. Die Rechtsgrundlage dafür findet sich in § 284 Abs 1 Satz 1 SGB V *(idF des Art 1 Nr 22 PDSG)* iVm § 67a Abs 1 und § 67b Abs 1 SGB X *(jeweils idF des Art 24 Nr 2 Gesetz zur Änderung des Bundesversorgungsgesetzes - BVG - und anderer Vorschriften vom 17.7.2017 BGBl I 2541, mWv 25.5.2018)*. Nach § 284 Abs 1 Satz 1 SGB V dürfen die KKn im Hinblick auf Versicherte Sozialdaten für Zwecke der Krankenversicherung insbesondere erheben und speichern, soweit diese für die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft *(Nr 1)*, die Ausstellung der eGK *(Nr 2)*, die Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte einschließlich der Voraussetzungen von Leistungsbeschränkungen sowie die Bestimmung des Zuzahlungsstatus *(Nr 4)*, die Abrechnung mit den Leistungserbringern *(Nr 8)*, die Vorbereitung von Versorgungsinnovationen, die Information der Versicherten und die Unterbreitung von Angeboten nach § 68b Abs 1 und 2 SGB V *(Nr 19)* und die administrative Zurverfügungstellung der ePA sowie für das Angebot zusätzlicher Anwendungen iS des § 345 Abs 1 Satz 1 SGB V *(Nr 20)* erforderlich sind *(zur Verwendung der eGK durch nicht versicherte Personen vgl § 264 Abs 4 SGB V)*. Das für die Ausstellung der eGK erforderliche Lichtbild dürfen die KKn für die Dauer des Versicherungsverhältnisses des Versicherten, jedoch längstens für zehn Jahre, für Ersatz- und Folgeausstellungen der eGK speichern *(§ 291a Abs 6 SGB V; zur früheren Rechtslage vgl BSG vom 18.12.2018 - B 1 KR 31/17 R - BSGE 127, 181 = SozR 4-2500 § 284 Nr 4, RdNr 20 f)*.

21

Weist ein Versicherter seine Berechtigung nicht mittels eGK nach, muss er den sich daraus ergebenden Nachteil hinnehmen: Er kann sich dort keine Sachleistungen verschaffen, wo die eGK zum Nachweis der Berechtigung und zur Ermöglichung von Verschaffungsvorgängen erforderlich ist *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 17)*.

22

c) Keine Obliegenheit trifft die Klägerin demgegenüber hinsichtlich der fakultativen Daten auf der eGK und zur Nutzung der im Rahmen der TI angebotenen freiwilligen Anwendungen. Hierzu gehören die ePA *(vgl § 341 Abs 1 Satz 2 SGB V)*, die elektronischen Notfalldaten *(vgl § 358 Abs 1 Satz 2 SGB V)*, der elektronische Medikationsplan *(vgl § 358 Abs 1 Satz 2, Abs 2 Satz 2 SGB V)* sowie die Abgabe von elektronischen Erklärungen zur Organ- und Gewebespende bzw die Speicherung von Hinweisen auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende und von Vorsorgevollmachten oder Patientenverfügungen *(vgl § 334 Abs 1 Nr 2 und 3, §§ 356 f SGB V)*.

23

Die Klägerin hat hinsichtlich dieser Daten und Anwendungen nach dem Gesamtzusammenhang der Feststellungen des LSG und ihrem Vorbringen kein Einverständnis erklärt. Dafür, dass trotz Fehlens ihres Einverständnisses mit ihrer eGK fakultative Daten verarbeitet werden, ist nichts ersichtlich. Dies würde zudem nicht im Einklang mit den von ihr angegriffenen Regelungen erfolgen, sondern in rechtswidriger Weise, wogegen sich die Klägerin mit den dafür zur Verfügung stehenden Rechtsbehelfen individuell zur Wehr setzen könnte *(s dazu noch unten 5.)*. Eine Überprüfung der Vereinbarkeit der Regelungen über die freiwilligen Daten und Anwendungen mit höherrangigem Recht erübrigt sich insoweit.

24

Dasselbe gilt auch, soweit die Klägerin geltend macht, auf der eGK seien über die im Gesetz vorgesehenen Merkmale hinaus in unzulässiger Weise weitere Daten gespeichert *(vgl BSG vom 24.5.2017 - B 1 KR 79/16 B - juris RdNr 7)*. Insofern stünde ihr ggf ein Löschungsanspruch nach Art 17 Abs 1 Buchst d DSGVO zu, den sie gesondert gegenüber der Beklagten geltend machen könnte *(vgl BSG vom 18.12.2018 - B 1 KR 31/17 R - BSGE 127, 181 = SozR 4-2500 § 284 Nr 4, RdNr 11 ff)*. Die hier allein streitentscheidende Obliegenheit zur Nutzung der eGK bliebe davon unberührt *(s unten 5.)*.

25

2. Es kann dahingestellt bleiben, ob die DSGVO im vorliegenden Zusammenhang unmittelbar Anwendung findet.

26

a) Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt *(vgl Art 2 Abs 2 Buchst a DSGVO)*. Das entspricht den durch Art 16 Abs 2 Satz 1 des Vertrages

über die Arbeitsweise der Europäischen Union (AEUV) gesetzten kompetenzrechtlichen Grenzen. Danach erlassen das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr.

27

Wie weit die durch Art 16 Abs 2 Satz 1 AEUV eingeräumte europäische Regelungskompetenz reicht, ist umstritten und durch den EuGH noch nicht abschließend geklärt *(für einen weiten Anwendungsbereich der DSGVO Generalanwalt Szpunar in den Schlussanträgen vom 17.12.2020 in der Rs C-439/19, juris RdNr 47 ff; Kieck/Pohl, DuD 2017, 567; Brühann in von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl 2015, Art 16 AEUV RdNr 65 ff; Kühling/Raab in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Einführung RdNr 8; Bieresborn, NZS 2017, 887, 891; speziell für das Gesundheitswesen Weichert in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 9 DSGVO RdNr 96; Niggemeier in von der Groeben/Schwarze/Hatje, aaO, Art 168 AEUV RdNr 75; für eine restriktive Auslegung des Art 16 Abs 2 AEUV dagegen M. Schröder in Streinz, EUV/AEUV, 3. Aufl 2018, Art 16 AEUV RdNr 9 mwN; speziell für das Gesundheitswesen Dochow, GesR 2016, 401, 403; Erbguth, KrV 2019, 1, 3 f; vgl auch Wolff in Schantz/Wolff, Das neue Datenschutzrecht, 2017, RdNr 22 ff).*

28

b) Ob die DSGVO auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der eGK und der TI unmittelbar Anwendung findet oder über § 35 Abs 2 Satz 2 SGB I lediglich entsprechend, ist fraglich, weil die Festlegung der Gesundheitspolitik sowie die Organisation des Gesundheitswesens und die medizinische Versorgung Sache der Mitgliedstaaten ist *(vgl Art 168 Abs 7 Satz 1 und 2 AEUV)* und die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt *(vgl Art 2 Abs 2 Buchst a DSGVO; vgl dazu BSG vom 18.12.2018 - B 1 KR 31/17 R - BSGE 127, 181 = SozR 4-2500 § 284 Nr 4, RdNr 14 f; BSG vom 18.12.2018 - B 1 KR 40/17 R - SozR 4-7645 Art 9 Nr 1 RdNr 29)*. Dies bedarf vorliegend jedoch keiner Entscheidung. Denn die gesetzlichen Regelungen zur eGK und ihrer Einbeziehung in die TI stehen mit den Vorgaben der DSGVO auch dann in Einklang, wenn die DSGVO unmittelbar anwendbar und damit als höherrangiges Recht anzusehen sein sollte.

29

3. Die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der eGK nach Maßgabe der einschlägigen Vorschriften des SGB V ist durch die Ermächtigungen in Art 6 Abs 1 Buchst c und e iVm Abs 3 DSGVO *(dazu a)* und - soweit besondere Kategorien von Daten iS von Art 9 Abs 1 DSGVO betroffen sind - Art 9 Abs 2 Buchst h, Abs 3 DSGVO gedeckt *(dazu b)*. Die gesetzlichen Regelungen stehen auch mit den Vorgaben zur Gewährleistung von Datensicherheit *(Art 5 Abs 1 Buchst f, Art 32, 35, 25 DSGVO)* in Einklang *(dazu c)*.

30

a) Art 6 Abs 1 DSGVO erlaubt die Verarbeitung personenbezogener Daten ua dann, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt, oder wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde *(Buchst c und e)*. Die gesetzlichen Grundlagen für die Datenverarbeitungen selbst werden durch Unionsrecht oder das Recht der Mitgliedstaaten festgelegt *(Art 6 Abs 3 Satz 1 DSGVO)*. Letzteres ist hier der Fall.

31

Einschlägig für die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der eGK sind die nationalen Vorschriften der § 35 Abs 2 Satz 1 SGB I, § 67a Abs 1 und § 67b Abs 1 SGB X, § 15 Abs 2 und §§ 284, 291, 291a, 291b SGB V *(dazu aa)*. Aus ihnen ergibt sich auch der von Art 6 Abs 3 Satz 2 DSGVO geforderte Zweck der Datenverarbeitung *(dazu bb)*. Auch die weiteren Rechtmäßigkeitsanforderungen des Art 6 Abs 1 Satz 1 Buchst c und e DSGVO sind erfüllt *(dazu cc)*. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen zudem ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen *(Art 6 Abs 3 Satz 4 DSGVO)*. Diese Voraussetzungen liegen hier vor *(dazu dd)*.

32

aa) Wie sich bereits aus Art 6 Abs 3 Satz 1 DSGVO ergibt und in den Erwägungsgründen (ErwGr) klargestellt wird, stellen Art 6 Abs 1 Buchst c und e DSGVO selbst noch keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar, sondern setzen eine den Anforderungen des Abs 3 genügende Rechtsvorschrift im Unionsrecht oder im Recht des Mitgliedstaats voraus, die eine rechtliche Verarbeitungspflicht bzw die hoheitliche Verarbeitungsbefugnis auslöst *(ErwGr 45 Satz 1 und 47 Satz 5 zur DSGVO; vgl BVerwG vom 27.9.2018 - 7 C 5.17 - Buchholz 422.1 Presserecht Nr 18 = juris RdNr 26; Buchner/Petri in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 6 DSGVO RdNr 78; Schulz in Gola, DSGVO, 2. Aufl 2018, Art 6 RdNr 48; Bieresborn in Schütze, SGB X, 9. Aufl 2020, Vorbemerkungen zu §§ 67-85a RdNr 50)*. Dies entspricht dem in Art 8 Abs 2 Satz 1 und Art 52 Abs 1 Satz 1 GRCh und Art 8 Abs 2 der Europäischen Menschenrechtskonvention (EMRK) verankerten Grundsatz, dass es für jede Beschränkung des Grundrechts auf Datenschutz einer gesetzlichen Grundlage bedarf *(vgl EuGH vom 16.7.2020 - C-311/18 - NJW 2020, 2613 = juris RdNr 173 f, Schrems II; EuGH vom 9.11.2010 - C-92/09 und C-93/09 - Slg 2010, I-11063 = juris RdNr 49 f, Schecke; EuGH vom 20.5.2003 - C-465/00 - Slg 2003, I-4989, RdNr 76, Österreichischer Rundfunk; Jarass in Jarass, Charta der Grundrechte der EU, 4. Aufl 2021, Art 8 RdNr 14 mwN)*.

33

Der nationale Gesetzgeber hat solche gesetzlichen Grundlagen geschaffen. Diese finden sich für die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der eGK in den Vorschriften der § 35 Abs 2 Satz 1 SGB I, § 67a Abs 1 und § 67b Abs 1 SGB X, § 15 Abs 2 und §§ 284, 291, 291a, 291b SGB V.

34

bb) Diese Vorschriften regeln die Reichweite des Datenschutzes *(dazu <1>)* und den Zweck der Verarbeitung *(dazu <2>)*.

35

(1) SGB I, SGB X und SGB V regeln den Schutz von Sozialdaten grundsätzlich gleichrangig vorbehaltlich ausdrücklich davon abweichender spezialgesetzlicher Kollisionsregeln. § 35 Abs 2 Satz 1 SGB I *(idF des Art 119 des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 <Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU> vom 20.11.2019, BGBl I 1626, mWv 26.11.2019)* bestimmt: Die Vorschriften des Zweiten Kapitels des Zehnten Buches und der übrigen Bücher des Sozialgesetzbuches regeln die Verarbeitung von Sozialdaten abschließend, soweit nicht die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) in der jeweils geltenden Fassung unmittelbar gilt. Ein Rückgriff auf das Bundesdatenschutzgesetz (BDSG) ist nur zulässig, wenn das SGB oder die DSGVO dies vorsehen *(BSG vom 8.10.2019 - B 1 A 3/19 R - BSGE 129, 156 = SozR 4-2500 § 11 Nr 6, RdNr 32 mwN)*. Die datenschutzrechtlichen Regelungen der § 67a Abs 1 Satz 1 und 2, § 67b Abs 1 Satz 1 und 2 SGB X jeweils iVm Art 9 Abs 1 DSGVO verweisen ua auf die bereichsspezifischen Datenschutzregelungen des SGB V. Danach ist das Erheben von Sozialdaten durch in § 35 SGB I genannte Stellen zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem SGB erforderlich ist *(§ 67a Abs 1 Satz 1 SGB X)*.

36

Dies gilt auch für die Erhebung der besonderen Kategorien personenbezogener Daten iS des Art 9 Abs 1 DSGVO, insbesondere also für Gesundheitsdaten *(§ 67a Abs 1 Satz 2 SGB X)*. § 67b Abs 1 Satz 1 SGB X erlaubt die Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten ua nur, soweit die datenschutzrechtlichen Vorschriften des SGB X oder eine andere Vorschrift des SGB es erlauben oder anordnen. Dies gilt auch für die besonderen Kategorien personenbezogener Daten iS des Art 9 Abs 1 DSGVO *(vgl § 67b Abs 1 Satz 2 SGB X; vgl zum Ganzen BSG vom 18.12.2018 - B 1 KR 40/17 R - SozR 4-7645 Art 9 Nr 1 RdNr 23 f; BSG vom 8.10.2019 - B 1 A 3/19 R - BSGE 129, 156 = SozR 4-2500 § 11 Nr 6, RdNr 32)*.

37

Zu den anderen Vorschriften des SGB zählen auch die hier einschlägigen datenschutzrechtlichen Regelungen des SGB V, insbesondere § 284 SGB V sowie § 15 Abs 2, §§ 291 bis 291b SGB V *(vgl oben 1.)*. Sie kategorisieren nach dem Regelungskonzept des Gesetzgebers den für die eGK erforderlichen Datenschutz nach Pflichtangaben, Pflichtanwendungen sowie einwilligungsabhängigen freiwilligen Angaben und Anwendungen und gestalten ihn ebenfalls als "Verbotsnorm mit Erlaubnisvorbehalt" aus *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 15)*. Hierbei dürfen die KKn Sozialdaten für Zwecke der Krankenversicherung ua erheben und speichern, soweit diese für die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft, die Ausstellung der eGK und für die administrative Zurverfügungstellung der ePA sowie für das Angebot zusätzlicher Anwendungen iS des § 345 Abs 1 Satz 1 SGB V erforderlich sind *(§ 284 Abs 1 Nr 1, 2, 20 SGB V; s oben 1. b)*.

38

(2) Die vorgenannten Rechtsgrundlagen zur Datenverarbeitung im Zusammenhang mit der eGK regeln und benennen selbst die Zwecke der Datenverarbeitung, wie dies § 6 Abs 3 Satz 2 DSGVO verlangt. Diese Vorschrift bestimmt, dass der Zweck in der Rechtsgrundlage festgelegt oder für die Erfüllung einer Aufgabe erforderlich sein muss, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Dies ist bei den hier einschlägigen Vorschriften der Fall.

39

§ 284 Abs 1 Satz 1 SGB V erlaubt allgemein die Erhebung und Speicherung von Sozialdaten "für Zwecke der Krankenversicherung". Spezielle Zwecke der Datenverarbeitung im Zusammenhang mit der eGK sind der Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung (Versicherungsnachweis) sowie der Abrechnung mit den Leistungserbringern *(vgl § 291a Abs 1 SGB V)*, die Prüfung der Gültigkeit und Aktualität der Angaben auf der eGK sowie ggf deren Aktualisierung *(vgl § 291b Abs 1 SGB V)* und zudem die Prüfung der Leistungspflicht der KK *(vgl § 291b Abs 2 SGB V)*.

40

cc) Die besonderen Voraussetzungen für die Verarbeitung personenbezogener Daten gemäß Art 6 Abs 1 Satz 1 DSGVO liegen vor.

41

Nach Art 6 Abs 1 Satz 1 DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn eine der unter Buchst a bis f aufgeführten Bedingungen erfüllt ist. Die Verarbeitung ist insbesondere dann rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt *(Buchst c)*, oder wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde *(Buchst e)*. Beides ist hier der Fall.

42

Die Regelungen des SGB V zur eGK statuieren in § 291 Abs 1, Abs 3 Satz 1, § 291a Abs 2, Abs 4, Abs 5 Satz 1, Abs 7 und § 291b Abs 1 Satz 1 SGB V für die KKn Verpflichtungen zur Verarbeitung der personenbezogenen Daten der Versicherten iS von Art 6 Abs 1 Buchst c DSGVO. Für die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer sind die Überprüfung der Leistungspflicht der KK unter Nutzung

der eGK und der von der KK zur Verfügung gestellten Dienste einschließlich der Online-Abgleich und ggf die Online-Aktualisierung der auf der eGK gespeicherten Daten in § 291b Abs 2 SGB V ebenfalls verpflichtend angeordnet. Die Verarbeitung der auf der eGK gespeicherten Daten, einschließlich der fakultativen Daten nach § 291a Abs 3 SGB V, erfolgt gemäß Art 6 Abs 1 Buchst e DSGVO zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt *(s dazu nachfolgend dd <1>)* und jedenfalls von Seiten der KKn auch in Ausübung öffentlicher Gewalt *(Art 6 Abs 1 Buchst e DSGVO; vgl dazu auch BVerwG vom 27.3.2019 - 6 C 2/18 - BVerwGE 165, 111, RdNr 45 f)*. Zur Ausübung öffentlicher Gewalt gehört auch die Tätigkeit von Sozialleistungsträgern *(vgl Bieresborn, NZS 2017, 926, 927)*.

43

dd) Die genannten Vorschriften genügen auch den Anforderungen des Art 6 Abs 3 Satz 4 DSGVO, denn sie verfolgen ein im öffentlichen Interesse liegendes (legitimes) Ziel *(dazu <1>)* und wahren das Verhältnismäßigkeitsgebot *(dazu <2>)*. Die Einwendungen der Klägerin hiergegen greifen nicht durch *(dazu <3>)*.

44

(1) Die eGK dient mit den in § 291a Abs 2 bis 5 SGB V genannten Angaben dem Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung (Versicherungsnachweis). Sie erschwert dadurch den Leistungsmissbrauch *(vgl dazu BVerfG vom 13.6.2007 - 1 BvR 1550/03 ua - BVerfGE 118, 168, 196 = juris RdNr 129: "bedeutsamer Gemeinwohlbelang")*. Sie dient ferner der Abrechnung mit den Leistungserbringern *(§ 291a Abs 1 Satz 1 SGB V)*. Beide Aspekte kommen der finanziellen Stabilität der gesetzlichen Krankenversicherung (GKV) zugute *(vgl BVerfG vom 13.9.2005 - 2 BvF 2/03 - BVerfGE 114, 196, 248 = SozR 4-2500 § 266 Nr 9, juris RdNr 239: "überragend wichtiges Gemeinschaftsgut")*.

45

Bei den vorgenannten Zwecken handelt es sich auch um legitime Zwecke iS des Art 6 Abs 3 Satz 4 DSGVO, wie die Regelbeispiele in Art 9 Abs 2 Buchst h DSGVO *("für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich"; s dazu noch unten b)* und Art 23 Abs 1 Buchst e DSGVO *(öffentliche Gesundheit und soziale Sicherheit)* sowie ErwGr 52 Satz 2 zur DSGVO zeigen *(vgl auch Buchner/Petri in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 6 DSGVO RdNr 88)*.

46

Im Einzelnen:

- Das Aufbringen eines Lichtbildes und die Angabe des Geschlechts *(§ 291a Abs 2 Nr 4, Abs 5 SGB V)* dienen dazu, die Zuordnung der eGK zum jeweiligen Karteninhaber zu überprüfen und dadurch Missbrauch zu verhindern *(vgl BT-Drucks 15/1525 S 143; BT-Drucks 19/18793 S 96)*.

- Der online auszuführende Versichertenstammdatendienst *(§ 291a Abs 2 Nr 1, 2, 3, 5, 6, 7, 9, 10, § 291b Abs 1 SGB V)* ermöglicht es, die Aktualität und Zuordnung der eGK zum jeweiligen Karteninhaber zu überprüfen, insbesondere ungültige sowie als verloren oder gestohlen gemeldete Karten zu identifizieren *(vgl Begründung des Ausschusses für Gesundheit BT-Drucks 17/2170 S 38)* und dadurch ebenfalls Missbrauch zu verhindern *(vgl BT-Drucks 15/1525 S 143; BT-Drucks 19/18793 S 96)*. Zugleich trägt er dazu bei, die Wirtschaftlichkeit der Leistungserbringung in der GKV zu verbessern *(§ 2 Abs 4, § 12 Abs 1, § 72 Abs 2 SGB V)*. Denn er erlaubt, administrative Daten auf den Karten zu berichtigen, wodurch der anderenfalls erforderliche Austausch der Karten in vielen Fällen entfällt *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 27)*. Überdies wird dadurch auch dem in Art 5 Abs 1 Buchst d DSGVO verankerten Grundsatz der Richtigkeit personenbezogener Daten Rechnung getragen.

- Die Speicherung des Zuzahlungsstatus auf der eGK *(§ 291a Abs 2 Nr 8 SGB V)* ist für die Realisierung der elektronischen ärztlichen Verordnung *(§ 360 SGB V)* erforderlich, um eine sichere Übernahme von Zuzahlungsbefreiungen sicherzustellen.

- Die in § 291a Abs 3 SGB V geregelten Daten, die die eGK über die in § 291a Abs 2 SGB V geregelten Pflichtdaten hinaus enthalten "kann", dienen ebenfalls zum Nachweis der Berechtigung zur Leistungsinanspruchnahme unter Berücksichtigung von Wahltarifen und besonderen Vertragsverhältnissen *(Nr 1 und Nr 2, vgl dazu den Gesetzentwurf der Fraktionen der CDU/CSU und SPD zum GKV-Wettbewerbsstärkungsgesetz <GKV-WSG>, BT-Drucks 16/3100 S 173 zu Nr 194)* bzw für die Inanspruchnahme von Leistungen in einem anderen Mitgliedstaat der EU bzw des Europäischen Wirtschaftsraums (EWR) oder der Schweiz *(Nr 5)*.

- Die Dokumentation des Ruhens des Leistungsanspruchs gemäß § 16 Abs 1 Satz 1 Nr 2 bis 4 und Abs 3a SGB V auf der eGK *(§ 291a Abs 3 Nr 3 SGB V)* dient dazu, diesen Umstand gegenüber den Leistungserbringern transparent zu machen, um eine eventuell missbräuchliche Leistungsinanspruchnahme durch die Versicherten selbst zu verhindern *(vgl Bericht des Ausschusses für Gesundheit zum Entwurf des GKV-WSG, BT-Drucks 16/4247 S 56 zu Nr 194)*.

- Die offene Ermächtigung des § 291a Abs 3 Nr 4 SGB V ermöglicht die Speicherung weiterer Daten auf der eGK, soweit die Verarbeitung dieser Daten zur Erfüllung der den KKn zugewiesenen Aufgaben erforderlich ist *(vgl dazu die Begründung zum Gesetzentwurf der Bundesregierung zum Digitale-Versorgung-Gesetz <DVG>, BT-Drucks 19/13438 S 65 zu Nr 32)*.

47

(2) Die mit der eGK verbundene Datenverarbeitung wahrt den Grundsatz der Verhältnismäßigkeit.

48

Nach Art 6 Abs 3 Satz 4 DSGVO müssen die die Datenverarbeitung legitimierenden Rechtsgrundlagen in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Die Vorschrift trägt dem in Art 52 Abs 1 Satz 2 GRCh verankerten Verhältnismäßigkeitsprinzip Rechnung *(vgl Frenzel in Paal/Pauly, DSGVO/BDSG, 3. Aufl 2021, Art 6 DSGVO RdNr 45; vgl auch ErwGr 4 Satz 2 zur DSGVO)*. Dieser Grundsatz verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist *(vgl EuGH vom 8.4.2014 - C-293/12, C-594/12 - NJW 2014, 2169 = juris RdNr 46, Digital Rights Ireland ua, mwN)*.

49

Geboten ist in dem vorliegenden Zusammenhang eine ausgewogene Gewichtung legitimer Verarbeitungsziele auf der einen und der den natürlichen Personen durch die Art 7 und 8 GRCh zuerkannten Rechte auf Achtung ihres Privatlebens und auf Schutz ihrer personenbezogenen Daten auf der anderen Seite. Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten müssen sich auf das absolut Notwendige beschränken *(vgl EuGH vom 16.12.2008 - C-73/07 - Slg 2008, I-9831 = juris RdNr 56, Satakunnan Markkinapörssi und Satamedia; EuGH vom 9.11.2010 - C-92/09, C-93/09 - Slg 2010, I-11063 = juris RdNr 77, 86, Schecke; EuGH vom 7.11.2013 - C-473/12 - juris RdNr 39; EuGH vom 8.4.2014 - C-293/12, C-594/12 - NJW 2014, 2169 = juris RdNr 52, Digital Rights Ireland ua; EuGH vom 6.10.2015 - C-362/14 - NJW 2015, 3151 = juris RdNr 92, Schrems I; EuGH vom 16.7.2020 - C-311/18 - NJW 2020, 2613 = juris RdNr 176, Schrems II)*.

50

Diesen Anforderungen werden die gesetzlichen Regelungen zur eGK gerecht. Ihnen liegt ein insgesamt ausgewogenes Konzept zugrunde, das die Verarbeitung personenbezogener Daten auf das zur Erreichung der verfolgten (legitimen) Ziele zwingend erforderliche Maß beschränkt und die Persönlichkeitsrechte der Versicherten wahrt *(vgl auch Dochow/Kreitz, ZfmE 2018, 147, 153)*.

51

Es ist nicht ersichtlich, dass es andere gleich geeignete, weniger belastende Möglichkeiten gibt, um die oben genannten legitimen Ziele zu erreichen. So war die frühere Krankenversichertenkarte ohne Lichtbild, Angabe des Geschlechts und Möglichkeit des Versichertenstammdatendienstes nur bedingt geeignet, einer missbräuchlichen Verwendung zu begegnen. Sie wies ein erhebliches Missbrauchspotential auf, das deutlich höher war als jenes der eGK, und eine flankierende Vorlage des Personalausweises stellte kein gleich geeignetes milderes Mittel zur Missbrauchsverhinderung dar *(vgl dazu näher BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 29 mwN)*. Auch für die Speicherung des Zuzahlungsstatus ist kein weniger belastender, ebenso effektiver Weg ersichtlich *(vgl BSG aaO RdNr 30)*.

52

Das Lichtbilderfordernis, die Speicherung des Geschlechts sowie der Versichertenstammdatendienst beschränken die Versicherten in ihrem Recht auf Schutz der personenbezogenen Daten *(Art 8 GRCh)* nur relativ geringfügig, zumal diese auch die alleinige Verfügungsgewalt über das auf der eGK aufgebrachte (nicht gespeicherte) Lichtbild haben. Dagegen wiegen die zu erwartenden Vorteile für die Missbrauchsabwehr und Wirtschaftlichkeit der vertragsärztlichen Versorgung schwer *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 31)*. Die mit den genannten Funktionen zu erwartende Sicherung der finanziellen Stabilität der GKV ist ein überragend wichtiges Gemeinschaftsgut *(vgl BVerfG vom 13.9.2005 - 2 BvF 2/03 - BVerfGE 114, 196, 248 = SozR 4-2500 § 266 Nr 9 RdNr 139 = juris RdNr 239; vgl auch BVerfG vom 8.6.2010 - 1 BvR 2011/07, 1 BvR 2959/07 - BVerfGE 126, 112, 143 = SozR 4-1100 Art 12 Nr 21 RdNr 99)*. Sie ist ein Gemeinwohlbelang von derart hoher Bedeutung, dass Maßnahmen, die ihr zu dienen bestimmt sind, auch dann gerechtfertigt sein können, wenn sie für die Betroffenen zu fühlbaren Einschränkungen führen *(vgl BVerfG vom 14.5.1985 - 1 BvR 449/82, 1 BvR 523/82, 1 BvR 728/82, 1 BvR 700/82 - BVerfGE 70, 1, 30 = SozR 2200 § 376d Nr 1 S 11 f = juris RdNr 88; BVerfG vom 12.6.1990 - 1 BvR 355/86 - BVerfGE 82, 209, 230 = juris RdNr 82)*.

53

Die Speicherung der von § 290 SGB V vorgegebenen Krankenversicherungsnummer ist ebenfalls erforderlich, um einen eindeutigen und auch bei einem Wechsel der KK bleibenden Bezug zu dem Versicherten sicherzustellen und im Rahmen von Abrechnungs- und Wirtschaftlichkeitsprüfungen eine Pseudonymisierung *(vgl § 87 Abs 3f, § 303c SGB V)* zu ermöglichen *(vgl BT-Drucks 15/1525 S 143)*.

54

Die Preisgabe des Zuzahlungsstatus ist für den Versicherten zwingend erforderlich, um in den Genuss der Befreiung bei der konkreten Versorgung zu gelangen *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 33)*. Die Speicherung auf der eGK ist hierbei für die Realisierung der elektronischen Verordnung *(vgl § 360 SGB V)* erforderlich, um eine sichere Übernahme des Zuzahlungsstatus *(anstelle der bislang erfolgenden händischen Übertragung durch das Praxispersonal, vgl die Praxisinformationen unter https://www.kbv.de/html/egk.php, aufgerufen am 14.1.2021)* und dessen Überprüfung und Aktualisierung im Rahmen des Versichertenstammdatenmanagements zu ermöglichen. Der Gesetzgeber des GKV-Modernisierungsgesetzes (GMG) erwartete durch das Verhindern von unberechtigten Zuzahlungsbefreiungen geschätzte Einsparungen von 150 bis 250 Mio Euro *(vgl Begründung des Gesetzentwurfs eines GMG der Fraktionen SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN, BT-Drucks 15/1525 S 143 f)*.

55

Zwar wird in der Literatur geltend gemacht, aus dem Zuzahlungsstatus könnten Schlussfolgerungen auf den Gesundheitszustand und/oder die wirtschaftlichen Verhältnisse der Versicherten gezogen werden, weshalb eine unverschlüsselte Speicherung auf der eGK nicht verhältnismäßig sei *(vgl Hornung, Die digitale Identität, 2005, S 279 f; ders in LPK-SGB V, 5. Aufl 2016, § 291 RdNr 5; Scholz in BeckOK Sozialrecht, SGB V, § 291 RdNr 5, Stand 1.9.2020; Dochow, WzS 2015, 104, 108; vgl auch LSG Berlin-Brandenburg vom 20.3.2015 - L 1 KR*

18/14 - juris RdNr 43 ff). Dem vermag der Senat nach wie vor nicht zu folgen *(vgl auch BSG aaO)*. Auch mit Blick auf den Umstand, dass Versicherte die bis zum Erreichen der individuellen Belastungsgrenze erforderliche Zuzahlungssumme an die KK vorauszahlen und so bereits zu Beginn eines Jahres eine Befreiung erhalten können *(vgl Schifferdecker in Kasseler Komm, SGB V, § 62 RdNr 51, Stand September 2020)*, erlaubt allein die Information darüber, ob jemand zuzahlungsbefreit ist oder nicht, allenfalls ganz entfernte Rückschlüsse auf den Gesundheitszustand und/oder die wirtschaftlichen Verhältnisse des Versicherten. Dass auch (der ärztlichen Schweigepflicht unterliegende) Leistungserbringer auf den Zuzahlungsstatus zugreifen können, für die dieser im konkreten Fall nicht relevant ist, beeinträchtigt das Recht der Versicherten auf Geheimhaltung ihrer persönlichen Daten daher nur geringfügig und erfordert nicht zwingend eine Verschlüsselung der Information zum Zuzahlungsstatus. Im Übrigen enthalten die gesetzlichen Regelungen zur eGK zu der Frage, ob und ggf in welchem Umfang die darauf gespeicherten Daten zu verschlüsseln sind, keine Vorgaben *(vgl Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 291 RdNr 10 ff; vgl demgegenüber - für die Daten über die Teilnahme an strukturierten Behandlungsprogrammen - § 291 Abs 2 Satz 1 Nr 7 SGB V in der bis zum 28.12.2015 geltenden Fassung)*. Die allgemeinen Regelungen der DSGVO und des BDSG gebieten insoweit nichts anderes *(vgl Art 5 Abs 1 Buchst c und f <Datenminimierung, Integrität und Vertraulichkeit>, Art 32 Abs 1 Halbsatz 2 Buchst a DSGVO <geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus durch Pseudonymisierung und Verschlüsselung personenbezogener Daten>, § 22 Abs 2 Satz 2 Nr 7 BDSG <Verschlüsselung personenbezogener Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen>)*.

56

Soweit § 291a Abs 3 SGB V die Speicherung weiterer Daten auf der eGK zulässt, räumt das Gesetz den KKn ein Ermessen ein, bei dessen Ausübung die Vorgaben der DSGVO ebenfalls zu beachten sind. Hierdurch wird sichergestellt, dass eine Speicherung dieser Daten auf der eGK nur erfolgt, soweit dies im jeweiligen Einzelfall zur Erreichung der in § 291a Abs 1 Satz 1 SGB V genannten Ziele erforderlich und auch angemessen ist. Hinsichtlich der durch § 291a Abs 3 Nr 4 SGB V ermöglichten Speicherung weiterer Angaben, "soweit die Verarbeitung dieser Daten zur Erfüllung von Aufgaben erforderlich ist, die den Krankenkassen gesetzlich zugewiesen sind", ergibt sich die Wahrung der Erforderlichkeit iS des Art 6 Abs 1 Buchst e und Abs 3 DSGVO bereits aus dem Wortlaut der Regelung *(vgl Begründung zum Gesetzentwurf der Bundesregierung zum DVG, BT-Drucks 19/13438 S 65 zu Nr 32)*.

57

Dem Interesse der Versicherten, soweit wie möglich selbst über die Preisgabe und Verarbeitung ihrer (insbesondere Gesundheits-)Daten entscheiden zu können, hat der Gesetzgeber in besonderem Maße dadurch Rechnung getragen, dass er die zentralen medizinischen Anwendungen der TI, wie die ePA, die elektronischen Notfalldaten und den elektronischen Medikationsplan, ebenso wie die Speicherung von elektronischen Erklärungen zur Organ- und Gewebespende sowie die Speicherung von Hinweisen auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende und von Vorsorgevollmachten oder Patientenverfügungen auf der eGK als freiwillige Dienste ausgestaltet hat. Über ihre Inanspruchnahme können die Versicherten frei und eigenverantwortlich entscheiden *(vgl oben 1. a und c; vgl auch Dochow/Kreitz, ZfmE 2018, 147, 160 f)*. Die Entscheidungsfreiheit der Versicherten wird hierbei durch das in § 335 SGB V geregelte Diskriminierungsverbot, welches auch dem in Art 5 Abs 1 Buchst b DSGVO und § 67b Abs 1 Satz 1 SGB X verankerten Zweckbindungsgrundsatz Rechnung trägt, zusätzlich abgesichert *(vgl Dochow, MedR 2020, 979, 990 f)*.

58

(3) Die hiergegen gerichteten Einwendungen der Klägerin greifen nicht durch.

59

(a) Sofern die Klägerin geltend macht, auf der eGK seien über die im Gesetz vorgesehenen Merkmale hinaus in unzulässiger Weise weitere Daten gespeichert, stünde ihr ggf ein Löschungsanspruch nach Art 17 Abs 1 Buchst d DSGVO zu, den sie gesondert gegenüber der Beklagten geltend machen könnte *(s oben 1. c und unten 5.)*.

60

Soweit sich ihre Ausführungen konkret auf Angaben zur Teilnahme an strukturierten Behandlungsprogrammen nach § 137f SGB V beziehen *(sog Disease-Management-Programme <DMP>-Kennzeichen, vgl dazu BSG vom 24.5.2017 - B 1 KR 79/16 B - juris RdNr 7)*, ist nicht ersichtlich, inwiefern die Klägerin davon persönlich betroffen ist. Dass sie an einem solchen strukturierten Behandlungsprogramm teilnimmt, hat das LSG nicht festgestellt und lässt sich dem Vorbringen der Klägerin nicht entnehmen. Zudem wurde mit dem DVG vom 9.12.2019 *(BGBl I 2562)* in § 291 Abs 2 Satz 1 SGB V *(jetzt § 291a Abs 3 Nr 4 SGB V)* eine Generalklausel eingefügt, die die Speicherung sog "statusergänzender Merkmale" wie der DMP-Kennzeichnung auf der eGK legitimiert *(vgl Schifferdecker in Kasseler Komm, SGB V, § 291 RdNr 35, Stand Juli 2020, mwN)*.

61

(b) Auch die Speicherung der Versichertendaten auf der eGK in einer erweiterbaren Auszeichnungssprache (XML) ist nicht zu beanstanden.

62

Die Datenspeicherung in diesem Format entspricht der Vorgabe des § 291a Abs 4 SGB V. Danach sind die Versichertendaten auf der eGK in einer Form zu speichern, die für eine maschinelle Übertragung auf die für die vertragsärztliche Versorgung vorgesehenen Abrechnungsunterlagen und Vordrucke geeignet ist. Ein gleich geeignetes milderes Mittel zur Zweckerreichung ist auch insofern nicht ersichtlich. Dass die betreffenden Daten nicht für Zwecke eines unzulässigen Profiling *(vgl zur Begriffsdefinition Art 4 Nr 4 DSGVO)* verwendet werden, wird durch die diesbezüglichen Regelungen der DSGVO und des BDSG gewährleistet *(vgl insbesondere Art 22 DSGVO;*

ferner Art 13 Abs 2 Buchst f, Art 14 Abs 2 Buchst g, Art 15 Abs 1 Buchst h, Art 21 Abs 1 Satz 1 Halbsatz 2, Art 35 Abs 3 Buchst a, Art 70 Abs 1 Buchst f DSGVO; § 37 BDSG).

63

Die Einhaltung dieser Vorgaben haben die datenschutzrechtlich Verantwortlichen durch geeignete technische und organisatorische Maßnahmen sicherzustellen *(vgl Art 24 Abs 1 DSGVO)* und die Aufsichtsbehörden mit den ihnen zustehenden Befugnissen zu überwachen *(vgl Art 57 f DSGVO)*. Verstöße sind straf- oder bußgeldbewehrt *(vgl Art 83 f DSGVO, §§ 41 ff BDSG, § 397 SGB V)*.

64

(c) Sofern sich die Klägerin gegen die Protokollierung der Zugriffsdaten und Online-Überprüfungen im Rahmen des Versichertenstammdatenmanagements *(vgl auch § 291b Abs 2 Satz 3 SGB V)* wendet, verkennt sie, dass die Zugriffsprotokollierung dem in Art 5 Abs 1 Buchst a DSGVO verankerten Transparenzgrundsatz Rechnung trägt *(vgl dazu auch ErwGr 39 zur DSGVO; für die Anwendungen im Rahmen der TI vgl § 309 SGB V)*. Hierdurch wird gewährleistet, dass die Versicherten im Bedarfsfall die Information erhalten können, wer wann welche der auf der eGK gespeicherten Daten verarbeitet hat *(vgl Art 15 Abs 1 Buchst c DSGVO)*, um ihnen die Durchsetzung ihrer Datenschutzrechte und den Aufsichtsbehörden eine effektive Datenschutzkontrolle zu ermöglichen. Die Protokolldaten dienen insofern ausschließlich den Interessen der Versicherten *(vgl auch § 309 Abs 2 SGB V)*. Sie werden auch nur auf der eGK gespeichert *(vgl die Spezifikation Fachmodul VSDM, Version 2.4.0, Stand 26.10.2018, S 42 und 50; vgl auch die Antwort der Bundesregierung auf die Kleine Anfrage Abgeordneter und der Fraktion der FDP in BT-Drucks 19/16228 S 3 zu Frage 4)*.

65

b) Die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der eGK ist auch insoweit mit der DSGVO vereinbar, als diese in Art 9 Sonderregelungen für besondere Kategorien von Daten, insbesondere Gesundheitsdaten, aufstellt.

66

Die Rechtmäßigkeit der Verarbeitung besonders geschützter Kategorien von Daten, vorliegend insbesondere von Gesundheitsdaten *(zum Begriff vgl Art 4 Nr 15 DSGVO; Weichert in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 4 Nr 15 DSGVO RdNr 1 ff, Art 9 DSGVO RdNr 1)*, nicht aber das Lichtbild auf der eGK *(vgl ErwGr 51 zur DSGVO; vgl auch BSG vom 18.12.2018 - B 1 KR 31/17 R - BSGE 127, 181 = SozR 4-2500 § 284 Nr 4, RdNr 16)*, richtet sich nach Art 9 DSGVO. Die Verarbeitung dieser besonders geschützten Daten ist nach Art 9 Abs 1 DSGVO grundsätzlich untersagt, sofern nicht eine der in Art 9 Abs 2 DSGVO normierten Ausnahmetatbestände einschlägig ist.

67

Letzteres ist vorliegend der Fall. Die Verarbeitung besonderer Kategorien von Daten im Zusammenhang mit der eGK ist durch Art 9 Abs 2 Buchst h DSGVO iVm § 67a Abs 1 Satz 2 und § 67b Abs 1 Satz 2 SGB X und §§ 291 ff SGB V legitimiert *(vgl Dochow, MedR 2020, 979, 980; Dochow/Kreitz, ZfmE 2018, 147, 152)*. Ob daneben auch die Voraussetzungen von Art 9 Abs 2 Buchst b DSGVO *(Verarbeitung zur Ausübung der aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und Nachkommen der diesbezüglichen Pflichten)* und Buchst i *(aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit)* vorliegen, kann dahinstehen.

68

aa) Nach Art 9 Abs 2 Buchst h DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten ua zulässig, wenn sie für Zwecke der Gesundheitsvorsorge, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs vorbehaltlich der in Art 9 Abs 3 DSGVO genannten Bedingungen und Garantien erforderlich ist *(vgl dazu auch BSG vom 18.12.2018 - B 1 KR 40/17 R - SozR 4-7645 Art 9 Nr 1 RdNr 30)*.

69

Die Regelungen in Art 9 Abs 2 Buchst h und Abs 3 DSGVO tragen der Bedeutung des Gesundheitsschutzes für den Einzelnen und für die Gesellschaft insgesamt Rechnung und berücksichtigen, dass im Gesundheits- und Sozialbereich in hohem Maße sensible Daten verarbeitet werden und dies für das Funktionieren der medizinischen Versorgung und des Sozialsystems auch notwendig ist *(vgl Albers/Veit in BeckOK DatenschutzR, DSGVO Art 9 RdNr 77, Stand 1.5.2020)*. Die Verarbeitung besonderer Kategorien personenbezogener Daten soll dabei nur erfolgen, soweit dies für das Erreichen dieser Zwecke erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden *(vgl ErwGr 53 zur DSGVO)*.

70

Die medizinische Versorgung und Behandlung im Gesundheits- und Sozialbereich umfasst sämtliche gesundheitsbezogenen Handlungen und Leistungen präventiver, diagnostischer, kurativer und nachsorgender Art *(vgl Schulz in Gola, DSGVO, 2. Aufl 2018, Art 9 RdNr 35)*. Zur Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich gehört der gesamte organisatorische Rahmen zur Erbringung von Gesundheitsdienstleistungen. Dies umfasst sämtliche Maßnahmen der Organisation, Planung und Abrechnung im Rahmen der GKV und damit auch die Verarbeitung von Versichertendaten unter Nutzung der eGK und der TI *(vgl Weichert in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 9 DSGVO RdNr 105, 107)*.

71

bb) Ergänzend sind für Gesundheitsdaten die im innerstaatlichen Recht zusätzlich statuierten Bedingungen und Beschränkungen zu beachten *(Art 9 Abs 4 DSGVO)*. § 67a Abs 1 Satz 2 und § 67b Abs 1 Satz 2 SGB X bestimmen, dass die jeweils in Satz 1 geregelten Verarbeitungsbefugnisse auch für besondere Kategorien personenbezogener Daten iS des Art 9 Abs 1 DSGVO gelten. Für die Übermittlung ua von Gesundheitsdaten fordert § 67b Abs 1 Satz 3 SGB X abweichend von Art 9 Abs 2 Buchst b, d bis j DSGVO eine besondere gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im SGB. Zur Gewährleistung geeigneter Garantien zum Schutz der personenbezogenen Daten ordnen § 67a Abs 1 Satz 3 und § 67b Abs 1 Satz 4 SGB X jeweils die entsprechende Geltung von § 22 Abs 2 BDSG an *(vgl dazu Beschlussempfehlung und Bericht des Ausschusses für Arbeit und Soziales zu dem Entwurf eines Gesetzes zur Änderung des BVG und anderer Vorschriften, BT-Drucks 18/12611 S 102 f; s dazu auch unten c cc)*.

72

cc) Die in § 15 Abs 2, §§ 291 bis 291b SGB V iVm § 35 Abs 2 Satz 1 SGB I und § 67a Abs 1 und § 67b Abs 1 SGB X geregelte Verarbeitung besonderer Kategorien personenbezogener Daten der Versicherten ist insbesondere für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich. Dies ist jedenfalls in dem hier in Rede stehenden Umfang hinsichtlich der für die Versicherten obligatorischen Datenverarbeitung im Zusammenhang mit der eGK der Fall. Insofern gelten die Ausführungen zu Art 6 DSGVO entsprechend *(vgl oben 3. a dd)*.

73

dd) Die einschränkenden Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art 9 Abs 3 DSGVO sind ebenfalls gewahrt.

74

Danach dürfen die besonderen Kategorien personenbezogener Daten zu den in Art 9 Abs 2 Buchst h DSGVO genannten Zwecken nur von Fachpersonal oder unter dessen Verantwortung verarbeitet werden, das nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder durch Personen, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegen.

75

Dies ist hinsichtlich der Verarbeitung der auf der eGK (und im Rahmen der TI) gespeicherten Daten, auch soweit es sich dabei um Gesundheitsdaten handelt, der Fall. Die Leistungserbringer und die bei ihnen sowie bei den und für die KKn tätigen Personen, die auf die eGK bzw die darauf gespeicherten Daten zugreifen können, unterliegen entweder der beruflichen Schweigepflicht gemäß § 203 Strafgesetzbuch und nach den einschlägigen berufsrechtlichen Regelungen oder dem Sozialgeheimnis gemäß § 35 SGB I. Dieses erstreckt sich auch auf Auftragsverarbeiter *(§ 80 SGB X, vgl Schifferdecker in Kasseler Komm, SGB I, § 35 RdNr 42 ff, Stand März 2019)* und ist als Berufsgeheimnis iS von Art 9 Abs 3 DSGVO zu werten *(vgl Weichert in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 9 DSGVO RdNr 142)*. Es bindet nach § 78 Abs 1 SGB X auch Personen und Stellen, die nicht in § 35 SGB I genannt und denen Sozialdaten übermittelt worden sind *(sog "verlängerter Sozialdatenschutz", vgl Bieresborn in Schütze, SGB X, 9. Aufl 2020, § 78 RdNr 3)*.

76

c) Die Regelungen zur eGK und zur TI stehen im Einklang mit den Vorgaben der DSGVO zur Gewährleistung einer ausreichenden Datensicherheit. Die Vorschriften des SGB V und SGB X sowie das BDSG ermöglichen in ihrer rechtlichen Ausgestaltung und ihrer tatsächlichen Handhabung im Spannungsfeld zwischen effektiver Erledigung von Verwaltungsaufgaben mittels Datenverarbeitung und effektiver Datensicherheit einen prozesshaft-dynamischen Schutz im Einklang mit den Anforderungen der DSGVO. Ob die rechtlichen Vorgaben im Rahmen der praktischen Umsetzung von den verantwortlichen Personen und Institutionen beachtet werden, ist nicht Gegenstand des vorliegenden Rechtsstreits und vom Senat daher nicht zu überprüfen *(s dazu im Einzelnen unten 5.)*.

77

aa) Nach Art 5 Abs 1 Buchst f DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit"). Dazu gehört auch, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können *(s ErwGr 39 zur DSGVO)*.

78

Eine absolute Datensicherheit kann es jedoch nicht geben. Insofern werden die zu ergreifenden Sicherheitsmaßnahmen durch den in Art 24 DSGVO zum Ausdruck kommenden Verhältnismäßigkeitsgrundsatz beschränkt *(vgl Kramer/Meints in Auernhammer, DSGVO/BDSG, 7. Aufl 2020, Art 24 DSGVO RdNr 32 ff; Heckmann/Scheurer in Heckmann, jurisPK-Internetrecht, 6. Aufl 2019, Kap 9 RdNr 414, Stand 6.1.2021; Jandt in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 32 DSGVO RdNr 8; Raschauer in Sydow, DSGVO, 2. Aufl 2018, Art 24 RdNr 30 ff; Martini in Paal/Pauly, DSGVO/BDSG, 3. Aufl 2021, Art 24 DSGVO RdNr 24; Piltz in Gola, DSGVO, 2. Aufl 2018, Art 24 RdNr 21)*.

79

Dabei verfolgt die DSGVO einen risikobasierten Ansatz. Abhängig vom spezifischen Risiko der Datenverarbeitung und dessen Eintrittswahrscheinlichkeit hat der jeweils Verantwortliche die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten *(vgl Art 24 Abs 1 DSGVO sowie ErwGr 74 ff zur DSGVO; näher dazu Lang in Taeger/Gabel, DSGVO/BDSG, 3. Aufl 2019, Art 24 DSGVO RdNr 29 ff; Piltz in Gola, DSGVO, 2. Aufl 2018, Art 24 RdNr 19 ff; Veil, ZD 2015,*

347, 348; Schröder, ZD 2019, 503). Näher konkretisiert werden diese allgemeinen Vorgaben in Art 25, 32 und 35 DSGVO *(zum Verhältnis dieser Vorschriften zu den allgemeinen Regelungen des Art 24 DSGVO vgl Hartung in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 24 RdNr 17 f)*.

80

Art 25 DSGVO enthält Regelungen zur Gewährleistung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen *(vgl dazu Baumgartner/Gausling, ZD 2017, 308)*. Art 25 Abs 1 DSGVO regelt hierbei die Verpflichtung, den Datenschutz bereits zu einem möglichst frühen Zeitpunkt bei der Auswahl, Festlegung und Einrichtung der Systeme für eine Verarbeitung zu berücksichtigen *("Privacy by Design" oder "Data Protection by Design"; vgl Hartung in Kühling/Buchner, DSGVO/BDSG, 3. Aufl 2020, Art 25 DSGVO RdNr 11 mwN)*. Art 25 Abs 2 DSGVO verpflichtet den Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist *("Privacy by Default" oder "Data Protection by Default")*.

81

Nach Art 32 Abs 1 DSGVO sind der Verantwortliche und der Auftragsverarbeiter verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Mögliche Maßnahmen sind dabei ua die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

82

Schließlich verpflichtet Art 35 Abs 1 Satz 1 DSGVO den Verantwortlichen für den Fall, dass eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen (Datenschutz-Folgenabschätzung).

83

bb) Diese Regelungen der DSGVO finden auf die Datenverarbeitung im Zusammenhang mit der eGK und der TI unmittelbar Anwendung, was in den Gesetzesmaterialien zum PDSG ausdrücklich erwähnt wird *(BT-Drucks 19/18793 S 100 zu § 307)*. Danach entbindet die Pflicht zur Verwendung bestimmter Dienste, Anwendungen, Komponenten und sonstiger Infrastrukturteile den oder die jeweiligen Verantwortlichen *(vgl Art 4 Nr 7 DSGVO; § 307 SGB V)* nicht von der Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen, soweit diese zusätzlich erforderlich sind, wie zB die Sicherung von Konnektoren gegen unbefugten Zugang, Verwendung geeigneter Verschlüsselungsstandards nach dem Stand der Technik etc.

84

Dies gilt auch für die Regelungen zu den Datenschutz-Folgenabschätzungen nach Art 35 DSGVO und der Benennung von Datenschutzbeauftragten nach Art 37 DSGVO *(s BT-Drucks aaO, allerdings mit dem Hinweis, dass die Regelungen mangels umfangreicher Verarbeitung von Gesundheitsdaten auf die allermeisten Arztpraxen nicht zutreffen würden; vgl dazu auch ErwGr 91 zur DSGVO)*. Soweit einzelne Verantwortliche im Rahmen der TI ihrer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung bislang nicht nachgekommen sein sollten, kann dies ggf Sanktionen nach sich ziehen *(vgl Art 83 Abs 4 Buchst a DSGVO)*. Es beeinträchtigt aber nicht die Rechtmäßigkeit der Datenverarbeitung *(vgl Kramer in Gierschmann ua, DSGVO, 2018, Art 35 RdNr 160 f; Nolte/Werkmeister in Gola, DSGVO, 2. Aufl 2018, Art 35 RdNr 74; Baumgartner in Ehmann/Selmayr, DSGVO, 2. Aufl 2018, Art 35 RdNr 78; zu der geplanten Datenschutz-Folgenabschätzung bezüglich der Komponenten der dezentralen TI bei den Leistungserbringern durch den Gesetzgeber vgl den Referentenentwurf des BMG für ein Gesetz zur digitalen Modernisierung von Versorgung und Pflege <Digitale Versorgung und Pflege Modernisierungs-Gesetz - DVPMG> vom 15.11.2020 S 16 Nr 20, S 48 ff, abrufbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Dowonloads/Gesetze_und_Verordnungen/GuV/D/Referentenentwurf_DVPMG.pdf, abgerufen am 19.1.2021)*.

85

cc) Die in Art 32 DSGVO geregelten Anforderungen an die Datensicherheit werden in § 22 Abs 2 BDSG, dessen entsprechende Anwendung § 67a Abs 1 Satz 3 und § 67b Abs 1 Satz 4 SGB X anordnen, für den Fall, dass besondere Kategorien von Daten verarbeitet werden, weitergehend konkretisiert *(vgl Heckmann/Scheurer in Gola/Heckmann, BDSG, 13. Aufl 2019, § 22 RdNr 50 mwN)*.

86

Darüber hinaus enthalten die Regelungen des SGB V zur eGK und TI eine Vielzahl von Vorschriften, durch die die Vorgaben der DSGVO im Einzelnen umgesetzt und konkretisiert werden. Dabei werden insbesondere die in Art 32 Abs 1 DSGVO beispielhaft aufgeführten allgemeinen Maßnahmen zur Gewährleistung einer angemessenen Datensicherheit spezifiziert.

87

Zentrale und koordinierende Aufgaben weist der Gesetzgeber hierbei der gematik zu *(vgl § 311 SGB V)*. Dass diese ihren Aufgaben ordnungsgemäß nachkommt, und nicht wie ein privater Diensteanbieter privatnützig unter den Bedingungen von Wirtschaftlichkeit und Kostendruck agiert *(vgl BVerfG vom 2.3.2010 - 1 BvR 256/08 ua - BVerfGE 125, 260, 325 = juris RdNr 222)*, wird zum einen dadurch gewährleistet, dass die Bundesrepublik Deutschland als Mehrheitsgesellschafterin einen bestimmenden Einfluss auf die Geschicke der Gesellschaft hat *(vgl § 310 Abs 2 Nr 1 und Abs 4 SGB V; vgl dazu auch Beschlussempfehlung und Bericht des Ausschusses für Gesundheit zum Entwurf des TSVG, BT-Drucks 19/8351 S 214 f)*. Zum anderen unterliegt die gematik ihrerseits der Kontrolle durch das BSI und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Im Ergebnis wird so auch eine kontinuierliche Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben durch die gematik und die Anbieter von Diensten und Anwendungen im Rahmen der TI gewährleistet *(vgl Art 32 Abs 1 Buchst d DSGVO)*. Die enge Einbindung des BSI in den gesamten Verfahrensablauf beim Ausbau und Betrieb der TI sichert zudem die durch Art 32 Abs 1 DSGVO angeordnete Berücksichtigung des Stands der Technik.

88

Insgesamt belegen die Regelungen, dass der Gesetzgeber beim Auf- und Ausbau der TI den Vorgaben der DSGVO Rechnung trägt und den Belangen des Datenschutzes und der Datensicherheit eine zentrale Bedeutung beimisst. Er ist sich bewusst, dass im Rahmen der TI besonders sensible Gesundheitsdaten verarbeitet werden, die im Interesse der Versicherten und der Leistungserbringer (als Berufsgeheimnisträger) eines besonderen Schutzes bedürfen *(vgl BT-Drucks 19/18793 S 2)*.

89

Im Einzelnen:

- § 306 Abs 3 SGB V regelt ergänzend zu Art 32 DSGVO, dass für die Verarbeitung der zu den besonderen Kategorien iS von Art 9 DSGVO gehörenden personenbezogenen Daten in der TI ein dem besonderen Schutzbedarf entsprechendes hohes Schutzniveau gilt, dem durch entsprechende technische und organisatorische Maßnahmen iS des Art 32 DSGVO Rechnung zu tragen ist. In den Gesetzesmaterialien wird hierzu ergänzend darauf hingewiesen, dass die TI durch die dem hohen Schutzniveau angemessenen und verhältnismäßigen technischen und organisatorischen Maßnahmen nach dem Stand der Technik die besonders schutzwürdigen personenbezogenen Daten gegen unbefugte Kenntnisnahme und Verwendung schützen und die Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit einhalten muss. Die hierbei in Betracht kommenden Maßnahmen werden in der Gesetzesbegründung beispielhaft aufgeführt *(ua die Kenntnisnahme und Nutzung personenbezogener Daten von unbefugten Personen zu unterbinden, den Zugriff auf Personen zu beschränken, die nach den gesetzlichen Vorgaben zugriffsberechtigt sind, und die regelmäßige Überprüfung, Bewertung und Evaluation der Gewährleistung der Sicherheit der Verarbeitung der Daten durch die Verantwortlichen nach § 307 SGB V zu gewährleisten, s BT-Drucks 19/18793 S 100 zu § 306 Abs 3)*.

- Ferner wurde mit dem PDSG das Authentifizierungsverfahren hinsichtlich der Ausgabe der eGK und der persönlichen Identifikationsnummer (PIN) neu geregelt und an den hohen Schutzbedarf der über den Zugang zur TI verfügbaren sensitiven Daten angepasst *(§ 217f Abs 4b Satz 4, § 291 Abs 6 Satz 2, § 311 Abs 1 Nr 9 und § 336 Abs 5 und 7 SGB V)*. Die eGK dient neben dem Versicherungsnachweis und der Abrechnung mit den Leistungserbringern auch dazu, den Versicherten den Zugriff auf die im Rahmen der TI gespeicherten Daten (ePA, Erklärungen zur Organ- und Gewebespende, Hinweise auf Vorsorgevollmachten und Patientenverfügungen, Medikationsplan, elektronische Notfalldaten) zu ermöglichen *(§ 336 Abs 1 SGB V)*. Nach der Einschätzung des BfDI gewährleistet die eGK hierbei das nach dem Stand der Technik höchstmögliche Sicherheitsniveau, weil nur jemand im Besitz der Karte und der dazugehörigen PIN Zugang erlangen kann *(vgl den Tätigkeitsbericht 2019 des BfDI vom 17.6.2020, BT-Drucks 19/19900 S 25 f)*. Als datenschutzrechtlich problematisch wurde allerdings das Verfahren hinsichtlich der Ausgabe der eGK nebst PIN wie auch des den Zugang für die Leistungserbringer ermöglichenden Heilberufsausweises *(vgl § 339 Abs 3 SGB V)* angesehen, soweit hier in der Vergangenheit die Übersendung offenbar zum Teil per einfacher Post an eine beliebige Lieferadresse erfolgte und dadurch die Gefahr bestand, dass Karte und PIN in die Hände von Unbefugten gelangen können *(vgl die Stellungnahme des Sachverständigen Tschirsich vom Chaos Computer Club eV gegenüber dem Ausschuss für Gesundheit des Deutschen Bundestages vom 19.5.2020, Ausschuss-Drucks 19(14)165(20), abrufbar unter https://www.bundestag.de/resource/blob/697134/8e7859c61136827b32dd2b4c000 fbd5b/19_14_0165-20-_CCC_PDSG-data.pdf, S 4 f; sowie die Ausführungen im Rahmen der mündlichen Anhörung am 27.5.2020, Protokoll-Nr 19/93 S 19 f; vgl ferner die Stellungnahme des BfDI vom 25.5.2020, abrufbar unter https://www.bfdi.bund.de/DE/Info-thek/Transparenz/Stellungnahmen/2020/StgN_Patienten-Datenschutz-Gesetz.pdf, auf-gerufen am 14.1.2021)*. Diesen Bedenken wurde im Gesetzgebungsverfahren zum PDSG durch die Regelungen in § 217f Abs 4b Satz 4, § 291 Abs 6 Satz 2, § 311 Abs 1 Nr 9 und § 336 Abs 5 SGB V hinreichend Rechnung getragen. Es wurden sichere Ausgabeverfahren verbindlich angeordnet *(vgl BT-Drucks 19/20708 S 167 f zu Nr 19 und Nr 24, S 172 zu § 336 Abs 5; zu den Anforderungen an eine sichere Identifikation vgl auch die Verordnung (EU) Nr 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vom 23.7.2014 <eIDAS-Verordnung>, ABl L 257 S 73, nebst der Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8.9.2015 an die Identifizierung und Authentisierung für elektronisch verfügbar gemachte Verwaltungsleistungen, ABl L 235 S 7, sowie die technischen Richtlinien des BSI TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen)*. Überdies kann der Spitzenverband Bund der KKn im Einvernehmen mit dem BSI abweichend von § 336 Abs 5 SGB V zusätzliche Maßnahmen festlegen, wenn dies aufgrund des Gefährdungspotentials erforderlich ist *(§ 336 Abs 7 SGB V)*. Schließlich werden die Ausgabeverfahren der in der TI genutzten Identifikations- und Authentifizierungsmittel, insbesondere der eGK und der Heilberufsausweise durch die gematik koordiniert und überwacht *(§ 311 Abs 1 Nr 9 SGB V)*.

- In § 307 SGB V hat der Gesetzgeber *(entsprechend einer Forderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder <DSK>, vgl https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/22_ZwDSK.html, aufgerufen am 14.1.2021; vgl auch den Tätigkeitsbericht 2017 und 2018 des BfDI vom 8.5.2019, BT-Drucks 19/9800 S 59; allgemein zu den Problemen der datenschutzrechtlichen Verantwortlichkeit bei arbeitsteiligem Zusammenwirken im Bereich der Telemedizin vgl Dochow, MedR 2019, 636, 639 ff)* auf der Grundlage der Ermächtigung des Art 4 Nr 7 2. Halbsatz DSGVO die datenschutzrechtliche Verantwortlichkeit für die Datenverarbeitung in der TI gesetzlich geregelt und bei der gematik eine koordinierende Stelle zum Zweck der Erteilung von Auskünften über die Zuständigkeiten innerhalb der TI eingerichtet. Hierdurch werden in den verschiedenen arbeitsteiligen Datenverarbeitungsprozessen die datenschutzrechtlichen Verantwortlichkeiten konkret und lückenlos zugewiesen. Zudem wird sichergestellt, dass den Nutzern der TI, insbesondere den Versicherten, ein einheitlicher Ansprechpartner zur Verfügung steht *(vgl BT-Drucks 19/18793 S 100 f; vgl auch die Stellungnahme des Sachverständigen Prof. Dr. Heckmann vor dem Ausschuss für Gesundheit des Deutschen Bundestages vom 27.5.2020, Protokoll-Nr 19/93 S 5 f)*.

- Die Komponenten und Dienste der TI einschließlich der Verfahren zum Zugriff auf diese Komponenten und Dienste sowie die Anbieter von Betriebsleistungen bedürfen der Zulassung durch die gematik *(§ 311 Abs 1 Nr 2, 4, 5, Abs 6 Satz 3, §§ 324 bis 326 SGB V)*, wobei der Nachweis der Sicherheit grundsätzlich durch eine Sicherheitszertifizierung nach den Vorgaben des BSI erfolgt *(§ 325 Abs 1, Abs 3 Satz 2 SGB V)*.

- Die gematik ihrerseits hat bei der Wahrnehmung ihrer Aufgaben die Interessen von Patienten zu wahren und die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie zur Barrierefreiheit sicherzustellen und Aufgaben nur insoweit wahrzunehmen, als dies zur Schaffung einer interoperablen, kompatiblen und sicheren TI erforderlich ist *(§ 311 Abs 4 SGB V)*. Festlegungen und Maßnahmen zur Schaffung der TI, die Fragen der Datensicherheit und des Datenschutzes berühren, hat sie im Einvernehmen mit dem BSI bzw dem BfDI zu treffen *(§ 311 Abs 2 Satz 1 SGB V)*.

- Mit der weiteren Neuregelung des § 330 SGB V trägt der Gesetzgeber der besonderen Bedeutung der TI als kritische Infrastruktur zur Vernetzung aller Akteure des Gesundheitswesens im Bereich der GKV Rechnung *(vgl BT-Drucks 19/18793 S 107 zu § 330)*. Die Vorschrift ordnet eine systematische und kontinuierliche Überprüfung der Sicherheit der TI an und erlegt zu diesem Zweck der gematik und den datenschutzrechtlich Verantwortlichen besondere Pflichten auf. Sie haben angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der TI zu treffen und fortlaufend zu aktualisieren und dabei den jeweiligen Stand der Technik zu berücksichtigen *(Abs 1)*. Die gematik hat mindestens alle zwei Jahre über die Erfüllung der Anforderungen an die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der TI geeignete Nachweise zu erbringen *(Abs 2 Satz 1)* und das BSI in geeigneter Weise über diese Nachweise und über erkannte Sicherheitsmängel zu informieren *(Abs 3 Satz 1)*.

- In diesem Zusammenhang hat der Gesetzgeber mit der Neufassung des § 331 SGB V auch die der gematik auferlegten Maßnahmen zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der TI gegenüber der vormaligen Regelung in § 291b Abs 7 SGB V aF verschärft. Diese hat (bislang "kann") künftig für Komponenten und Dienste der TI sowie für Komponenten und Dienste, die die TI nutzen, aber außerhalb der TI betrieben werden, im Benehmen mit dem BSI solche Maßnahmen zur Überwachung des Betriebs zu treffen, die erforderlich sind, um die Sicherheit, Verfügbarkeit und Nutzbarkeit der TI zu gewährleisten *(vgl dazu BT-Drucks 19/20708 S 171 zu § 331)*.

- Zur Überwachung der ordnungsgemäßen Aufgabenerfüllung durch die gematik ordnet § 333 Abs 1 SGB V eine Rechenschaftspflicht gegenüber dem BSI an, das der gematik auch verbindliche Anweisungen zur Beseitigung festgestellter Sicherheitsmängel erteilen kann *(Abs 2)*. Die gematik kann ihrerseits Anbietern von zugelassenen Diensten und bestätigten Anwendungen verbindliche Anweisungen zur Beseitigung der Sicherheitsmängel erteilen, die von ihr oder dem BSI festgestellt wurden *(Abs 3)*.

90

4. Die gesetzliche Obliegenheit zur Nutzung der eGK verletzt die Klägerin nicht in ihren Grundrechten. Der Senat lässt dabei offen, ob vorliegend die Grundrechte des GG oder diejenigen der GRCh Anwendung finden *(dazu a)*. Denn der in der Obliegenheit zur Nutzung der eGK und der Verarbeitung der damit im Zusammenhang stehenden personenbezogenen Daten der Klägerin liegende Grundrechtseingriff ist sowohl am Maßstab des nationalen Grundrechts auf informationelle Selbstbestimmung *(Art 2 Abs 1 iVm Art 1 Abs 1 GG; dazu b)*, als auch am Maßstab der durch die Art 7 und 8 GRCh garantierten Grundrechte auf Achtung des Privatlebens und auf Schutz der personenbezogenen Daten *(dazu c)* gerechtfertigt.

91

a) Ob bei der Anwendung von Unionsrecht durch die Mitgliedstaaten *(vgl Art 51 Abs 1 Satz 1 GRCh)* die Grundrechte des GG oder der GRCh anzuwenden sind, hängt maßgeblich davon ab, ob es sich bei den in Rede stehenden unionsrechtlichen Vorschriften um vollständig vereinheitlichtes oder um gestaltungsoffenes Unionsrecht handelt *(vgl BVerfG vom 6.11.2019 - 1 BvR 16/13 - BVerfGE 152, 152 = juris RdNr 42, Recht auf Vergessen I; BVerfG vom 6.11.2019 - 1 BvR 276/17 - BVerfGE 152, 216 = juris RdNr 77, Recht auf Vergessen II; BVerfG vom 1.12.2020 - 2 BvR 1845/18 ua - juris RdNr 34 ff; vgl dazu auch Kühling, NJW 2020, 275)*. Unionsrechtlich nicht vollständig determiniertes innerstaatliches Recht ist primär am Maßstab der Grundrechte des GG zu überprüfen *(vgl BVerfG vom 6.11.2019 - 1 BvR 16/13 - BVerfGE 152, 152 = juris RdNr 42, Recht auf Vergessen I)*. Eine Prüfung unmittelbar an den Grundrechten der GRCh ist hier lediglich dann geboten, wenn konkrete und hinreichende Anhaltspunkte gegeben sind, dass durch eine Prüfung an den Grundrechten des GG das grundrechtliche Schutzniveau des Unionsrechts ausnahmsweise nicht gewährleistet wird *(BVerfG vom 6.11.2019 - 1 BvR 16/13 - BVerfGE 152, 152 = juris RdNr 63 ff, Recht auf Vergessen I)*. Demgegenüber sind bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen grundsätzlich allein die Unionsgrundrechte maßgeblich, die insoweit gegenüber den Grundrechten des GG Anwendungsvorrang genießen *(BVerfG vom 6.11.2019 - 1 BvR 276/17 - BVerfGE 152, 216 = juris RdNr 42 ff, Recht auf Vergessen II; BVerfG vom 1.12.2020 - 2 BvR 1845/18 - juris RdNr 36)*. Ob es sich danach bei den hier in Rede stehenden Regelungen des SGB V zur eGK und zur TI um vollständig vereinheitlichtes oder um gestaltungsoffenes Unionsrecht handelt, kann im Ergebnis dahinstehen, da der Grundrechtseingriff nach beiden Maßstäben gerechtfertigt ist.

92

b) Bei einer Prüfung am Maßstab der Grundrechte des GG begründet die Obliegenheit zur Nutzung der eGK gemäß § 15 Abs 2, §§ 291 bis 291b SGB V einen Eingriff in das Grundrecht der Klägerin auf informationelle Selbstbestimmung als eine Ausprägung des allgemeinen Persönlichkeitsrechts *(Art 2 Abs 1 iVm Art 1 Abs 1 GG)*. Dieser ist aber gerechtfertigt *(dazu aa und bb)*. Die gesetzliche Konzeption gewährleistet auch die von Verfassungs wegen gebotene (faktische) Datensicherheit *(dazu cc)*. Die Klägerin wird nicht in ihren Grundrechten dadurch verletzt, dass ihr kein anderer Weg eröffnet wird, als der durch Nutzung der eGK, ihre Berechtigung zur Inanspruchnahme von vertragsärztlichen Leistungen nachzuweisen und die Abrechnung der KKn mit den Leistungserbringern zu ermöglichen *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 23 ff; zustimmend Schifferdecker in Kasseler Komm, SGB V, § 291a RdNr 14 ff, Stand Juli 2020)*.

93

aa) Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es umfasst den Schutz gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten *(vgl BVerfG vom 15.12.1983 - 1 BvR 209/83 ua - BVerfGE 65, 1, 43; BVerfG vom 17.7.1984 - 2 BvE 11/83, 2 BvE 15/83 - BVerfGE 67, 100, 143; BVerfG vom 27.5.2020 - 1 BvR 1873/13 - NJW 2020, 2699 = juris RdNr 92)*. Die Gewährleistung greift insbesondere, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können *(BVerfG vom 27.5.2020, aaO, mwN)*. Mit dem Recht auf informationelle Selbstbestimmung wäre es nicht vereinbar, wenn die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß *(BVerfG vom 15.12.1983, aaO)*. Das Recht auf informationelle Selbstbestimmung ist aber nicht uneingeschränkt und schrankenlos gewährleistet. Eingriffe in dieses Grundrecht bedürfen wie jede Grundrechtsbeschränkung einer gesetzlichen Ermächtigung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt *(vgl BVerfG vom 15.12.1983, aaO, S 44; BVerfG vom 27.5.2020, aaO, RdNr 123; BVerfG vom 10.11.2020 - 1 BvR 3214/15 - juris RdNr 84, stRspr)*. Sie müssen daher zur Erreichung des legitimen Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein. Dabei bedürfen sie einer gesetzlichen Grundlage, welche die Datenverwendung auf spezifische Zwecke hinreichend begrenzt. Alle angegriffenen Befugnisse sind zudem am Grundsatz der Normenklarheit und Bestimmtheit zu messen, der der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Verwaltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient *(vgl BVerfG vom 10.11.2020, aaO, RdNr 85, mwN, stRspr; vgl auch BSG vom 14.2.2007 - B 1 A 3/06 R - BSGE 98, 129 = SozR 4-2400 § 35a Nr 1, RdNr 20 ff)*.

94

bb) Diesen Anforderungen genügt die gesetzliche Pflicht der KKn, die eGK herzustellen und im von der Klägerin angegriffenen, zu überprüfenden Umfang zu nutzen *(vgl auch BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 224 ff)*.

95

(1) § 15 Abs 2 und §§ 284, 291, 291a, 291b SGB V iVm § 35 Abs 2 Satz 1 SGB I, § 67a Abs 1 und § 67b Abs 1 SGB X regeln die angegriffenen Beschränkungen des Rechts auf informationelle Selbstbestimmung einfachgesetzlich für die eGK *(s dazu oben 3. a bb <1>)*. Hieraus ergeben sich Voraussetzungen und Umfang der Beschränkungen klar erkennbar. Die Regelungen entsprechen dem rechtsstaatlichen Gebot der Normenklarheit. Es unterliegt keinem Zweifel, welche Angaben von wem zu welchem Zweck verarbeitet werden dürfen *(vgl zu § 15 Abs 2, § 291, § 291a Abs 2 SGB V aF BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 25)*.

96

Das gilt auch für § 291a Abs 3 Nr 4 SGB V, der die Speicherung weiterer Angaben auf der eGK erlaubt, soweit deren Verarbeitung zur Erfüllung von Aufgaben erforderlich ist, die den KKn gesetzlich zugewiesen sind. Insoweit hat der Gesetzgeber die Regelungsbefugnis unter klarer Begrenzung von Inhalt, Zweck und Ausmaß der Ermächtigung (zur bundesweiten Verwendung der eGK "als Versicherungsnachweis" und soweit die Verarbeitung der Daten zur Erfüllung der den KKn gesetzlich zugewiesenen Aufgaben erforderlich ist) in verfassungsrechtlich zulässiger Weise gemäß § 291b Abs 6 SGB V auf die Vertragspartner der gemeinsamen Selbstverwaltung auf Bundesebene gemäß § 87 Abs 1 SGB V übertragen *(vgl zur Zulässigkeit der Delegation von Rechtssetzungsbefugnissen auf die zuständigen Spitzenverbände im Rahmen der gemeinsamen Selbstverwaltung auch BVerfG vom 17.12.2002 - 1 BvL 28/95 ua - BVerfGE 106, 275, 305 = SozR 3-2500 § 35 Nr 2 S 22 f)*. Diese sind bei der Ausübung ihrer Regelungskompetenz ihrerseits den Geboten der Normenklarheit, der Bestimmtheit und der Verhältnismäßigkeit verpflichtet.

97

Die detaillierte und normenklare Ausgestaltung der bereichsspezifischen Normen der §§ 291 ff SGB V belegt, dass der Gesetzgeber im Falle der eGK und der TI dem Sozialdatenschutz einschließlich der Datensicherheit in ganz besonderem Maße hohe Bedeutung beimisst *(vgl BT-Drucks 19/18793 S 2; vgl zur Rechtslage vor dem PDSG BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 25 mwN)*.

98

(2) Die von der Klägerin angegriffenen Beschränkungen des Rechts auf informationelle Selbstbestimmung durch die Regelungen über die eGK sind durch überwiegende Allgemeininteressen gerechtfertigt. Denn sie sind zur Verhinderung von Missbrauch und zur Kosteneinsparung zwecks Erhalt der finanziellen Stabilität der GKV geeignet, erforderlich und angemessen. Insofern wird auf die Ausführungen zu Art 6 Abs 3 Satz 4 DSGVO verwiesen *(s oben 3. a dd)*.

99

(3) Durch die speziellen datenschutzrechtlichen Rechtsbehelfe nach Art 77 ff DSGVO iVm §§ 81 ff SGB X *(idF des Art 24 Nr 2 Gesetz zur Änderung des BVG und anderer Vorschriften vom 17.7.2017, BGBl I 2541, mWv 25.5.2018)* ist auch eine effektive Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben durch die Gerichte gewährleistet.

100

Ob die datenschutzrechtlichen Vorgaben der DSGVO und des SGB V durch die dafür nach Art 4 Nr 7 DSGVO iVm § 307 SGB V Verantwortlichen im Einzelnen eingehalten werden, ist durch die zuständigen Aufsichtsbehörden im Rahmen ihrer Aufgaben und Befugnisse nach Art 57 f DSGVO zu überwachen. Nach Art 77 Abs 1 DSGVO hat jede betroffene Person das Recht, sich bei der zuständigen Aufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Dementsprechend regelt § 81 Abs 1 SGB X, dass sich eine betroffene Person, die der Ansicht ist, bei der Verarbeitung ihrer Sozialdaten in ihren Rechten verletzt worden zu sein, entweder an den Bundesbeauftragten oder die Bundesbeauftragte *(Nr 1)* oder an die nach Landesrecht für die Kontrolle des Datenschutzes zuständige Stelle *(Nr 2)* wenden kann. Gegen die daraufhin ergehende Entscheidung, wie auch gegen die Untätigkeit der genannten Stellen kann die betroffene Person nach Art 78 DSGVO iVm § 81a SGB X bzw § 20 BDSG gerichtlichen Rechtsschutz in Anspruch nehmen. Darüber hinaus besteht für die betroffene Person nach Art 79 DSGVO iVm § 81b SGB X auch das Recht, unmittelbar gegen den oder die datenschutzrechtlich Verantwortlichen und/oder Auftragsverarbeiter gerichtlich vorzugehen, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden *(vgl dazu im Einzelnen Bieresborn/Giesberts-Kaminski, SGb 2018, 609; Leopold, ZESAR 2018, 326)*.

101

cc) Untrennbarer Bestandteil der gesetzlichen Anordnung zur Offenbarung und Verarbeitung personenbezogener Daten ist neben einer normenklaren Begrenzung der Datenverwendung auch die verfassungsrechtlich gebotene Gewährleistung der Datensicherheit *(vgl BVerfG vom 2.3.2010 - 1 BvR 256/08 ua - BVerfGE 125, 260, 344 f; BVerfG vom 27.5.2020 - 1 BvR 1873/13 - NJW 2020, 2699 = juris RdNr 135, 188)*. Der Gesetzgeber hat ausreichende Vorkehrungen zur Gewährleistung der Datensicherheit im Zusammenhang mit der eGK und der TI getroffen und ist insoweit auch seiner Beobachtungs- und Nachbesserungspflicht ausreichend nachgekommen.

102

Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind *(vgl BVerfG vom 2.3.2010 - 1 BvR 256/08 ua - BVerfGE 125, 260, 326)*, sondern belässt dem Gesetzgeber insofern einen Einschätzungs-, Wertungs- und Gestaltungsspielraum, der auch Raum lässt, etwa konkurrierende öffentliche und private Interessen zu berücksichtigen *(vgl BVerfG vom 29.10.1987 - 2 BvR 624/83 ua - BVerfGE 77, 170, 215 f; BVerfG vom 2.7.2018 - 1 BvR 612/12 - juris RdNr 41 mwN)*. Insofern liegt auch der Rspr des BVerfG zugrunde, dass es keine absolute Datensicherheit gibt und dass allein dieser Umstand die automatisierte Verarbeitung personenbezogener Daten nicht verbietet. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der insbesondere der Sensibilität der betroffenen Daten und dem jeweiligen Gefährdungsrisiko hinreichend Rechnung trägt. Dabei ist sicherzustellen, dass sich dieser Standard - etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik *(vgl hierzu allgemein Ekrot/Fischer/Müller in Kipker, Cybersecurity, 1. Aufl 2020, Kap 3)* - an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Hierbei erfolgt auch nach der Rspr des BVerfG eine Überprüfung vor allem am Maßstab des vorhandenen Normengeflechts zur Gewährleistung von Datensicherheit.

103

Erforderlich sind gesetzliche Regelungen, die einen ausreichend hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Verfassungsrechtlich geboten sein können weiterhin eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung unabhängiger Datenschutzbeauftragter sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst *(vgl BVerfG vom 2.3.2010 aaO S 326 f)*. Darüber hinaus trifft den Gesetzgeber eine Beobachtungs- und ggf Nachbesserungspflicht *(vgl dazu allgemein BVerfG vom 28.5.1993 - 2 BvF 2/90 ua - BVerfGE 88, 203, 309 ff; BVerfG vom 24.1.2012 - 1 BvR 1299/05 - BVerfGE 130, 151 RdNr 161; BVerfG vom 2.7.2018 - 1 BvR 612/12 - juris RdNr 42, mwN; Isensee in Isensee/Kirchhof, Handbuch des Staatsrechts, Bd IX, 3. Aufl 2011, § 191 RdNr 285 ff)*, um zB auf sich künftig zeigende Sicherheitslücken zu reagieren *(vgl BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 34; Kühling/Seidel in Kingreen/Kühling, Gesundheitsdatenschutzrecht, S 181)*.

104

Die gesetzlichen Regelungen des SGB V zur eGK und zur TI werden diesen verfassungsrechtlichen Anforderungen gerecht *(vgl auch BSG vom 18.11.2014 - B 1 KR 35/13 R - BSGE 117, 224 = SozR 4-2500 § 291a Nr 1, RdNr 34; Kühling/Seidel in Kingreen/Kühling, Gesundheitsdatenschutzrecht, S 181)*. Die mit dem PDSG neu gefassten und inhaltlich überarbeiteten Neuregelungen der §§ 291 ff SGB V enthalten ein hinreichend normdichtes und klares Regelungsgefüge, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler Maßnahmen der Datensicherheit dient *(s dazu im Einzelnen oben 3. c)*, der der Gesetzgeber beim Auf- und Ausbau der TI eine "herausragende Rolle" beimisst *(s oben bb <1>)*.

105

Dabei ist der Gesetzgeber auch seiner Beobachtungs- und Nachbesserungspflicht nachgekommen, indem er etwa auf die in der Praxis zu Tage getretenen datenschutzrechtlichen Defizite und Sicherheitslücken, auf die zum Teil auch die Klägerin hingewiesen hat, reagiert und entsprechende Gegenmaßnahmen ergriffen hat. So hat er auf die zuvor bestehenden Unklarheiten hinsichtlich der Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten im Rahmen der TI durch die gesetzliche Normierung dieser Verantwortlichkeiten und die Einrichtung einer koordinierenden Stelle bei der gematik reagiert *(§ 307 SGB V; s dazu oben 3. c cc)*. Den ua vom Chaos Computer Club eV aufgedeckten Mängeln des Authentifizierungsverfahrens hinsichtlich der Ausgabe der eGKn und der Heilberufsausweise hat der Gesetzgeber

durch die Neuregelungen in § 217f Abs 4b Satz 4, § 291 Abs 6 Satz 2, § 311 Abs 1 Nr 9 und § 336 Abs 5 und 7 SGB V Rechnung getragen *(s oben 3. c cc)*. Soweit die Klägerin auf Schwachstellen in den IT-Systemen einzelner Arztpraxen hinweist, hat der Gesetzgeber darauf mit der bereits durch das DVG eingefügten und mit dem PDSG nochmals nachgebesserten Neuregelung des § 75b SGB V reagiert. Danach ist die Kassenärztliche Bundesvereinigung verpflichtet, in einer für die Leistungserbringer verbindlichen Richtlinie die - mit dem BSI abzustimmenden - Anforderungen zur Gewährleistung von IT-Sicherheit in der vertragsärztlichen Versorgung festzulegen und jährlich anzupassen *(vgl die Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit vom 16.12.2020, abrufbar unter https://www.kbv.de/media/sp/02_15_KBV-Vo_Richtlinien_Anlage_1.pdf, aufgerufen am 14.1.2021)*. Damit wird gewährleistet, dass das hohe Sicherheitsniveau der TI auch der Maßstab für die Datensicherheit in den Vertragsarztpraxen ist *(vgl Beyer, SDSRV 2020, 69, 81)*. Der Verbesserung der IT-Sicherheit in Krankenhäusern dient die mit dem PDSG eingefügte Neuregelung des § 75c SGB V *(vgl dazu BT-Drucks 19/20708 S 167)*.

106

Schließlich wurde dem mit der Einführung von medizinischen Anwendungen gewachsenen Sicherheitsbedürfnis auch durch die Schaffung weiterer Bußgeldtatbestände und der deutlichen Erhöhung des Bußgeldrahmens Rechnung getragen *(§ 397 SGB V, s dazu BT-Drucks 19/18793 S 83, 136)*.

107

c) Bei einer Überprüfung am Maßstab der Unionsgrundrechte ist der in der Obliegenheit der Klägerin zur Nutzung der eGK liegende Grundrechtseingriff ebenfalls gerechtfertigt.

108

aa) Nach Art 7 GRCh hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Nach Art 8 Abs 1 GRCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten *(zum Verhältnis der Grundrechte aus Art 7 und Art 8 GRCh vgl Reinhardt, AöR 142 <2017>, 528, 538 ff)*. Nach Art 8 Abs 2 Satz 1 GRCh dürfen diese Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden *(s dazu bereits oben 3. a aa)*. Nach Satz 2 hat jede Person das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Art 8 Abs 3 GRCh verlangt, dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht wird.

109

Eine Unionsregelung, die einen Eingriff in die durch die Art 7 und 8 GRCh garantierten Grundrechte auf Achtung des Privatlebens und auf Schutz der personenbezogenen Daten enthält, muss nach der Rspr des EuGH dem Erfordernis der Verhältnismäßigkeit genügen. Die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten müssen sich auf das absolut Notwendige beschränken *(s die Nachweise oben unter 3. a dd <2>)*. Die den Eingriff enthaltende Regelung muss zudem klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht *(vgl EuGH vom 8.4.2014 - C-293/12 , C-594/12 - NJW 2014, 2169 = juris RdNr 54 f, Digital Rights Ireland ua; EuGH vom 6.10.2015 - C-362/14 - NJW 2015, 3151 = juris RdNr 91, Schrems I; EuGH vom 16.7.2020 - C-311/18 - NJW 2020, 2613 = juris RdNr 176, Schrems II)*.

110

bb) Auch diesen Anforderungen, die sich mit denen des GG im Wesentlichen decken, werden die entscheidungserheblichen Regelungen zur eGK gerecht *(s oben b)*.

111

5. Soweit die Klägerin im Einzelnen faktische Lücken und Mängel außerhalb der datenschutzrechtlichen Verantwortlichkeit der Beklagten in Bezug auf die TI als Ganzes oder in Teilbereichen geltend macht, ist dies nicht Streitgegenstand des Rechtsstreits. Insoweit ist die Klägerin auf die speziellen datenschutzrechtlichen Rechtsbehelfe nach Art 77 ff DSGVO iVm §§ 81 ff SGB X zu verweisen. Durch sie ist eine effektive Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben durch die Gerichte im Hinblick auf die einzelnen Verantwortlichen spezifisch gewährleistet *(s dazu oben 4. b bb <3>)*. Ob die datenschutzrechtlichen Vorgaben der DSGVO und des SGB V durch die dafür Verantwortlichen im Einzelnen eingehalten werden, ist durch die zuständigen Aufsichtsbehörden im Rahmen der ihnen durch Art 57 f DSGVO zugewiesenen Aufgaben und Befugnisse zu überwachen und kann von den Versicherten sowohl im Verhältnis zu den Aufsichtsbehörden, als auch unmittelbar im Verhältnis zu den Verantwortlichen selbst einer gerichtlichen Überprüfung zugeführt werden.

112

Aus der von der Klägerin angeführten Entscheidung des BVerfG vom 13.2.2006 *(1 BvR 1184/04 - juris)* ergibt sich insofern nichts anderes. In dieser Entscheidung wurde eine gegen die damaligen gesetzlichen Regelungen zur eGK gerichtete Rechtssatz-Verfassungsbeschwerde nicht zur Entscheidung angenommen und in der Begründung ua darauf hingewiesen, dass zur Prüfung der datenschutzrechtlichen Zulässigkeit der angegriffenen Normen konkret zu beurteilen sei, wie die jeweiligen Stellen mit den fraglichen Daten nach ihrer Speicherung oder Übermittlung umgehen und welche datenschutzrechtlichen Vorkehrungen insoweit bestehen. Dies bedürfe umfangreicher Ermittlungen, Einschätzungen und Wertungen. Hierzu seien in erster Linie die Fachgerichte wegen ihrer besonderen Sachnähe, ihrer umfassenden Erfahrung und den ihnen zur Verfügung stehenden Möglichkeiten zur Erhebung von Beweisen berufen.

113

Ungeachtet des Umstandes, dass diese Entscheidung vor dem Inkrafttreten der DSGVO und den darauf beruhenden nationalen datenschutzrechtlichen Neuregelungen mit den speziellen datenschutzrechtlichen Rechtsbehelfen ergangen ist, kann hieraus nicht abgeleitet werden, dass die Verfassungsmäßigkeit der in Rede stehenden gesetzlichen Regelungen davon abhängig ist, dass die gesetzlichen Vorgaben zum Datenschutz und zur Datensicherheit in der Praxis durchgehend beachtet werden. Entscheidend für die Vereinbarkeit der gesetzlichen Obliegenheit zur Nutzung der eGK mit den Grundrechten sowohl des GG als auch der GRCh ist nach der dargestellten Rspr des BVerfG und des EuGH vielmehr, dass der Gesetzgeber ausreichende Vorkehrungen zur Gewährleistung eines dem Schutzniveau der (potenziell) betroffenen Daten und der Gefährdungslage angemessen Rechnung tragenden Maßes an Datensicherheit getroffen hat und dabei auch seiner Beobachtungs- und Nachbesserungspflicht nachgekommen ist. Dafür, dass trotz der vielfältigen institutionellen Sicherungsmechanismen ein angemessenes Maß an Datenschutz und Datensicherheit nicht gewährleistet ist, etwa weil zuständige Aufsichtsbehörden konkreten Hinweisen auf Datenschutzverstöße systematisch nicht nachgehen und diese über längere Zeiträume hinweg nicht abgestellt werden, ist nichts ersichtlich.

114

Dass die Beklagte selbst als datenschutzrechtlich Verantwortliche die datenschutzrechtlichen Vorgaben im Zusammenhang mit der eGK verlassen hat, ist ebenfalls weder vorgetragen noch sonst ersichtlich. Die Klägerin hat entsprechende Beweisanträge auch nicht gestellt.

115

6. Eine Vorlage an den EuGH nach Art 267 Abs 3 AEUV ist nicht geboten. Die Anwendung der DSGVO und der Unionsgrundrechte auf den vorliegenden Fall wirft keine Auslegungsfragen auf, die nicht schon aus sich heraus klar oder durch die Rspr des EuGH hinreichend geklärt sind.

116

Die Voraussetzungen einer konkreten Normenkontrolle nach Art 100 Abs 1 GG liegen ebenfalls nicht vor. Der Senat konnte sich aus den aufgezeigten Gründen nicht von der Verfassungswidrigkeit der von der Klägerin angegriffenen gesetzlichen Vorschriften überzeugen.

117

7. Da sich die Entscheidung des LSG im Ergebnis als richtig darstellt, kommt es auf die von der Klägerin gerügten Verfahrensfehler nicht an *(§ 170 Abs 1 Satz 2 SGG)*. Der Senat muss daher weder entscheiden, ob das LSG ausgehend von seiner Rechtsauffassung den Beweisanträgen der Klägerin zu den von ihr geltend gemachten Datensicherheitsmängeln des eGK/TI-Systems hätte nachgehen müssen, noch, ob es den Anspruch der Klägerin auf Verletzung ihres rechtlichen Gehörs verletzt hat, indem es Ausführungen nicht zur Kenntnis genommen oder in Erwägung gezogen hat *(vgl BSG vom 12.12.2008 - GS 1/08 - BSGE 102, 166 = SozR 4-1500 § 41 Nr 1, RdNr 36 f; Röhl in jurisPK-SGG, 1. Aufl 2017, § 170 RdNr 23)*.

118

8. Die Kostenentscheidung beruht auf § 193 SGG.

Rechtskraft
Aus
Saved
2021-12-15