# S 38 KA 190/20

## Sozialgerichtsbarkeit Bundesrepublik Deutschland

| | |
|---|---|
| Land | Freistaat Bayern |
| Sozialgericht | Sozialgericht München |
| Sachgebiet | Vertragsarztangelegenheiten |
| Abteilung | - |
| Kategorie | Urteil |
| Bemerkung | - |
| Rechtskraft | - |
| Deskriptoren | - |
| Leitsätze | 1. Die in den Quartalen des Jahres 2019 vorgenommene Honorarkürzung (Honorarabzug wegen Nichtteilnahme an der Telematikinfrastruktur), die ihre rechtliche Grundlage in § 291 Abs. 2b S. 14 SGB V a.F. findet, ist rechtmäßig. Die Regelungen über die Telematikinfrastruktur (§§ 291ff. SGB V) sind mit höherrangigem Recht, der Datenschutzgrundverordnung (DSGVO) und dem Grundgesetz zu vereinbaren (vgl BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R; SG Stuttgart, Urteil vom 27.01.2022, Az S 24 KA 166/20; SG Mainz, Urteil vom 27.07.2022, Az S 3 KA 84/20; SG München, Urteile vom 09.11.2022, u.a. Az S 38 KA 5155/21; SG München, Urteil vom 26.01.2023, Az S 38 KA 72/22).<br><br>2. In den Quartalen des Jahres 2019 findet kein Abgleich aller Patientenstammdaten im eigentlichen Sinne statt. Vielmehr wird nur verschlüsselt bei den Krankenkassen angefragt, ob es ein Update gibt. Es handelt sich um eine Datenverarbeitung auf sehr niedrigem Niveau, weshalb lediglich geringere Anforderungen an den Datenschutz zu stellen sind.<br><br>3. Die Gematik als Institution wird den Anforderungen an eine angemessene Datensicherheit formell und materiell gerecht. Sowohl die Beteiligung des Spitzenverbandes der Apotheker, als auch |

eine eventuelle Beteiligung der Privaten Krankenversicherer ist rechtlich nicht zu beanstanden.

4. Die Regelungen in §§ 291ff. SGB V zeugen von dem großen Bemühen des Gesetzgebers, ein Optimum an Datenschutz zu erreichen.

5. Im Hinblick darauf, dass die Digitalisierung gerade auch im Gesundheitsbereich rasant zunimmt, dementsprechend eine kurzfristige und laufende Anpassung der Sicherheitsvorkehrungen zur Einhaltung des Datenschutzes notwendig ist, aber auch im Hinblick auf die Anfangs-und Erprobungsregelung im Zusammenhang mit der Einführung der TI und im Hinblick auf den Verarbeitungsprozess auf niedrigster Stufe erscheint es akzeptabel und mit dem Bestimmtheitsgrundsatz und der Wesentlichkeitstheorie vereinbar, wenn in den gesetzlichen Regelungen detaillierte Vorgaben und Regelungen zum Sicherheitsniveau und zu den geeigneten Sicherheitsmaßnahmen einschließlich konkreter Gefahren Regelungen zur Gefahrenvorsorge nicht oder nur ungenügend enthalten sind.

6. Maßgeblich für die Beurteilung des Sicherheitsniveaus ist nicht das Sicherheitsprofil (EAL3+) für den Konnektor, sondern das vom Bundesamt für Sicherheit in der Informationstechnik vorgegebene Schutzprofil.

7. Daraus, dass vor dem 14.10.2020 (Gesetzesänderung) keine ausdrücklichen Verantwortlichkeiten im SGB V festgelegt wurden, ergibt sich kein Verstoß gegen die DSGVO (Art. 24, 26).

8. Ein Verstoß gegen Art. 12 Grundgesetz und gegen Art. 2 Grundgesetz (Recht auf informationelle Selbstbestimmung) ist nicht ersichtlich.

| | |
|---|---|
| | 9. Bei bestimmungsgemäßem Anschluss an die TI, bestimmungsgemäßer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen Datenschutzmaßnahmen ist mangels Vorliegen des subjektiven Tatbestandes der strafrechtliche Tatbestand des § 203 StGB nicht erfüllt. |
| Normenkette | - |

**1. Instanz**

| | |
|---|---|
| Aktenzeichen | S 38 KA 190/20 |
| Datum | 26.01.2023 |

**2. Instanz**

| | |
|---|---|
| Aktenzeichen | - |
| Datum | - |

**3. Instanz**

| | |
|---|---|
| Datum | - |

Â

I. Dem Antrag, Beweis durch Einholung eines SachverstÃ¤ndigengutachtens entsprechend der schriftlichen Vorlage des ProzessbevollmÃ¤chtigten zu erheben, wird nicht stattgegeben. Â

II. Die Klage wird abgewiesen.

III. Der KlÃ¤ger trÃ¤gt die Kosten des Verfahrens.

T a t b e s t a n d :

Der KlÃ¤ger, der als Vertragsarzt (Facharzt fÃ¼r Augenheilkunde) zugelassen ist, wendet sich gegen die mit dem angefochtenen Ausgangsbescheid in der Fassung des Widerspruchsbescheids vorgenommenen HonorarkÃ¼rzungen in den Quartalen 1/19 â 4/19 in HÃ¶he von 1 % (= 2.399,11â¬) wegen Nichtteilnahme an der Telematikinfrastruktur (TI).

Zur BegrÃ¼ndung der KÃ¼rzung wurde auf die Rechtsgrundlage des Â§ 291 Abs. 2b Satz 14 a.F. (Satz 9 n.F; Anmerkung: genannte Â§Â§ SGB V ohne Zusatz sind solche, die in den strittigen Quartalen galten oder nach wie vor gelten) hingewiesen. Die Teilnahme an der Telematikinfrastruktur (Online-Abgleich der Versichertenstammdaten) sei u.a. fÃ¼r VertragsÃ¤rzte und VertragszahnÃ¤rzte verpflichtend. Ein VerstoÃ gegen hÃ¶herrangiges Recht liege nicht vor. Die Beklagte setzte sich insbesondere mit den Argumenten des KlÃ¤gers, die dieser im Rahmen des Vorverfahrens vortrug bzw. vortragen lieÃ, auseinander.

So wurde betont, eine Verletzung von Privatgeheimnissen Â§ 203 StGB sei nicht ersichtlich, wenn die Telematikinfrastruktur eingefÃ¼hrt und bestimmungsgemÃ¤Ã betrieben werde; etwas anders stelle sich die Situation dar, wenn es aufgrund fehlender DatenschutzmaÃnahmen (fehlende Absicherung der Hard-oder Software mittels Firewall, ZugriffsbeschrÃ¤nkung oder Ã¤hnlichem) zu einem Datenmissbrauch kommen sollte. Eine Verletzung erfordere immer ein Verschulden oder einen Vorsatz. Ferner sei ein VerstoÃ gegen die Datenschutzgrundverordnung (DSGVO), insbesondere gegen Art. 6 Abs. 1c und e, Abs. 2, Abs. 3 und Art. 9 Abs. 1 Absatz 2, Abs. 3, Abs. 4 DSGVO nicht zu besorgen. Vor allem sei eine GefÃ¤hrdung der Datensicherheit der Praxis-IT-Systeme durch eine Implementierung der TI nicht zu erwarten. Denn die TI sei ein geschlossenes Netz, zu dem nur registrierte Nutzer mit einem elektronischen Ausweis Zugang erhielten. Wesentliches Element sei der Konnektor. Dieser schÃ¼tze die Praxen bzw. Apotheken vor unberechtigten Zugriffen aus dem Internet und aus der TI, indem er die Kommunikation zwischen Praxissoftware, elektronischer Gesundheitskarte, Institutionsausweis und TI koordiniere und verschlÃ¼ssle. Gleichzeitig schÃ¼tze der Konnektor auch die TI vor beispielsweise Schadstoffsoftware in der Arztpraxis. Es sei zwar einzurÃ¤umen, dass die in Â§ 291b Abs. 2 S. 2 SGB V vorgesehenen Stand-Alone-LÃ¶sungen (= Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer) zwar nur bis 19.12.2019 bestanden hÃ¤tten. Diese LÃ¶sungen seien aber nunmehr nicht mehr vorgesehen, da sie mit EinfÃ¼hrung des Anspruchs auf die Notfalldaten nicht mehr einsetzbar seien.

Durch das Zertifizierungsverfahren und die dafÃ¼r notwendige SicherheitsÃ¼berprÃ¼fung fÃ¼r die Herstellung und den Betrieb von Produkten der TI und Diensten gewÃ¤hrleiste dieÂ  G., die die Architektur der TI maÃgeblich definiere und entwickle, dass die sensiblen Gesundheitsdaten vor unbefugtem Zugriff sicher seien. Bei derÂ  G. handle es sich um eine private Gesellschaft mit einer Mehrheitsbeteiligung der Bundesrepublik Deutschland (Gesellschafterbeteiligung: Bundesrepublik Deutschland zu 51 %, vertreten durch das BMG). Es liege im Regelungsspielraum des Gesetzgebers, die Regelungskompetenzen abzugeben.

Auch wenn eine Haftung der Hersteller der Kennektoren und des Betreibers der TI nicht im SGB V geregelt sei, fÃ¼hre das nicht zur Rechtswidrigkeit und Unvereinbarkeit mit hÃ¶herrangigem Recht. Im Ãbrigen hafteten die Hersteller nach Zivilrecht. AuÃerdem stÃ¼nden diese zivilrechtlich auch in einer GewÃ¤hrleistungspflicht.

Soweit der KlÃ¤ger auf Klagen beim Bundeskartellamt wegen unerlaubter Preisabsprachen der Konnektor- und KartenlesegerÃ¤tehersteller hinweise, ergebe sich auch hieraus keine Rechtswidrigkeit. Insgesamt vier Hersteller bÃ¶ten zertifizierte Konnektoren an. FÃ¼r den bundesweiten Betrieb der zentralen TI sei die Firma A. zustÃ¤ndig.

Auch die Finanzierung der Installation der Konnektoren und der laufenden Kosten sei rechtlich nicht zu beanstanden. Die TI-KostenÃ¼bernahme sei in Â§ 291a Abs. 7

S. 5 SGB V geregelt. KBV und GKV-Spitzenverband hÃ¤tten sich in einem Schiedsverfahren auf die Finanzierung der TI in Form von Pauschalen verstÃ¤ndigt (Anlage 32 BMV-Ã). In dem Zusammenhang habe das SG MÃ¼nchen (Beschluss vom 22.03.2019, Az S 38 KA 52/19 ER) die Ansicht vertreten, es handle sich um eine Anschubfinanzierung.

Zusammenfassend seien die angefochtenen Bescheide rechtmÃ¤Ãig. Die KÃ¼rzung sei somit zu Recht erfolgt.

Gegen den Ausgangsbescheid in der Fassung des Widerspruchsbescheides lieÃ der KlÃ¤ger durch seinen Prozessbevollmächtigten Klage zum Sozialgericht MÃ¼nchen einlegen. Zur BegrÃ¼ndung fÃ¼hrte dieser aus, es habe bis zum 19.12.2019 sog. Stand-Alone-LÃ¶sungen gegeben (Â§ 291 Abs. 2 SGB V; = Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer). Eine dem Schutz der Patientendaten angemessene Datensicherheit wÃ¤re nur durch eine Stand-Alone-LÃ¶sung erreichbar. Die Abschaffung sei deshalb erfolgt, weil angeblich die Stand-Alone-LÃ¶sungen nicht vereinbar seien mit der EinfÃ¼hrung des Anspruchs auf Notfalldaten. Zentrales Element der TI sei der Konnektor (=Router, der zusammen mit der Zugangssoftware ein Virtual Private Network (VPN) aufbaut und dabei einen VSDM-Konnektor verwendet).

Hinsichtlich der Datensicherheit des Gesamtsystems bestÃ¼nden massive Bedenken. So habe der Computer Chaos Club (CCC) bereits MÃ¤ngel beim Vergabeprozess der Berechtigungskarten aufgedeckt. Denn es finde die PrÃ¼fung der IdentitÃ¤t der Antragsteller nicht zuverlÃ¤ssig statt. Jedermann habe bis Ende 2019 eine Berechtigungskarte bestellen und diese auch an eine abweichende Anschrift schicken lassen kÃ¶nnen. Ferner sei das Sicherheitsniveau der TI-Konnektoren und Kartenterminals auf der Basis der Norm ISO/IEC 15408 mit EAL3+ niedrig und damit unterhalb dem Niveau digitaler StromzÃ¤hler oder Tachos. Zudem werde gegen das Grundrecht auf informationelle Selbstbestimmung verstoÃen. Zwar handle es sich um keinen gezielten Eingriff in das Grundrecht, wohl aber um massive faktische BeeintrÃ¤chtigungen. Der Einzelne mÃ¼sse stets die Kontrolle Ã¼ber seine Daten behalten (vgl. BVerfG, Entscheidung vom 15. Dezember 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 BVerfGE 65/1). Es fehlten konkrete Regelungen zum erforderlichen Sicherheitsniveau und zu den grundsÃ¤tzlichen Anforderungen an SicherheitsmaÃnahmen. Auch wÃ¼rden konkrete Regeln zur Gefahrenvorsorge unterlassen. Dies sei notwendig, da es hier um besonders sensible Daten im Gesundheitsbereich gehe. AuÃerdem seien solche Eingriffe nur dann zulÃ¤ssig, wenn der Gesetzgeber geeignete SicherheitsmaÃnahmen angeordnet habe. Es sei auch zu besorgen, dass die Ã¤rztliche Schweigepflicht (Â§ 203 StGB) tangiert werde. Unvereinbar sei auch die Beteiligung der Privaten Krankenversicherer und des Wirtschaftlichen Spitzenverbandes der Apotheker mit den Anforderungen des Bundesverfassungsgerichts. Insgesamt verstieÃen die Regelungen im SGB V (Â§Â§ 291 ff. SGB V) gegen die Datenschutzgrundverordnung (DSGVO), insbesondere gegen Art. 32 DSGVO, aber auch gegen Art. 26 DSGVO. Bisher sei der Praxisinhaber fÃ¼r die Verarbeitung von Daten alleinverantwortlich. Andere in die TI Involvierte seien dagegen nicht als (Mit-)Verantwortliche aufgefÃ¼hrt. SchlieÃlich werde auch

gegen die Berufsfreiheit aus Art. 12 GG verstoÃen. Der ProzessbevollmÃ¤chtigte des KlÃ¤gers beantragte, ein SachverstÃ¤ndigengutachten einzuholen.

In ihrer Replik rÃ¤umte die Beklagte ein, es habe Schwachstellen beim Vergabeprozess gegeben. Diese seien aber mit dem Patientendatenschutzgesetz (PDSG) vom 14.10.2020, in Kraft getreten am 20.10.2020 behoben worden. Die von der KlÃ¤gerseite geÃ¤uÃerte BefÃ¼rchtung, wonach von anderen Praxen eine GefÃ¤hrdung ausgehen kÃ¶nne, treffe nicht zu. In dem Zusammenhang werde auf die AusfÃ¼hrungen der G. im White Paper Datenschutz und Informationssicherheit (Stand September 2020) hingewiesen. Danach wÃ¼rden die IT-Systeme der Heilberufe vor Angriffen aus dem Internet, aber auch vor unberechtigten Zugriffen aus der zentralen TI-Plattform geschÃ¼tzt. Das Problem sei nicht der Konnektor, sondern â der richtige Umgang mit den Gegebenheiten vor Ort und das enge Zusammenspiel aller an einer Praxis-IT beteiligten Dienstleisterâ. Zum Argument des ProzessbevollmÃ¤chtigten des KlÃ¤gers, die Regelungen zum Sicherheitsniveau und zu den geeigneten SicherheitsmaÃnahmen einschlieÃlich konkreter Regelungen zur Gefahrenvorsorge mÃ¼ssten durch den Gesetzgeber, nicht aber durch dieÂ  G. erfolgen, vertrat die Beklagte die Auffassung, hierbei mÃ¼sse die rasante Entwicklung auf dem Sektor der Informationstechnologie berÃ¼cksichtigt werden. Es sei fraglich, ob der Gesetzgeber dem Rechnung tragen kÃ¶nne. Eventuell seien die Regelungen dann bei Inkrafttreten des Gesetzes bereits Ã¼berholt. Im Ãbrigen habe der Gesetzgeber mit dem PDSG die Regelungen in den Â§Â§ 291 ff. SGB V Ã¼berarbeitet. So seien auch die Aufgaben derÂ  G. in Â§ 311 Abs. 2 SGB V neu definiert worden. Dies zeige, dass der Gesetzgeber seiner Beobachtungs-und Nachbesserungspflicht nachgekommen sei. Zur Frage der Haftung des Praxisinhabers werde auf das Infoblatt derÂ  G. zum Thema Haftung und Datenschutz im Juli 2019 hingewiesen. Voraussetzung fÃ¼r eine Haftung sei ein Verschulden, das jedenfalls bei einem sachgemÃ¤Ãen Anschluss zu verneinen sei. Haftungsfragen seien als solche zu klÃ¤ren und kein Grund, eine Teilnahme an der TI von vornherein grundsÃ¤tzlich abzulehnen. Ferner lÃ¤gen keinerlei GrundrechtsverstÃ¶Ãe vor, auch nicht gegen das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht aus Art. 12 Grundgesetz. Denn Eingriffe seien im Ã¼berwiegenden Allgemeininteresse unter Beachtung des Grundsatzes der VerhÃ¤ltnismÃ¤Ãigkeit durch Gesetz oder aufgrund eines Gesetzes hinzunehmen und gerechtfertigt. Die Eingriffe seien durch vernÃ¼nftige Belange des Gemeinwohls legitimiert. Im Ãbrigen werde das Grundrecht auf informationelle Selbstbestimmung in seinem Schutz der personenbezogenen Daten durch den Versichertenstammdatenabgleich nur geringfÃ¼gig beschrÃ¤nkt, wie das Bundessozialgericht in seiner Entscheidung vom 20.01.2021 zum Ausdruck gebracht habe (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R). Zudem kÃ¶nne sich der KlÃ¤ger â im subjektiv geprÃ¤gten Sozialgerichtsverfahrenâ grundsÃ¤tzlich nicht auf die Verletzung von Rechten Dritter berufen (LSG Niedersachsen-Bremen, Beschluss vom 17.03.2021, Az L 3 KA 63/20 B ER).

In der mÃ¼ndlichen Verhandlung am 26.01.2023 wurde die Sach-und Rechtslage mit den Beteiligten besprochen. Das Gericht stellte zur weiteren SachaufklÃ¤rung zusÃ¤tzliche Fragen an die anwesenden Beteiligten. Danach, so die Beigeladene ( G.), sei es notwendig gewesen, die Stand-Alone-LÃ¶sung abzuschaffen. Dies sei

fÃ¼r die DurchfÃ¼hrung des Notfalldatenmanagements notwendig gewesen. Im Ãbrigen sei es jedem Leistungserbringer freigestellt, sich zwei Konnektoren zu beschaffen, wobei allerdings darauf hinzuweisen sei, dass der zweite Konnektor nicht mitfinanziert werde. Was die Schwierigkeiten mit dem Vergabeprozess (Stichwort: Berechtigungskarten) betreffe, so habe es auÃer den vom CCC gemeldeten FÃ¤llen keine weiteren konkreten FÃ¤lle gegeben. Es habe sich um kein echtes â□□Szenarioâ□□ gehandelt, sondern nur um DemonstrationsfÃ¤lle. Zur Frage nach dem laut dem Vorbringen der KlÃ¤gerseite niedrigen Sicherheitsprofil (EAL3+) wird ausgefÃ¼hrt, aus dieser Bezeichnung sei nicht auf das tatsÃ¤chliche Sicherheitsniveau zu schlieÃen. Das eigentliche Sicherheitsniveau sei wesentlich grÃ¶Ãer. Das BSI habe auf insgesamt 155 Seiten das Schutzprofil vorgegeben. So gebe es 27 Bausteine; davon seien 25 sowohl fÃ¼r Konnektoren, als auch fÃ¼r smart meter gateway bestimmt. Lediglich bei zwei PrÃ¼fbausteinen, die sich auch nicht auf das Produkt selbst, sondern auf den Entwicklungsprozess beim Hersteller beziehen wÃ¼rden, sei der smart meter gateway hÃ¶her eingestuft, nÃ¤mlich bei insgesamt sieben Stufen, davon die siebte Stufe als die hÃ¶chste Stufe, mit Stufe 4 statt mit Stufe 3. Auf Frage des ProzessbevollmÃ¤chtigten des KlÃ¤gers wurde durch die Beigeladene ( G.) ausgefÃ¼hrt, es treffe nicht zu, dass die Stufe der Schwachstellenanalyse von 5 auf 3 abgesenkt wurde. Was den Austausch der Konnektoren betreffe, so sei dieser wegen des Auslaufens der Sicherheitszertifikate nach fÃ¼nf Jahren fÃ¼r notwendig erachtet worden, da eine ZertifikatsverlÃ¤ngerung nicht stattfand. Denn einer der Hersteller von Konnektoren habe die fÃ¼r die Umsetzung notwendige Software nicht bereitgestellt. Zum sog. Patientenstammdatenabgleich wurde ausgefÃ¼hrt, es seien zu keiner Zeit Patientenstammdaten an die Krankenkassen Ã¼bertragen worden. Der Konnektor frage verschlÃ¼sselt (Kartennummer) lediglich bei der Krankenkasse an, ob es ein Update gebe. Habe sich eine Ãnderung, beispielsweise eine AdressÃ¤nderung ergeben und sei es damit zu einem Update gekommen, werde ebenfalls verschlÃ¼sselt RÃ¼ckmeldung von der Krankenkasse gegeben und die Anpassung auf die Patientenkarte geschrieben.

In der mÃ¼ndlichen Verhandlung am 26.01.2023 Ã¼bergab der ProzessbevollmÃ¤chtigte des KlÃ¤gers dem Gericht einen schriftlich formulierten Beweisantrag, der den Vertretern der Beklagten und den Vertretern der Beigeladenen in Kopie ausgehÃ¤ndigt wurde.

Der KlÃ¤ger selbst trug vor, er halte seit Jahren eine Vielzahl von digitalen PlÃ¤tzen in seiner Praxis vor. Daten von zig-1000 Patienten seien gespeichert. Es handle sich um Ã¤uÃerst sensible Daten. Da seines Erachtens der Datenschutz im Zusammenhang mit der EinfÃ¼hrung der TI unsicher sei, bestehe die Gefahr, dass er der Ã¤rztlichen Schweigepflicht nicht genÃ¼gen kÃ¶nne und sich letztendlich strafrechtlich verantworten mÃ¼sse (Â§ 203 StGB). Es sei ihm ein Anliegen, nicht zwangsweise an die TI angeschlossen zu werden.

Zu der Thematik sind bereits mehrere erstinstanzliche sozialgerichtliche Entscheidungen ergangen, die nach dem aktuellen Kenntnisstand alle noch nicht rechtskrÃ¤ftig sind. Es handelt sich um Entscheidungen des Sozialgerichts Stuttgart (SG Stuttgart, Urteil vom 27.01.2022, Az S 24 KA 166/20), des Sozialgerichts Mainz

(SG Mainz, Urteil vom 27.07.2022, Az S 3 KA 84/20), aber auch des Sozialgerichts MÃ¼nchen (SG MÃ¼nchen, Urteile vom 09.11.2022, u.a. Az S 38 KA 5155/21; bislang nur
im Zahnarzt-Bereich). Die Klagen wurden abwiesen.

Der ProzessbevollmÃ¤chtigte des KlÃ¤gers stellte folgende AntrÃ¤ge:

Es wird beantragt, Beweis durch SachverstÃ¤ndigengutachten entsprechend dem in der mÃ¼ndlichen Verhandlung Ã¼bergebenen schriftlichen Beweisantrag zu erheben (- Der Vergabeprozess fÃ¼r die Berechtigungskarten im Jahr 2019 war aus den auf Seite 5f. der KlagebegrÃ¼ndung genannten GrÃ¼nden unsicher.- In den der Zertifizierung der Netzkonnektoren als Teil der Konnektoren zugrunde liegenden CC-Schutzprofilen BSI-CC-PP-0047 und BSI-CC-PP-0097 wird vorausgesetzt, dass die angeschlossenen Anwendungskonnektoren sicher betrieben werden. Eine Abwehr von Angriffen von Personen, die sich den Zugang zur Telematikinfrastruktur im Gesundheitswesen erschlichen haben, ihn durch Manipulation von IT-Systemen der Leistungserbringern erreicht haben oder ihn zu illegalen Zwecken missbrauchen, ist nicht Gegenstand der Zertifizierung und wird auch sonst in den Vorgaben zum Betrieb der Telematikinfrastruktur im Gesundheitswesen nirgends auf einem dem Schutz von Gesundheitsdaten angemessenen Sicherheitsniveau verlangt. â Ferner wird im Schutzprofil BSI-CC-PP-0047 vorausgesetzt, dass der Betreiber des Netzwerkkonnektors einen sicheren Betrieb des Anwendungskonnektors sicherstellt, ohne dass der einzelne Praxisbetreiber dies sicherstellen kann, weil er keinen Einfluss auf den im Konnektor betriebenen Anwendungskonnektor hat. â Das Sicherheitsniveau EAL3+ fÃ¼r den Konnektor ist nicht ausreichend, weil es kein hohes Sicherheitsniveau beschreibt. Vielmehr ist EAL4+ erforderlich).

Hilfsweise stellte der ProzessbevollmÃ¤chtigte des KlÃ¤gers den Antrag aus dem Schriftsatz vom 28.08.2020.

Die Beklagte beantragte, die Klage abzuweisen.

Die Vertreter der Beigeladenen schlossen sich dem Antrag der Beklagten an.

Beigeladen und Gegenstand der mÃ¼ndlichen Verhandlung
war die Beklagtenakte. Im Ãbrigen wird auf den sonstigen Akteninhalt, insbesondere die SchriftsÃ¤tze der Beteiligten, sowie die Sitzungsniederschrift vom 26.01.2023 verwiesen.

E n t s c h e i d u n g s g r Ã¼ n d e:

Das Gericht hat dem Antrag des ProzessbevollmÃ¤chtigten des KlÃ¤gers, Beweis durch SachverstÃ¤ndigengutachten entsprechend dem in der mÃ¼ndlichen Verhandlung Ã¼bergebenen schriftlichen Beweisantrag zu erheben, nicht stattgegeben. Entsprechend hat es unter I. des Urteils tenoriert. Dies wÃ¤re an sich nicht notwendig gewesen, da es ausreicht, in den EntscheidungsgrÃ¼nden darauf einzugehen (Meyer-Ladewig/Keller Leitherer/ Schmidt, Kommentar zum SGG, Rn. 12c zu Â§ 103), ist aber unschÃ¤dlich. Nach Â§ 103 Satz 2 SGG ist das Gericht an

das Vorbringen und die BeweisantrÃ¤ge der Beteiligten nicht gebunden. Hintergrund hierfÃ¼r ist, dass in sozialgerichtlichen Verfahren nach Â§ 103 Satz 1 SGG eine sog. Amtsermittlungspflicht besteht. Der Sachverhalt ist umfassend, losgelÃ¶st von dem Vorbringen und BeweisantrÃ¤gen der Beteiligten zu ermitteln. BeweisantrÃ¤ge sind daher grundsÃ¤tzlich als Anregungen zu verstehen (Meyer-Ladewig/Keller Leitherer/ Schmidt, Kommentar zum SGG, Rn. 12c zu Â§ 103). Nicht zuletzt aufgrund der Einlassungen der Beteiligten, aber auch im Hinblick auf die vorausgegangenen Entscheidungen der Sozialgerichte wurde nach Auffassung des Gerichts eine Ermittlungsdichte erreicht, die weitere Ermittlungen von Amts wegen erÃ¼brigt und dazu fÃ¼hrt, den Rechtsstreit als entscheidungsreif anzusehen.

Die zum Sozialgericht MÃ¼nchen eingelegte Klage ist zulÃ¤ssig, erweist sich jedoch als unbegrÃ¼ndet. Der angefochtene Ausgangsbescheid in der Fassung des Widerspruchsbescheides ist rechtmÃ¤Ã□ig.
Rechtsgrundlage fÃ¼r die vorgenommene KÃ¼rzung (Honorarabzug) ist Â§ 291 Abs. 2b S. 14 SGB V. Danach ist die VergÃ¼tung vertragsÃ¤rztlicher Leistungen pauschal um ein Prozent zu kÃ¼rzen, wenn die an der vertrags(-zahn)Ã¤rztlichen Versorgung teilnehmenden Ã□rzte die PrÃ¼fung nach Â§ 291 Abs. 2b S. 2 SGB V nicht durchfÃ¼hren. Nach Â§ 291 Abs. 2c S. 2 SGB V ist die VergÃ¼tung vertrags(-zahn)Ã¤rztlicher Leistungen pauschal um ein Prozent solange zu kÃ¼rzen, bis der Nachweis, dass die Ã□rzte Ã¼ber die fÃ¼r den Zugriff auf die elektronische Patientenakte erforderlichen Komponenten und Dienste verfÃ¼gen, nicht erbracht wird. Konkret hat der KlÃ¤ger weder den Nachweis gefÃ¼hrt, noch hat er den online-Datenabgleich vorgenommen, sodass die seit dem PflegepersonalstÃ¤rkungsgesetz (PpSG) gewÃ¤hrte FristverlÃ¤ngerung zur Anbindung an die Telematikinfrastruktur und DurchfÃ¼hrung des Versichertenstammdatenmanagements bis zum 30.06.2019 (Â§ 291 Abs. 2b S. 14 und 15 in der Fassung vom 11.12.2018) nicht gilt.
Die HonorarkÃ¼rzung ist nur dann rechtmÃ¤Ã□ig, wenn die Verpflichtung zur Teilnahme an der Telematikinfrastruktur ihrerseits rechtmÃ¤Ã□ig ist. Dies setzt insbesondere voraus, dass die Regelungen Ã¼ber die Telematikinfrastruktur mit hÃ¶herrangigem Recht, insbesondere der Datenschutzgrundverordnung (DSGVO) zu vereinbaren sind.
Das Sozialgericht Stuttgart (SG Stuttgart, Urteil vom 27.01.2022, Az S 24 KA 166/20 ) hatte in einem Verfahren ebenfalls Ã¼ber die RechtmÃ¤Ã□igkeit der HonorarkÃ¼rzung wegen Nichtteilnahme von VertragsÃ¤rzten an der Telematikinfrastruktur zu entscheiden. Diese Entscheidung betraf das Quartal 1/2019. Das Gericht kam zu dem Ergebnis, Â§Â§ 291 Absatz 2b S. 3, S. 14 SGB V a.F. seien nicht wegen VerstoÃ□es gegen hÃ¶herrangiges Recht, insbesondere nicht wegen eines VerstoÃ□es gegen die DSGVO nichtig.
Im Einzelnen setzte sich das SG Stuttgart mit der Vereinbarkeit der Regelungen der Â§Â§ 291 ff. SGB V a.F. mit Art. 6 Abs. 1 DSGVO (Wahrnehmung einer Aufgabe, die im Ã¶ffentlichen Interesse liegt), Art. 6 Abs. 3 S. 4 DSGVO (VerhÃ¤ltnismÃ¤Ã□igkeitsgrundsatz), Art. 9 Abs. 1 DSGVO, Art. 5 Abs. 1f DSGVO (Grundsatz der angemessenen Datensicherheit der Datenverarbeitung), Art. 4 Nr 7 DSGVO (Verantwortlichkeit), Art. 24, 26 Abs. 1 S. 1 DSGVO, Art. 35 DSGVO (DatenschutzfolgenabschÃ¤tzung) und Art. 12 Grundgesetz (GG) sehr ausfÃ¼hrlich auseinander. Das Urteil ist nicht rechtskrÃ¤ftig (Berufung zum LSG Baden-WÃ¼rttemberg).

Zudem gelangte das Sozialgericht Mainz (SG Mainz, Urteil vom 27.07.2022, Az S 3 KA 84/20) zu dem Ergebnis, die erfolgte HonorarkÃ¼rzung auf der Grundlage von Â§ 291 Abs. 2b S 3, S. 14 SGB V a.F. sei rechtmÃ¤Ã□ig. Vom Gericht geprÃ¼ft wurde insbesondere die Vereinbarkeit der Vorschriften des SGB V (Â§Â§ 291ff.) mit Art. 6 Abs. 1 S. 1 DSGVO, Art. 6 Abs. 1e DSGVO, Art. 6 Abs. 3 DSGVO, Art. 9 DSGVO, Art. 5 Abs. 1f DSGVO, Art. 32 DSGVO und Art. 35 DSGVO sowie mit Art. 12 Grundgesetz. Das SG Mainz fÃ¼hrte aus, die Vorschriften wÃ¼rden nicht gegen die Vorgaben der DSGVO verstoÃ□en. Insbesondere handle es sich um einen Ã¼berschaubaren Datenverarbeitungsprozess. AuÃ□erdem sei eine kontinuierliche Ã□berwachung der Einhaltung der datenschutzrechtlichen Vorgaben durch die Gesellschaft und die Anbieter von Diensten und Anwendungen im Rahmen der TI hinreichend gewÃ¤hrleistet.
Ende 2022 war das SG MÃ¼nchen (SG MÃ¼nchen, Urteile vom 09.11.2022, u.a. Az S 38 KA 5155/21) mit HonorarkÃ¼rzungen im Zahnarzt-Bereich wegen Nichtteilnahme an der TI (Klagen mehrerer VertragszahnÃ¤rzte) befasst. Auch hier wurden die Klagen abgewiesen.

Des Weiteren prÃ¼fte das Bundessozialgericht (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R), wenn auch in anderem Zusammenhang, die RechtmÃ¤Ã□igkeit und Vereinbarkeit der Â§Â§ 291 ff. SGB V mit der DSGVO. Gegenstand des dortigen Verfahrens war, ob fÃ¼r die beklagte Krankenkasse eine Verpflichtung bestand, einer Versicherten einen Weg zu erÃ¶ffnen, ihre Berechtigung zur Inanspruchnahme von vertragsÃ¤rztlichen Leistungen nachweisen zu kÃ¶nnen, ohne dabei die E-Gesundheitskarte verwenden und einen online erfolgenden Abgleich von Versichertenstammdaten dulden zu mÃ¼ssen. Das Bundessozialgericht hat hierzu ausgefÃ¼hrt, die aktuellen gesetzlichen Vorgaben zur E-Gesundheitskarte und ihre Einbeziehung in die TI stÃ¼nden im Einklang mit den Vorgaben der Datenschutzgrundverordnung (Art. 6 Abs. 1 S. 1 DSGVO, Art. 6 Abs. 3 S. 4 DSGVO, Art. 5 Abs. 1 Buchst. f DSGVO). Es handle sich um legitime Zwecke und bedeutende Gemeinwohlbelange, zumal hierdurch der Leistungsmissbrauch erschwert werde und dies der finanziellen StabilitÃ¤t der gesetzlichen Krankenversicherung zugutekomme. Das Bundessozialgericht betonte auch, es gebe keine absolute Datensicherheit. Im Ã□brigen sprach das Bundessozialgericht (aaO) von einem hinreichend normdichten und klaren RegelungsgefÃ¼ge, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler MaÃ□nahmen der Datensicherheit diene. Der Gesetzgeber sei auch spÃ¤ter seiner Beobachtungs-und Nachbesserungspflicht nachgekommen.
Das Sozialgericht MÃ¼nchen nimmt auf die o.g. Entscheidungen Bezug. Zudem ist im streitgegenstÃ¤ndlichen Verfahren wie folgt auszufÃ¼hren:
Was die genannte Entscheidung des Bundessozialgerichts betrifft (BSG, aaO), ist diese auf die vorliegende Rechtsstreitigkeit nicht unmittelbar Ã¼bertragbar. Denn Gegenstand des hier anhÃ¤ngigen Verfahrens ist die Frage, ob insbesondere unter Wahrung der Vorschriften der DSGVO ein Leistungserbringer, hier der Vertrags-(zahn)arzt zur Teilnahme an der Telematikinfrastruktur verpflichtet werden kann. Das Bundessozialgericht hat sich aber mit den auch hier maÃ□geblichen Regelungen im SGB V (Â§Â§ 291 ff SGB V) umfassend auseinandersetzt und die Regelungen fÃ¼r datenschutzrechtlich unbedenklich und mit der DSGVO vereinbar

angesehen. Die rechtlichen ErwÃ¤gungen kÃ¶nnen folglich mittelbar und ohne weiteres auch auf das streitgegenstÃ¤ndliche Verfahren aus dem Bereich des Vertragsarztrechtes Ã¼bertragen werden.
Die Teilnahme der VertragsÃ¤rzte an der Telematikinfrastruktur steht im Zusammenhang mit der EinfÃ¼hrung der sog. elektronischen Gesundheitskarte (E-Gesundheitskarte), die den Versicherten von der Krankenkasse ausgestellt wird (Â§ 291a Abs. 1 SGB V). Nach Â§ 291 Abs. 2 SGB V enthÃ¤lt sie verschiedene Angaben, nÃ¤mlich sog. Patientenstammdaten. Â§ 291 Abs. 2, Abs. 3 SGB V regelt die Zwecke, fÃ¼r die die E-Gesundheitskarte geeignet sein muss. In dem strittigen Zeitraum (Jahr 2019) stellen die an der vertragsÃ¤rztlichen Versorgung teilnehmenden Ã□rzte/ZahnÃ¤rzte bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten im Quartal die Leistungspflicht der Krankenkasse durch Nutzung der Dienste fest. Dazu ermÃ¶glichen sie den Online-Abgleich und die Aktualisierung der auf der elektronischen Gesundheitskarte gespeicherten Daten nach Abs. 1 und 2 mit den bei der Krankenkasse vorliegenden aktuellen Daten. Die PrÃ¼fungspflicht gilt ab dem Zeitpunkt, ab dem die Dienste nach Â§ 291 Abs. 1 SGB V sowie die Anbindung an die Telematikinfrastruktur zur VerfÃ¼gung stehen (Â§ 291 Abs. 2b S. 4 SGB V). Nach Â§ 291 Abs. 2b S. 6 SGB V ist die DurchfÃ¼hrung der PrÃ¼fung auf der E-Gesundheitskarte zu speichern. GegenÃ¼ber den zustÃ¤ndigen Kassen(-zahn)Ã¤rztlichen Vereinigungen besteht eine Nachweispflicht durch die an der vertrags(-zahn)Ã¤rztlichen Versorgung teilnehmenden Leistungserbringer (Â§ 291 Abs. 2c S. 1 SGB V). Nach der ErlÃ¤uterung der Beigeladenen findet ein sog. Patientenstammdatenabgleich jedenfalls in der Weise nicht statt, dass Stammdaten an die Krankenkassen Ã¼bertragen werden. Vielmehr wird nach Einlesen der Versichertenkarte in der Arztpraxis Ã¼ber den Konnektor verschlÃ¼sselt (Kartennummer) bei der Krankenkasse angefragt, ob es ein Update gibt. Liegt ein solches vor, erfolgt eine verschlÃ¼sselte RÃ¼ckmeldung von der Krankenkasse. Diese Ã□nderung wird dann auf die Patientenkarte geschrieben.

Komponenten und Dienste der Telematikinfrastruktur werden von derÂ  G. zugelassen (Â§ 291 b Abs. 1 a S.1 SGB V). DieÂ  G. prÃ¼ft dabei die FunktionsfÃ¤higkeit und InteroperabilitÃ¤t auf der Grundlage der von ihr verÃ¶ffentlichen PrÃ¼fkriterien (Â§ 291 b Abs. 1 a S.4 SGB V). Vorgesehen ist auch eine sogenannte Sicherheitszertifizierung nach Â§ 291b Abs. 1a S. 5 SGB V. Kommt es zu StÃ¶rungen, die zu einer betrÃ¤chtlichen Auswirkung auf die Sicherheit und FunktionsfÃ¤higkeit der Telematikinfrastruktur fÃ¼hren kÃ¶nnen oder bereits gefÃ¼hrt haben, hat die Gesellschaft fÃ¼r Telematik dies dem Bundesamt fÃ¼r Sicherheit in der Informationstechnik zu melden (Â§ 291b Abs. 6 S. 4 SGB V). Bei SicherheitsmÃ¤ngeln kann das Bundesamt fÃ¼r Sicherheit in der Informationstechnik der Gesellschaft fÃ¼r Telematik verbindliche Anweisungen zur Beseitigung der festgestellten SicherheitsmÃ¤ngel erteilen (Â§ 291b Abs. 8 S. 2 SGB V).
Bei der DSGVO handelt es sich um EU-Recht. Die Verordnung entfaltet unmittelbare Wirkung und ist verbindlich, ohne dass diese in nationale Rechtsakte umgesetzt werden muss. Bei einer Kollision der DSGVO mit einfachem nationalen Recht ergibt sich ein Vorrang des EU-Rechts. Es handelt sich um einen sogenannten Anwendungsvorrang (vgl EuGHE 1964, 1251/1279).

Ohne Zweifel stellt der Abgleich der personenbezogenen Daten nach Â§ 291 Abs. 2b S. 2 SGB V eine Datenverarbeitung nach Art. 4 DSGVO dar. Nach Art. 4 Ziff 2 DSGVO ist unter Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgefÃ¼hrte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten zu verstehen. Darunter fallen auch ein Auslesen und ein Abgleich von Daten (Art. 4 Ziff. 2 DSGVO). Die Legaldefinition fÃ¼r personenbezogene Daten findet sich in Art. 4 Ziff. 1 DSGVO. Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natÃ¼rliche Person beziehenâ¦ Damit ist der Anwendungsbereich der DSGVO (Art. 1 DSGVO) erÃ¶ffnet.
Die Regelungen des Â§Â§ 291 ff. SGB V sind mit den allgemeinen GrundsÃ¤tzen der DSGVO (Art. 4, 5, 6) vereinbar. Insbesondere dient der Datenabgleich der Wahrnehmung einer Aufgabe, die im Ã¶ffentlichen Interesse liegt (Art. 6 Abs. 1 DSGVO). Ebenso wird der Grundsatz der VerhÃ¤ltnismÃ¤Ãigkeit in Art. 6 Abs. 3 S. 4 DSGVO eingehalten. Danach muss auch das Recht des Mitgliedstaats ein im Ã¶ffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen VerhÃ¤ltnis zu dem verfolgten legitimen Zweck stehen. Die PrÃ¼fung des VerhÃ¤ltnismÃ¤Ãigkeitsgrundsatzes erfordert die Beurteilung der Eignung und Erforderlichkeit des gewÃ¤hlten Mittels zur Erreichung des erstrebten Zwecks sowie eine vorzunehmende EinschÃ¤tzung und Prognose der dem Einzelnen oder der Allgemeinheit drohenden Gefahren (BVerfG, Urteil vom 09.03.1994, Az 2 BvL 43/92 ). Der mit der Telematikinfrastruktur verfolgte Zweck, konkret der von dem Vertrags-(zahn) Arzt im Jahr 2019 vorzunehmende Datenabgleich nach Â§ 291 Abs. 2b S. 2 SGB V bestand insbesondere in der Verhinderung von Missbrauch der Krankenversichertenkarte, zur Kosteneinsparung und zur Abrechnung der Leistungen durch den Vertrags-(zahn)Arzt, insgesamt zur GewÃ¤hrleistung der finanziellen StabilitÃ¤t der GKV. Es ist nicht ersichtlich, dass es andere, gleich geeignete, weniger belastende MÃ¶glichkeiten gibt, um die legitimen Ziele zu erreichen (vgl BSG, Beschluss vom 20.01.2021, B 1 KR 7/20 ER). Vielmehr drÃ¤ngt sich auf, die MÃ¶glichkeiten der elektronischen Datenverarbeitung auch im gesundheitlichen Bereich, allerdings bei gleichzeitiger besonderer Wahrung des Datenschutzes zu nutzen, wie sie auch in anderen Bereichen seit lÃ¤ngerer Zeit bereits Verwendung finden.
Zu den wichtigsten zu beachtenden Regelungen in der DSGVO gehÃ¶rt die Sicherheit der Daten. Damit die Ziele der DSGVO (Art. 1 Abs. 2 DSGVO), nÃ¤mlich der Schutz der Grundrechte und Grundfreiheiten natÃ¼rlicher Personen, insbesondere deren Rechte auf Schutz persÃ¶nlicher personenbezogener Daten erreicht werden, mÃ¼ssen nach Art. 5 Abs. 1 Buchst. f DSGVO â die Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewÃ¤hrleistet, einschlieÃlich Schutz vor unbefugter oder unrechtmÃ¤Ãiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter ZerstÃ¶rung oder unbeabsichtigter SchÃ¤digung durch geeignete technische und organisatorische MaÃnahmen (â IntegritÃ¤t und Vertraulichkeitâ)â.
Der Verarbeitungsprozess in den Quartalen 1/19-4/19 besteht darin, dass der an der vertragsÃ¤rztlichen Versorgung teilnehmende Vertrags-(zahn)arzt bei der erstmaligen Inanspruchnahme seiner Leistungen durch einen Versicherten im Quartal die Leistungspflicht der Krankenkasse durch Nutzung der Dienste nach Â§

291 Abs. 2b S. 2 SGB V prÃ¼ft. Dies geschieht durch einen Online-Abgleich der auf der elektronischen Gesundheitskarte gespeicherten Daten nach Abs. 1 und 2 mit den bei der Krankenkasse vorliegenden aktuellen Daten (Â§ 291 Abs. 2b S. 3 SGB V ). Zu den Patientenstammdaten zÃ¤hlen die Bezeichnung der ausstellenden Krankenkasse, einschlieÃlich eines Kennzeichens fÃ¼r die KassenÃ¤rztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat (Nr 1), der Familienname und Vorname des Versicherten (Nr 2), das Geburtsdatum des Versicherten (Nr 3), das Geschlecht des Versicherten (Nr 4), die Anschrift des Versicherten (Nr 5), die Krankenversichertennummer des Versicherten (Nr 6), der Versichertenstatus, fÃ¼r die Personengruppe nach Â§ 264 Abs. 2 der Status der auftragsweisen Betreuung (Nr 7), der Zuzahlungsstatus des Versicherten (Nr 8), der Tag des Beginns des Versicherungsschutzes (Nr 9), bei befristeter GÃ¼ltigkeit elektronischen Gesundheitskarte das Datum des Fristablaufs (Nr 10). Das Sozialgericht MÃ¼nchen, wohl aber auch die bisher befassten Sozialgerichte sind bisher von einem Abgleich aller sog. Patientenstammdaten im Wege der Ãbermittlung von der jeweiligen Praxis an die Krankenkassen und RÃ¼ckleitung ausgegangen. Wie dies im Einzelnen geschieht, wurde, soweit ersichtlich, in den vorangegangenen Entscheidungen nicht thematisiert. Nunmehr, nÃ¤mlich im Rahmen der mÃ¼ndlichen Verhandlung am 26.01.2023 vor dem Sozialgericht MÃ¼nchen wurden Einzelheiten des sog. Online-Datenabgleich bekannt. Danach â so die Vertreter derÂ  G. â wird bei der Krankenkasse verschlÃ¼sselt angefragt, ob es ein Update gibt. Ist dies der Fall, beispielsweise, weil sich beim Patienten eine AdressÃ¤nderung ergeben hat und es damit zu einem Update gekommen ist, wird ebenfalls verschlÃ¼sselt RÃ¼ckmeldung von der Krankenkasse gegeben und die Anpassung auf die Patientenkarte geschrieben. In den strittigen Quartalen findet somit weder ein Abgleich der Patientenstammdaten im eigentlichen Sinn statt, denn es wird nur verschlÃ¼sselt angefragt, ob es ein update gibt, geschweige denn werden Daten Ã¼ber den einzelnen Gesundheitsstatus des Versicherten verarbeitet. Auch werden vom Vertrags(-zahn)arzt selbst Daten nicht erhoben, nicht erfasst, nicht angepasst oder verÃ¤ndert (Landessozialgericht Niedersachsen-Bremen, Beschluss vom 17.03.2022, Az L 3 KA 63/20 B ER Rn 32).

Nach Art. 5 Abs. 1 Buchstabe f DSGVO wird eine âangemesseneâ Datensicherheit gefordert. Bei dem Begriff âangemessenâ handelt es sich um einen unbestimmten Rechtsbegriff, der der Auslegung zugÃ¤nglich ist. In dem Zusammenhang bekrÃ¤ftigt das Gericht seine Auffassung, wonach umso hÃ¶here Anforderungen an die Datensicherheit zu stellen sind, um das Risiko vor unbefugtem Zugriff Dritter mÃ¶glichst gering zu halten, je umfangreicher und personenbezogener Daten sind, die verarbeitet werden. Die Anforderungen an die Datensicherheit sind somit unterschiedlich und abhÃ¤ngig von der Art, dem Umfang der Daten und der konkreten Datenverarbeitung. Ganz allgemein gilt, eine absolute Datensicherheit ist nicht zu fordern und wÃ¤re auch mit einem noch so groÃen technischen und organisatorischen Aufwand nicht darstellbar (vgl BSG, Urteil vom 20.01.2021, B 1 KR 7/20 R).

In Umsetzung dieser grundsÃ¤tzlichen ErwÃ¤gungen auf das streitgegenstÃ¤ndliche Verfahren, ist zunÃ¤chst festzustellen, dass die Nutzung der Dienste zwar im Zusammenhang mit der elektronischen Patientenkarte steht, es

sich in den strittigen Quartalen aber um einen Verarbeitungsprozess auf niedrigster Stufe handelt. Denn es findet rein tatsÃ¤chlich nicht einmal ein Abgleich der Patientenstammdaten im eigentlich Sinn statt. Entsprechend Art und Umfang des Verarbeitungsprozesses sind folglich geringe Anforderungen an den Datenschutz zu stellen.

Nachdem der Gesetzgeber derÂ  G. im Zusammenhang mit der Telematikinfrastruktur eine wesentliche Rolle zugedacht hat, kommt es darauf an, ob diese Institution den Anforderungen an eine â angemesseneâ Datensicherheit formell und materiell gerecht wird. Auch stellt sich die Frage, ob es derÂ  G. qua Gesetz Ã¼berlassen werden kann, die wesentlichen, mit der EinfÃ¼hrung der Telematikinfrastruktur zusammenhÃ¤ngenden MaÃnahmen, darunter insbesondere SicherheitsmaÃnahmen zur GewÃ¤hrleistung des Datenschutzes zu treffen. Als Aufgaben derÂ  G. sind die Erstellung der funktionalen und technischen Vorgaben einschlieÃlich eines Sicherheitskonzepts (Â§ 291b Abs. 1 Ziff 1 SGB V), die Festlegung des Inhalts und der Struktur der DatensÃ¤tze fÃ¼r deren Bereitstellung und Nutzung (Â§ 291b Abs. 1 Ziff 2 SGB V), die Erstellung und Ãberwachung der Vorgaben fÃ¼r den sicheren Betrieb der Telematikinfrastruktur (Â§ 291b Abs. 1 Ziff 3 SGB V), die Sicherstellung der notwendigen Test-und ZertifizierungsmaÃnahmen (Â§ 291b Abs. 1 Ziff 4 SGB V) und die Festlegung der Verfahren einschlieÃlich der dafÃ¼r erforderlichen Authentisierungsverfahren zur Verwaltung der in Â§ 291a Abs. 4 und 5a geregelten Zugriffsberechtigungen und der Steuerung der Zugriffe auf Daten nach Â§ 291 Abs. 3 (Â§ 291b Abs. 1 Ziff 5 SGB V) genannt. DieÂ  G. wird in der Rechtsform einer GmbH gefÃ¼hrt, bestehend aus mehreren Gesellschaftern, konkret die Bundesrepublik Deutschland und die in Â§ 291a Abs. 7 SGB V genannten Spitzenorganisationen (Spitzenverband Bund der Krankenkassen, die KassenÃ¤rztliche Bundesvereinigung, die KassenzahnÃ¤rztliche Bundesvereinigung, die BundesÃ¤rztekammer, die BundeszahnÃ¤rztekammer, die Deutsche Krankenhausgesellschaft, Spitzenorganisationen der Apotheker). Dabei entfallen auf die Bundesrepublik Deutschland ein Anteil von 51 %, ein Anteil von 24,5 % auf den Spitzenverband Bund der Krankenkassen und ein weiterer Anteil von 24,5 % auf die Ã¼brigen Spitzenorganisationen (Â§ 291b Abs. 2 Ziff. 1 SGB V). Mit Gesetz vom 14.10.2020 erfolgte eine Ãnderung des SGB V u.a. durch Neuformulierung bestehender Vorschriften und durch EinfÃ¼gung der Vorschriften der Â§Â§ 306 ff SGB V.
Der KlÃ¤ger Ã¤uÃert Vorbehalte dahingehend, die Beteiligung der Privaten Krankenversicherer und des wirtschaftlichen Spitzenverbandes der Apotheker sei mit den Anforderungen des Bundesverfassungsgerichts unvereinbar. In dem Zusammenhang ist zunÃ¤chst zu bemerken, dass in Â§ 291a Abs. 7 SGB V eine Beteiligung der Privaten Krankenversicherer nicht vorgesehen war. Erst mit GesetzesÃ¤nderung zum 14.10.2020 wurde eine Beteiligung der Privaten Krankenversicherer fakultativ durch Beschluss der Gesellschafter derÂ  G. (Â§ 310 Abs. 3 SGB V) mÃ¶glich; sie ist aber nicht verbindlich. Was die Beteiligung des Spitzenverbandes der Apotheker anbelangt, aber auch eine eventuelle Beteiligung der Privaten Krankenversicherer, bestehen dagegen keine rechtlichen Bedenken, soweit die Anteile Ã¼berwiegend bei der Bundesrepublik Deutschland, vertreten durch das BMG (= Mehrheitsgesellschafterin mit 51 %) und den KÃ¶rperschaften des Ã¶ffentlichen Rechts liegen. Denn die Einbindung des Spitzenfachverbandes der

Apotheker in die TI erscheint im Zusammenhang mit der EinfÃ¼hrung des E-Rezeptes unerlÃ¤sslich. Soll die Vernetzung einheitlich sein und auch sinnvollerweise Privatversicherten zugute kommen, kann die Einbindung der Privaten Krankenversicherer nicht ernsthaft infrage gestellt werden.
Im Rahmen der ErfÃ¼llung der Aufgaben derÂ  G. hat der Gesetzgeber eine Zusammenarbeit mit dem Bundesamt fÃ¼r Sicherheit in der Informationstechnik (BSI) und mit der/dem Bundesbeauftragten fÃ¼r den Datenschutz und die Informationsfreiheit (BfDI) verbindlich vorgegeben. So ist, wenn bei den Festlegungen und MaÃnahmen nach Â§ 291b Abs. 1 SGB V Fragen der Datensicherheit berÃ¼hrt sind, ein Einvernehmen mit dem BSI herzustellen. Ferner ist in Â§ 291b Abs. 1e S. 1 SGB V geregelt, dass die Gesellschaft fÃ¼r Telematik sichere Verfahren zur Ãbermittlung medizinischer Dokumente in Abstimmung mit dem BSI festlegt. FÃ¼r die Zulassung von Komponenten und Diensten der Telematikinfrastruktur entwickelt das BSI geeignete PrÃ¼fvorschriften und verÃ¶ffentlicht diese im Bundesanzeiger. Das NÃ¤here zum Zulassungsverfahren und zu den PrÃ¼fkriterien wird von derÂ  G. in Abstimmung mit dem BSI beschlossen (Â§ 291 b Abs. 1a S. 6 und 7 SGB V). Nach Â§ 291b Abs. 4 SGB V ist vor der Beschlussfassung zu Regelungen, dem Aufbau und dem Betrieb der Telematikinfrastruktur dem BSI und dem BfDI Gelegenheit zur Stellungnahme zu geben, sofern Belange des Datenschutzes oder der Datensicherheit berÃ¼hrt sind. Auch, soweit von Komponenten und Diensten eine Gefahr fÃ¼r die FunktionsfÃ¤higkeit oder Sicherheit der Telematikinfrastruktur ausgeht, ist dieÂ  G. in Abstimmung mit dem BSI befugt, die erforderlichen technischen und organisatorischen MaÃnahmen zur Abwehr dieser Gefahr zu treffen. FÃ¼r die zugelassenen Dienste und Betreiber besteht die Pflicht, erhebliche StÃ¶rungen der VerfÃ¼gbarkeit, der IntegritÃ¤t, der AuthentizitÃ¤t und Vertraulichkeit dieser Dienste unverzÃ¼glich derÂ  G. zu melden (Â§ 291b. Abs. 6 S. 2 SGB V). DieÂ  G. ist dann ihrerseits verpflichtet, diese StÃ¶rungen unverzÃ¼glich dem BSI zu melden (Â§ 291b. Abs. 6 S. 4 SGB V). Auf Verlangen des BSI hat dieÂ  G. die in Â§ 291b Abs. 8 S. 1 SGB V genannten Dokumente vorzulegen. Wenn sich daraus SicherheitsmÃ¤ngel ergeben sollten, kann das BSI derÂ  G. verbindliche Anweisungen zur Beseitigung der festgestellten SicherheitsmÃ¤ngel erteilen (Â§ 291b Abs. 8 S. 2 SGB V).
Des Weiteren sieht das Gesetz in Â§ 291b Abs. 2a SGB V die Einrichtung eines Beirats durch die Gesellschaft fÃ¼r Telematik vor, der diese in fachlichen Belangen berÃ¤t. Der Beirat besteht zwingend aus insgesamt 17 Vertretern, nÃ¤mlich aus vier Vertretern der LÃ¤nder, drei Vertretern der fÃ¼r die Wahrnehmung der Interessen der Patienten und der Selbsthilfe chronisch kranker und behinderter Menschen maÃgeblichen Organisationen, drei Vertretern der Wissenschaft, einen durch das Bundesministerium fÃ¼r Gesundheit im Einvernehmen mit dem Bundesministerium fÃ¼r Bildung und Forschung zu benennenden Vertreter aus dem Bereich der Hochschulmedizin, drei Vertretern der fÃ¼r die Wahrnehmung der Interessen der Industrie maÃgeblichen BundesverbÃ¤nde aus dem Bereich der Informationstechnologie im Gesundheitswesen, einem Vertreter der fÃ¼r die Wahrnehmung der Interessen der hausarztzentrierten Versorgung teilnehmenden VertragsÃ¤rzte maÃgeblichen Spitzenorganisationen sowie der oder dem Bundesbeauftragten fÃ¼r den Datenschutz und die Informationsfreiheit und der oder dem Beauftragten der Bundesregierung fÃ¼r die Belange der Patientinnen und

Patienten.
In Â§ 291c SGB V ist ferner die verbindliche Einrichtung einer Schlichtungsstelle bei der Gesellschaft fÃ¼r Telematik vorgesehen, deren Entscheidungen fÃ¼r alle Gesellschafter, fÃ¼r die Leistungserbringer und Krankenkassen sowie fÃ¼r ihre VerbÃ¤nde nach diesem Buch verbindlich sind.
Die BeschlÃ¼sse der Gesellschaft fÃ¼r Telematik zu den Regelungen, dem Aufbau und dem Betrieb der Telematikinfrastruktur sind fÃ¼r die Leistungserbringer und die Krankenkassen sowie ihre VerbÃ¤nde nach diesem Buch verbindlich (Â§ 291b Abs. 4 S. 1 SGB V). AuÃerdem ist dieÂ  G. Betreibern von Diensten gegenÃ¼ber weisungsbefugt (Â§ 291b Abs. 8 S. 6 SGB V).
Somit verfÃ¼gt dieÂ  G. einerseits Ã¼ber umfangreiche eigene Kompetenzen, so vor allem eine eigene Kompetenz, Festlegungen und MaÃnahmen der Datensicherheit (Â§Â§ 291b Abs. 1, 291b Abs. 1e SGB V), darunter auch MaÃnahmen der Gefahrenabwehr zu treffen (Â§ 291b Abs. 6 S. 1 SGB V), Entscheidungen Ã¼ber die Zulassung von Diensten und Betreibern zu treffen (Â§ 291b Abs. 1a SGB V), auch gegebenenfalls den Zugang zur Telematikinfrastruktur zu sperren oder nur unter Auflagen zu gestatten (Â§ 291b Abs. 6 S. 6 SGB V).
Andererseits ist den Regelungen, insbesondere Â§ 291b SGB V immanent, dass bei MaÃnahmen und Entscheidungen, die die Datensicherheit betreffen, ein Einvernehmen bzw. eine Abstimmung mit dem BSI und/oder der/dem BfDI erforderlich ist. FÃ¼r dieÂ  G. besteht auch gegenÃ¼ber dem BSI eine Meldepflicht bei erheblichen StÃ¶rungen (Â§ 291b Abs. 4 S. 2 SGB V). Das BSI ist ebenfalls gegenÃ¼ber derÂ  G. zu Weisungen befugt. Hinzu kommt auch die Einrichtung des Beirates nach Â§ 291b Abs. 2a SGB V und einer Schlichtungsstelle nach Â§ 291c SGB V, beides Einrichtungen, die ihrerseits ein zusÃ¤tzliches â□□Mehrâ□□ an Datensicherheit garantieren. Auch wenn ein solches Procedere auf den ersten Blick raschen Entscheidungsprozessen zuwiderlÃ¤uft, trÃ¤gt dieses nicht unmaÃgeblich zu einem â□□Mehrâ□□ an Datensicherheit bei. Es handelt sich also um eine nicht unerhebliche Kompetenzzuweisung an dieÂ  G., in der strukturell neben der Bundesrepublik Deutschland die maÃgeblichen Institutionen im Gesundheitswesen vertreten sind, diese aber begrenzt durch zahlreiche Kontrollmechanismen, die vor allem dem BSI und der/dem BfDI Ã¼berantwortet wurden.
Damit zeugen die Regelungen in Â§Â§ 291 ff. SGB V von dem groÃen BemÃ¼hen des Gesetzgebers, ein Optimum an Datenschutz zu erreichen. Das Bundessozialgericht (aaO) spricht deshalb nicht umsonst von einem â□□risikobasierten Ansatzâ□□ der Regelungen der Â§Â§ 291 ff. SGB V, einem normdichten und klaren RegelungsgefÃ¼ge, das durch eine Vielzahl aufeinander abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler MaÃnahmen der Datensicherheit dient und eine ausreichende Datensicherheit gewÃ¤hrleistet. Es ist kaum vorstellbar, dass in einem der anderen Mitgliedstaaten, in dem auch die Vorschriften der DSGVO gelten, bei der Verarbeitung personenbezogener Daten im Gesundheitswesen eine vergleichbare Regelungsdichte zum Schutz dieser Daten vorhanden ist. Dies hat auch der Vertreter derÂ  G. in der mÃ¼ndlichen Verhandlung so deutlich gemacht. Nicht bekannt ist auch, dass in anderen Bereichen des Wirtschaftslebens Ã¤hnliche Sicherheitsvorkehrungen bestehen.
Zudem ist festzustellen, dass der Gesetzgeber in den Regelungen, die elektronische Patientenkarte und die Telematikinfrastruktur betreffend (Â§Â§ 291ff. SGB V),

umfangreich festgelegt hat, wer an der Umsetzung der Telematikinfrastruktur beteiligt ist und welche Aufgaben den einzelnen an der TI Beteiligten Ã¼berantwortet sind. Das Gericht rÃ¤umt aber zugleich ein, dass im SGB V keine oder kaum detaillierte Vorgaben und Regelungen zum Sicherheitsniveau und zu den geeigneten SicherheitsmaÃnahmen einschlieÃlich konkreter Regelungen zur Gefahrenvorsorge enthalten sind (Stand: Jahr 2019). Trotzdem teilt das Gericht nicht die Auffassung des ProzessbevollmÃ¤chtigten des KlÃ¤gers, es sei Aufgabe des Gesetzgebers, diese Punkte durch Gesetz oder aufgrund eines Gesetzes zu regeln. Im Zusammenhang mit dem Vorbehalt des Gesetzes in Art. 20 Grundgesetz wurde die sog. Wesentlichkeitstheorie von der Rechtsprechung entwickelt. Danach muss der Gesetzgeber alle wesentlichen Entscheidungen, die von Grundrechtsrelevanz sind, selbst treffen (BVerfGE 77,170/230f; 98, 218/251; 101, 1 /34, 108, 282/312, 136, 69; Jarass/Pieroth, Kommentar zum Grundgesetz fÃ¼r die Bundesrepublik Deutschland, Rn. 72 zu Art. 20). AuÃerdem ist den Bestimmtheitsanforderungen Rechnung zu tragen (Jarass/Pieroth, Kommentar zum Grundgesetz fÃ¼r die Bundesrepublik Deutschland, Rn. 72 zu Art. 20). Dabei handelt es sich nicht nur darum, dass Ã¼berhaupt ein bestimmter Gegenstand geregelt ist, sondern darum, in welchem Umfang die Regelungen den Gegenstand festzulegen haben. Vorauszusetzen ist daher, dass die Regelungen ausreichend detailliert sind (Jarass/Pieroth, Kommentar zum Grundgesetz fÃ¼r die Bundesrepublik Deutschland, Rn. 82 zu Art. 20). Die ausreichende Bestimmtheit hÃ¤ngt von Art und Schwere des Eingriffs in die Grundrechte ab. Wird gegen den Bestimmtheitsgrundsatz und den Grundsatz, dass der Gesetzgeber selbst alle wesentlichen Entscheidungen mit Grundrechtsrelevanz treffen muss, verstoÃen, sind solche MaÃnahmen verfassungswidrig.
Im Hinblick auf das Verarbeitungsgeschehen und den Verarbeitungsprozess auf niedrigster Stufe in den Quartalen des Jahres 2019 sind an die ausreichende Bestimmtheit allerdings relativ geringe Anforderungen zu stellen, auch wenn ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung als Ausfluss der allgemeinen Handlungsfreiheit bei Verarbeitung von Patientendaten grundsÃ¤tzlich nicht auszuschlieÃen ist. Bei der Frage, welche wesentlichen Regelungen dem Gesetzgeber hier vorbehalten sind, damit der Wesentlichkeitstheorie und dem Bestimmtheitsgrundsatz Rechnung getragen wird, ist auch zu berÃ¼cksichtigen, dass die Digitalisierung auf allen Gebieten, so auch im Gesundheitsbereich weltweit rasant zunimmt und immer mehr die Lebenswirklichkeit bestimmt. In immer kÃ¼rzeren zeitlichen AbstÃ¤nden besteht Veranlassung, solche Regelungen neu einzufÃ¼gen bzw. bereits bestehende Regelungen anzupassen. Dies macht es erforderlich, dass die Sicherheitsvorkehrungen zur Einhaltung des Datenschutzes ebenfalls kurzfristig und laufend angepasst sowie nachjustiert werden mÃ¼ssen. Es handelt sich somit um eine Besonderheit der Materie, die schnelles Handeln verlangt. Die BefÃ¼rchtung der Beklagten, es sei fraglich, ob der Gesetzgeber dem Rechnung tragen kÃ¶nne, weil die Regelungen bereits bei Inkrafttreten des Gesetzes bereits Ã¼berholt sein kÃ¶nnten, erscheint deshalb nicht unbegrÃ¼ndet, auch wenn sich die Gesetzgebungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 13, Art. 72 Abs. 2 GG ergibt und eine gesetzliche Neuregelung, Anpassung oder Ãnderung nicht der Zustimmung der BundeslÃ¤nder bedarf. Im Hinblick darauf, dem Umstand, dass es sich um eine Anfangs-und Erprobungsregelung handelt, und der Datenverarbeitungsprozess auf niedrigster Stufe, verbunden mit einem

entsprechend geringen Risiko stattfindet, erscheint es akzeptabel und mit den dargestellten GrundsÃ¤tzen vereinbar, wenn in den gesetzlichen Regelungen (Â§Â§ 291 ff. SGB V) detaillierte Vorgaben und Regelungen zum Sicherheitsniveau und zu den geeigneten SicherheitsmaÃnahmen einschlieÃlich konkreter Regelungen zur Gefahrenvorsorge nicht oder nur ungenÃ¼gend enthalten sind.
Gleichwohl wird immer wieder Ã¼ber Probleme bei der praktischen Umsetzung berichtet (zm 108, Nummer 4, 16.02.2018 (245)). Konkret war zum Beispiel im Jahr 2020 die Rede von einer StÃ¶rung der Versichertenstammdaten bei der Telematikinfrastruktur und von konfigurationsbedingten SicherheitsmÃ¤ngeln bei Konnektoren bestimmter Hersteller. Davon seien Ã¼ber einen Zeitraum von acht Wochen bis zu 80.000 Arzt/Zahnarztpraxen betroffen gewesen (zm 110, Nummer 15-16, 16.08.2020, (1472)). Die EinfÃ¼hrung des sogenannten E- Rezeptes wurde gestoppt. Auch die EinfÃ¼hrung der sogenannten elektronischen ArbeitsunfÃ¤higkeitsbescheinigung (eAU) ist â soweit ersichtlich -noch nicht abgeschlossen. AuÃerdem besteht die Absicht, die Konnektoren zu tauschen, was zu erheblichen Kosten fÃ¼hren dÃ¼rfte. Insgesamt wird sogar zum Teil die Auffassung vertreten, âdie regelmÃ¤Ãigen Pannen belegen, dass der gegenwÃ¤rtige Ansatz der Vernetzung nicht hinreichend praxiserprobt und fÃ¼r die Digitalisierung im Gesundheitswesen im Ergebnis dysfunktional istâ (BZB, November 2021). SchlieÃlich hat auch der Chaos Computer Club (CCC) auf verschiedene SicherheitslÃ¼cken hingewiesen.
Es mag sein, dass die in den Medien geschilderten Probleme mehr oder weniger auftraten. Zum Teil drÃ¤ngt sich allerdings der Eindruck auf, dass die Berichterstattung hierzu zu plakativ ist, dem Gerieren von Schlagzeilen geschuldet ist und als âAufhÃ¤ngerâ dienen soll, der Schaffung der Telematikinfrastruktur nicht nur kritisch gegenÃ¼ber zu stehen, sondern diese pauschal und gÃ¤nzlich abzulehnen. Aus den in den Medien geschilderten Problemen ist jedoch nicht auf mangelnde Datensicherheit zu schlieÃen.
ZunÃ¤chst kann nicht erwartet werden, dass die EinfÃ¼hrung der Telematikinfrastruktur von Beginn an âreibungslosâ verlÃ¤uft. Die Telematikinfrastruktur befindet sich in einer Anfangs- und Erprobungsphase, die bis zur definitiven Umsetzung der in Â§ 291a Abs. 3 SGB V genannten, sehr ambitionierten Ziele nicht nur Monate, sondern Jahre dauern dÃ¼rfte. Denn es handelt sich um ein Novum im Gesundheitswesen, das in den fortgeschrittenen Ausbaustufen geradezu als revolutionÃ¤r zu bezeichnen ist und fÃ¼r das nicht auf Erfahrungswerte aus der Vergangenheit zurÃ¼ckgegriffen werden kann. Der Chief Produktion Office derÂ  G., Herr H. hat darauf hingewiesen, âwir befinden uns in einer EinfÃ¼hrungsphase eines der wichtigsten Massenprozesse des Gesundheitswesens, das jÃ¤hrlich rund 77 Millionen Mal durchgefÃ¼hrt wird.â
Vor diesem Hintergrund, dem Umstand, dass es sich um eine Anfangs- und Erprobungsphase handelt, sind gewisse UnschÃ¤rfen bei den gesetzlichen Regelungen und deren Umsetzung hinzunehmen, vorausgesetzt, dass der Beobachtungs- und Nachbesserungspflicht nachgekommen wird (vgl BSG, Beschluss vom 20.01.2021, B 1 KR 7/20 ER). Werden SicherheitslÃ¼cken im Datenschutz bekannt, so sind diese umgehend zu beheben. Der Datenschutz muss auch jeweils dem Stand der Technik entsprechen. Eine absolute Datensicherheit ist, wie bereits ausgefÃ¼hrt, nicht darstellbar. Dass der Gesetzgeber der Beobachtungs- und Nachbesserungspflicht genÃ¼gt, ergibt sich daraus, dass immer

wieder die gesetzlichen Regelungen angepasst werden (vgl. Gesetz vom 14.10.2020 (BGBl I S. 2115)). Ausgeschlossen ist es aber, die EinfÃ¼hrung der Telematikinfrastruktur grundsÃ¤tzlich infrage zu stellen. Denn der Gesetzgeber hat sich hierfÃ¼r entschieden. In diesem Zusammenhang wird darauf hingewiesen, dass die Bundesrepublik Deutschland, obwohl zu einer der fÃ¼hrenden Wirtschaftsnationen gehÃ¶rend, im Ranking unter den 27 bewerteten europÃ¤ischen LÃ¤ndern nach dem Digital economy and society index (DESI) im Jahr 2022 lediglich einen mittleren Platz (Platz 13) einnimmt.
Was den Vortrag der KlÃ¤gerseite betrifft, es gebe Schwachstellen im Vergabeprozess â angeblich fand keine zuverlÃ¤ssige PrÃ¼fung der IdentitÃ¤t der Antragsteller statt; jedermann habe bis Ende 2019 eine Berechtigungskarte bestellen und diese auch an eine abweichende Anschrift schicken lassen kÃ¶nnen â ist dies auch nach dem Vortrag der KlÃ¤gerseite ab Anfang 2020 nicht mehr mÃ¶glich. In den Quartalen des Jahres 2019 handelte es sich um eine Anfangs-und Erprobungsregelung, in denen gewisse Schwachstellen hinzunehmen sind, sofern diese nach Art und Umfang nicht ein AusmaÃ annehmen, die die Telematikinfrastrukur insgesamt in Frage stellt. Dies ist aber nicht der Fall, wie sich darin zeigt, dass es nach den AusfÃ¼hrungen der Beigeladenen auÃer den vom Computer-Chaos-Club (CCC) gemeldeten FÃ¤llen keine weiteren konkreten FÃ¤lle gab, es sich um kein echtes Szenario handelte, sondern nur um DemonstrationsfÃ¤lle. Hinzu kommt, dass diese Schwachstellen spÃ¤ter behoben wurden und insofern der Beobachtungs-und Nachbesserungspflicht nachgekommen wurde.
Nach Auffassung des Gerichts kann aus dem vergebenen Sicherheitsprofil (EAL3+) nicht auf ein zu niedriges Sicherheitsniveau geschlossen werden. Denn es gibt insgesamt sieben EAL-Stufen, sodass die Einstufung mit EAL3+ in der Mitte liegt. Dass smart meter gateway mit einem Sicherheitsprofil von EAL4 hÃ¶her eingestuft sind, bedeutet nicht zwangslÃ¤ufig, dass das Sicherheitsniveau der Konnektoren zu niedrig wÃ¤re. Abgesehen davon sind nach Aussage der Beigeladenen in der mÃ¼ndlichen Verhandlung am 26.01.2023 smart meter gateway lediglich bei zwei PrÃ¼fbausteinen, die sich auch nicht auf das Produkt selbst, sondern auf den Entwicklungsprozess beim Hersteller beziehen, hÃ¶her eingestuft, nÃ¤mlich mit Stufe 4 statt mit Stufe 3. AuÃerdem wurde die Stufe der Schwachstellenanalyse nicht von 5 auf 3 abgesenkt. Im Ãbrigen spiegelt die Einstufung mit EAL3+ nicht das tatsÃ¤chliche Sicherheitsniveau wieder. Dieses ergibt sich vielmehr aus dem vom Bundesamt fÃ¼r Sicherheit in der Informationstechnik (BSI) nach Â§ 291b Abs. 1a S. 6 SGB V auf 155 Seiten vorgegebenen Schutzprofil.
Zutreffend haben die Beteiligten darauf hingewiesen, dass dem Konnektor eine zentrale Bedeutung zukommt. Denn der Zugang der Heilberufler zur Telematikinfrastruktur findet Ã¼ber den Konnektor statt. DieÂ  G. hat in ihrem White Paper Datenschutz und Informationssicherheitsstand September 2020 die Sicherheitsstruktur allgemein, aber auch im Einzelnen erlÃ¤utert. Zu unterscheiden ist zwischen der TI-Plattform dezentrale Zone und der TI-Plattform zentrale Zone. Zur zentralen Zone gehÃ¶ren die Karten aller Beteiligten, die Kartenterminals, der sogenannte Konnektor, sowie die GerÃ¤tekarten, die den Kartenterminals und Konnektoren eine eindeutige IdentitÃ¤t zuordnen. Dagegen enthÃ¤lt die zentrale TI-Plattform Zone Zentraldienste der TI-Plattform, die die Anwendungen der Telematikinfrastruktur mit grundlegenden FunktionalitÃ¤ten unterstÃ¼tzen. In dem

White Paper Datenschutz und Informationssicherheit wird zum Konnektor wie folgt ausgefÃ¼hrt: â□□Damit die Heilberufe auf die zentrale TI-Plattform zugreifen kÃ¶nnen, baut der Konnektor einen sicheren Kanal zu den VPN-Zugangsdiensten der Telematikinfrastruktur auf. Diese auf Netzebene gesicherte Verbindung (ein Virtuell-Private-Netzwerk-Tunnel mittels Internet Protocol Security) zur zentralen TI-Plattform wird Ã¼ber das Internet hergestellt. Sensible Daten, die Ã¼ber diese Verbindung versandt werden, sind zusÃ¤tzlich auf Transportebene geschÃ¼tzt (Transport Layer Security)â□¦In seiner Funktion als Firewall auf Netz-und Anwendungsebene schÃ¼tzt der Konnektor sowohl die IT-Systeme der Heilberufler als auch die zentrale TI-Plattform. Die IT-Systeme der Heilberufler werden vor Angriffen aus dem Internet, aber auch vor unberechtigten Zugriffen aus der zentralen TI-Plattform geschÃ¼tzt.â□□ Insofern kann die von KlÃ¤gerseite geÃ¤uÃ□erte BefÃ¼rchtung, wonach von anderen Praxen eine GefÃ¤hrdung ausgehen kÃ¶nne, nicht geteilt werden.
Ebenfalls nicht geteilt wird auch die Ansicht der KlÃ¤gerseite, nur durch sog. Stand-Alone-LÃ¶sungen (= Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer) kÃ¶nne eine dem Schutz der Patientendaten â□□angemesseneâ□□ Sicherheit gewÃ¤hrleistet werden. Diese Stand-Alone-LÃ¶sungen gab es noch bis Ende 2019, sodass der Einwand jedenfalls fÃ¼r die hier streitbefangenen Quartale nicht gilt. Im Ã□brigen ist nicht ersichtlich, dass die Aufgabe der Stand-Alone-LÃ¶sungen nicht hinnehmbare Auswirkungen auf die Datensicherheit hat. Auch zukÃ¼nftig sind die Leistungserbringer, so auch der KlÃ¤ger nicht gehindert, sich einen zweiten Konnektor allerdings auf eigene Kosten zu beschaffen, falls trotzdem Zweifel an der Sicherheit der Daten bestehen sollten. Ein VerstoÃ□ der gesetzlichen Regelungen der Â§Â§ 291 ff. SGB V gegen Art. 5 Buchst. f DSGVO ist deshalb nicht festzustellen.
Die KlÃ¤gerseite beanstandet ferner, dass die datenschutzrechtliche Verantwortlichkeit ganz oder jedenfalls Ã¼berwiegend dem Vertrags-(zahn)arzt auferlegt ist. Es trifft zu, dass erst mit Gesetz vom 14.10.2020 (BGBl I S. 2115) datenschutzrechtliche Verantwortlichkeiten in Â§ 307 SGB V geregelt sind. Danach (Â§ 307 Abs. 1 SGB V) liegt die Verantwortung fÃ¼r die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach Â§ 306 Abs. 2 Nr 1 SGB V (insbesondere ordnungsgemÃ¤Ã□e Inbetriebnahme, Wartung und Verwendung der Komponenten) bei denjenigen, die diese Komponenten fÃ¼r die Zwecke der Authentifizierung und elektronischen Signatur sowie zur VerschlÃ¼sselung, EntschlÃ¼sselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen. Ferner ist der Anbieter des gesicherten Netzes innerhalb des gesicherten Netzes fÃ¼r Ã□bertragung von personenbezogenen Daten verantwortlich, insbesondere von Gesundheitsdaten der Versicherten, zwischen Leistungserbringern, KostentrÃ¤gern sowie Versicherten und fÃ¼r die Ã□bertragung im Rahmen der Anwendungen der elektronischen Gesundheitskarte (Â§ 307 Abs. 3 S. 2 SGB V). Auch dieÂ  G. wurde nunmehr in den Kreis der datenschutzrechtlich Verantwortlichen in Â§ 307 Abs. 5 S. 1 SGB V mit aufgenommen. So ist sie verantwortlich fÃ¼r die Verarbeitung personenbezogener Daten in der Telematikinfrastruktur, soweit sie im Rahmen ihrer Aufgaben nach Â§ 311 Abs. 1 die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden AbsÃ¤tzen begrÃ¼ndet ist. Es handelt sich somit um eine subsidiÃ¤re Verantwortlichkeit derÂ  G., was sich daraus ergibt,

dass diese nur dann besteht, soweit nicht die in Â§ 307 Abs. 1, 3 und 4 SGB V genannten verantwortlich sind.
Daraus, dass vor dem 14.10.2020 keine ausdrÃ¼cklichen Verantwortlichkeiten im SGB V festgelegt wurden, ergibt sich allerdings kein VerstoÃ gegen die DSGVO. Denn, wer datenschutzrechtlicher Verantwortlicher ist, folgt bereits aus der Legaldefinition in Art. 4 Ziff 7 DSGVO. Danach ist Verantwortlicher die natÃ¼rliche oder juristische Person, BehÃ¶rde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen Ã¼ber die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dieser setzt unter BerÃ¼cksichtigung der Art, des Umfangs, der UmstÃ¤nde und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken fÃ¼r die Rechte und Freiheiten natÃ¼rlicher Personen geeignete technische und organisatorische MaÃnahmen um, um sicherzustellen und den Nachweis dafÃ¼r zu erbringen zu kÃ¶nnen, dass die Verarbeitung gemÃ¤Ã dieser Verordnung erfolgt (Art. 24 DSGVO). Daraus folgt zumindest indirekt die Verantwortlichkeit fÃ¼r die natÃ¼rliche Person oder juristische Person, BehÃ¶rde, Einrichtung oder andere Stelle fÃ¼r die Einhaltung des Datenschutzes innerhalb der eigenen SphÃ¤re. Der Vertragszahnarzt hat keine Verantwortung fÃ¼r die Datenschutzsicherheit der zentralen Zone der TI (TI-Plattformzone zentral), auf die er keinen Einfluss hat. Es ergibt sich auch keine Gesamtverantwortlichkeit des Vertrags-(zahn)arztes, sondern nur eine Verantwortlichkeit fÃ¼r die dezentrale Zone. Eine solche Verantwortlichkeit des Vertragszahnarztes fÃ¼r die dezentrale Zone stellt kein Novum dar. Denn bereits vor EinfÃ¼hrung der E-Gesundheitskarte lag es im Verantwortungsbereich des Vertrags-(zahn)arztes, die datenschutzrechtlichen Vorgaben in seiner SphÃ¤re zu beachten. Jegliche Haftung ist auÃerdem verschuldensabhÃ¤ngig, sodass ein Haftungsrisiko fÃ¼r den Vertragsarzt bei bestimmungsgemÃ¤Ãem Anschluss an die TU, bestimmungsgemÃ¤Ãer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen DatenschutzmaÃnahmen (zum Beispiel Absicherung der Hard-und Software) nicht besteht. Im Ãbrigen wurde, wie der Vertreter derÂ  G. in der mÃ¼ndlichen Verhandlung am 09.11.2022 in den vorausgegangenen Verfahren (aaO) ausfÃ¼hrte, bereits Mitte 2019 ein Informationsblatt zum Datenschutz und Haftung in der Telematikinfrastruktur herausgegeben.
AuÃerdem schreibt die DSGVO nicht verpflichtend die Nennung eines/der Verantwortlichen vor. Vielmehr steht es im Ermessen der Mitgliedstaaten nach Art. 4 Ziff.7 DSGVO, ob der Verantwortliche als solcher nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen wird (vgl. SG Stuttgart, Urteil vom 27.01.2022, Az S 24 KA 166/20).
Auch ein VerstoÃ gegen Art. 26 DSGVO ist nicht ersichtlich, wenn keine gemeinsame Verantwortlichkeit festgelegt wurde. Es ist bereits fraglich, ob dieÂ  G. in den Quartalen des Jahres 2019 als verantwortlich im Sinne von Art. 4 Nr 7 DSGVO anzusehen ist. Allein dadurch, dass dieÂ  G. Komponenten und Dienste der Telematikinfrastruktur (Â§ 291b Abs. 1a SGB V) zulÃ¤sst und als â actus contrariusâ Komponenten und Dienste fÃ¼r den Zugang sperren kann (Â§ 291b Abs. 5 S. 6 SGB V), besitzt sie zumindest eine Entscheidungsbefugnis Ã¼ber die Mittel der Datenverarbeitung. Dagegen ist eine Entscheidungsbefugnis derÂ  G., was den Zweck, also das ob, wofÃ¼r und wie weit der Datenverarbeitung betrifft, nicht ersichtlich. Denn die Entscheidungsbefugnis mÃ¼sste von einem

Eigeninteresse an der Datenverarbeitung getragen sein, was aber nicht der Fall ist. Vielmehr fungiert dieÂ  G. lediglich als organisatorische und koordinierende Institution und erfÃ¼llt als solche nur die ihr auferlegten gesetzlichen Pflichten (aA . Dochau in MedR 2020, 979, 985; KÃ¼hling/Sackmann, Datenschutzrecht, Rn. 538, 541).
Abgesehen davon bestimmt Art. 26 Abs. 1 S. 2 DSGVO, dass â gemeinsam Verantwortlicheâ in einer Vereinbarung in transparenter Form festlegen, wer von Ihnen welche Verpflichtung gemÃ¤Ã dieser Verordnung erfÃ¼lltâ¦ Eine solche Vereinbarung wurde nicht geschlossen und wÃ¤re auch nicht umsetzbar, zumal jeder einzelne an der TI teilnehmende Vertrags-(zahn)arzt in einer Individualvereinbarung mit derÂ  G. die wechselseitigen Verpflichtungen festlegen mÃ¼sste. Es mÃ¼ssten also etliche 1.000 Vereinbarungen allein in Bayern geschlossen werden. Hinzu kommt, dass in die Telematikinfrastruktur zahlreiche unterschiedliche Dienste und Komponenten eingebunden sind, die durchaus als verantwortlich im Sinne von Art. 4 Ziff. 7 DSGVO anzusehen wÃ¤ren. An sich mÃ¼ssten mit diesen Diensten ebenfalls Individualvereinbarungen, betreffend die gemeinsame Verantwortlichkeit im Sinne von Art. 26 DSGVO abgeschlossen werden, was ebenfalls nicht umsetzbar ist.
Dass in Zukunft Ã¼ber die TI weitere Anwendungen stattfinden sollen (so zum Beispiel Verarbeitung von Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form fÃ¼r eine einrichtungsÃ¼bergreifende, fallbezogene Kooperation (elektronischer Arztbrief; Â§ 291a Abs. 3 Ziff. 2 SGB V) und die Verarbeitung von Daten Ã¼ber Befunde, Diagnosen, TherapiemaÃnahmen, Behandlungsberichten sowie Impfungen fÃ¼r eine fall-und einrichtungsÃ¼bergreifende Dokumentation Ã¼ber die Versicherten sowie durch von Versicherten selbst oder fÃ¼r Sie zur VerfÃ¼gung gestellte Daten (elektronische Patientenakte; Â§ 291a Abs. 3 Ziff. 2 SGB V), ist nicht Gegenstand im streitgegenstÃ¤ndlichen Verfahren, sodass Ã¼ber deren Vereinbarkeit mit der DSGVO nicht zu befinden ist. In der Tat gehen diese Anwendungen weit Ã¼ber den in Â§ 291 Abs. 2b S. 2 SGB V verpflichtenden Datenabgleich hinaus. Ohne einer spÃ¤teren rechtlichen Bewertung und Entscheidung vorgreifen zu wollen, wird zu beachten sein, dass, je umfangreicher die Datenverarbeitung stattfinden soll, umso grÃ¶Ãer also das GefÃ¤hrdungspotenzial ist, umso grÃ¶Ãere Anforderungen sind an die Datensicherheit zu stellen.
Zusammenfassend kommt das Gericht zu dem Ergebnis, dass die Vorschriften der Â§Â§ 291 ff. SGB V mit der DSGVO rechtlich zu vereinbaren sind.
SchlieÃlich muss auch der mit der Nichtteilnahme an der Telematikinfrastruktur verbundene Honorarabzug seinerseits verhÃ¤ltnismÃ¤Ãig sein. Bei VerstoÃ gegen die Pflicht zur Fortbildung nach Â§ 95d SGB V betrÃ¤gt der Honorarabzug zunÃ¤chst 10 % fÃ¼r die ersten vier Quartale, spÃ¤ter dann 25 % (Â§ 95d Abs. 3 S. 3 SGB V). Wird der Fortbildungsnachweis nicht spÃ¤testens zwei Jahre nach dem Ablauf des FÃ¼nfjahreszeitraums gefÃ¼hrt, steht auch die Zulassung zur vertrags(-zahn) Ã¤rztlichen TÃ¤tigkeit zur Disposition (Â§ 95 Abs. 6 SGB V). Gemessen daran handelt sich um einen moderaten Honorarabzug (zunÃ¤chst 1 %, spÃ¤ter 2,5 % vom Gesamthonorar) bei Nichtteilnahme an der Telematikinfrastruktur. Eine Verpflichtung des Vertrags-(zahn)arztes zur Teilnahme an der Telematikinfrastruktur ohne jegliche Sanktion wÃ¼rde dazu fÃ¼hren, dass sich ein

Teil der Vertrags-(zahn)Ã¤rzte der Telematikinfrastruktur trotzdem anschlieÃen, ein anderer Teil aber sanktionslos davon Abstand nehmen kÃ¶nnte. Damit kÃ¶nnten die Ziele der EinfÃ¼hrung der E- Gesundheitskarte nicht erreicht werden. Der Grundsatz der VerhÃ¤ltnismÃ¤Ãigkeit in Bezug auf die HonorarkÃ¼rzung ist trotz der in den Quartalen des Jahres 2019 Ã¤uÃerst eingeschrÃ¤nkten Datenverarbeitung (Online-Abgleich) gewahrt. Wenn es bei der Datenverarbeitung solcher Art und solchen AusmaÃes bliebe, dann wÃ¤re in der Tat die VerhÃ¤ltnismÃ¤Ãigkeit der HonorarkÃ¼rzung grundsÃ¤tzlich, zumindest aber der HÃ¶he nach kritisch zu wÃ¼rdigen. Jedoch ist hier zu berÃ¼cksichtigen, dass die Nutzung der Dienste in mehreren Schritten gesteigert werden und die Telematikinfrastruktur kÃ¼nftig zu einem BÃ¼ndel unterschiedlicher Anwendungen dienen soll. WÃ¼rden bereits bei den ersten Schritten der EinfÃ¼hrung keine Sanktionen (KÃ¼rzungen) erfolgen oder wÃ¼rden die Sanktionen geringer sein mit der Folge, dass ein Teil der Vertrags-Ãrzte keine Veranlassung sehen wÃ¼rden, sich an die TI anzuschlieÃen, hÃ¤tte dies weitreichende Konsequenzen fÃ¼r die vom Gesetzgeber in Zukunft beabsichtigte umfangreichere Nutzung der TI. Insofern ist es mit dem VerhÃ¤ltnismÃ¤Ãigkeitsgrundsatz vereinbar, dass bereits am Anfang der EinfÃ¼hrung der TI Sanktionen (KÃ¼rzungen) in der genannten HÃ¶he erfolgen.
Wenn allerdings ein Vertrags-(zahn)arzt seiner Verpflichtung zur Teilnahme an der Telematikinfrastruktur deshalb nicht nachkommen kann, weil dieser technische Probleme entgegenstehen, handelt es sich um eine rechtliche und tatsÃ¤chliche UnmÃ¶glichkeit. In diesem Fall wÃ¤re es als unverhÃ¤ltnismÃ¤Ãig anzusehen, das Honorar zu kÃ¼rzen. Allerdings wÃ¤re vom Vertrags-(zahn)arzt der Nachweis zu fÃ¼hren, dass eine solche Konstellation vorliegt.
Soweit wegen der verpflichtenden Teilnahme der Vertrags-(zahn)Ã¤rzte an der Telematikinfrastruktur ein VerstoÃ gegen Art. 12 Grundgesetz geltend gemacht wird, ist diese Auffassung nicht zu teilen. Denn es ist zu differenzieren zwischen einer Berufswahl- und einer BerufsausÃ¼bungsregelung. Allenfalls kÃ¶nnte hier in der verpflichtenden Teilnahme an der Telematikinfrastruktur, konkret im Online-Abgleich der auf der elektronischen Gesundheitskarte gespeicherten Daten mit den bei der Krankenkasse vorliegenden aktuellen Daten eine BerufsausÃ¼bungsregelung gesehen werden. Dabei ist festzustellen, dass die Eingriffstiefe in das Grundrecht im Jahr 2019 relativ gering ist. Vor diesem Hintergrund ist anerkannt, dass eine solche BerufsausÃ¼bungsregelung zulÃ¤ssig ist, wenn â sachlich nachvollziehbare ErwÃ¤gungen des Normgebers im Hinblick auf die Gestaltungsfreiheitâ vorliegen (BVerfG, Beschluss vom 16.07.2004, Az 1 BvR 1127/01; BSG, Urteil vom 13.05.2020, Az B 6 KA 24/18 R). Wie bereits im Zusammenhang mit dem in Art. 6 Abs. 3 DSGVO enthaltenen VerhÃ¤ltnismÃ¤Ãigkeitsgrundsatz ausgefÃ¼hrt, dient die EinfÃ¼hrung der Telematikinfrastruktur dazu, einen Missbrauch der Krankenversichertenkarte, wie in der Vergangenheit nicht selten zu beobachten war, zu verhindern, sie dient der Kosteneinsparung und der Abrechnung der Leistungen durch den Vertrags-(zahn)arzt, also insgesamt zur GewÃ¤hrleistung der finanziellen StabilitÃ¤t der GKV. Es handelt sich somit um sachlich nachvollziehbare ErwÃ¤gungen des Normgebers, die einen Eingriff in die BerufsausÃ¼bungsfreiheit nach Art. 12 GG rechtfertigen (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R).
Genausowenig ist ein VerstoÃ gegen Art. 2 Abs. 1 GG (allgemeine

Handlungsfreiheit) ersichtlich. Es ist anerkannt, dass es sich hierbei um ein sog. Auffanggrundrecht handelt, das gegenÃ¼ber dem in Art. 12 Abs. 1 GG speziellen Grundrecht zurÃ¼cktritt (BVerfG, Beschluss vom 06.06.1989, Az 1 BvR 921/85; Bayerischer Verwaltungsgerichtshof, Urteil vom 18.04.2013, Az 10 B 11.1529). Von dem Schutzbereich des Art. 2 Abs. 1 GG erfasst und Ausfluss der allgemeinen Handlungsfreiheit in Art. 2 Abs. 1 GG ist auch das Recht auf informationelle Selbstbestimmung (vgl BVerfG, Beschluss vom 13.06.2007, Az 1 BvR 1550/03). GeschÃ¼tzt wird der Einzelne gegen informationsbezogene MaÃnahmen, die ihn betreffen und die fÃ¼r ihn weder Ã¼berschaubar, noch beherrschbar sind. Der Einzelne ist befugt, grundsÃ¤tzlich selbst Ã¼ber die Preisgabe und Verwendung seiner persÃ¶nlichen Daten zu bestimmen (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R). Nachdem der Vertrags-(zahn)arzt nicht Grundrechtsbetroffener ist, da seine eigenen personenbezogenen Daten nicht betroffen sind, kann allein deshalb ein VerstoÃ gegen das Recht auf informationelle Selbstbestimmung nicht vorliegen. So hat das Landessozialgericht Niedersachsen-Bremen (LSG Niedersachsen-Bremen, Beschluss vom 17.03.2021, Az L 3 KA 63/20 B ER) ausgefÃ¼hrt, â im subjektiv geprÃ¤gten Sozialgerichtsverfahrenâ kÃ¶nne sich der KlÃ¤ger grundsÃ¤tzlich nicht auf die Verletzung von Rechten Dritter berufen. Selbst wenn dies zu bejahen wÃ¤re, kann nichts Anderes gelten als fÃ¼r den betroffenen Patienten, dessen Daten erfasst und weitergegeben werden. Denn das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos. Eine solche GrundrechtseinschrÃ¤nkung ist zulÃ¤ssig, wenn sie auf einer gesetzlichen ErmÃ¤chtigung beruht, die ihrerseits einen legitimen Gemeinwohlzweck verfolgt und der Grundsatz der VerhÃ¤ltnismÃ¤Ãigkeit eingehalten wird (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R). Dies ist, wie wiederholt ausgefÃ¼hrt wurde, der Fall.
Neben der haftungsrechtlichen Fragestellung hat die KlÃ¤gerseite die BefÃ¼rchtung geÃ¤uÃert, es sei zu besorgen, dass sich der Vertragsarzt strafrechtlich (Â§ 203 StGB) verantworten mÃ¼sse, wenn er sich an die TI anschlieÃe und es zu einem Datenmissbrauch komme. Nach Â§ 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persÃ¶nlichen Lebensbereich gehÃ¶rendes Geheimnis oder ein Betriebs-oder GeschÃ¤ftsgeheimnis offenbart das ihm als Arzt, Zahnarzt anvertraut worden oder sonst bekannt gegeben worden ist. Selbst wenn der objektive Tatbestand von Â§ 203 StGB erfÃ¼llt wÃ¤re, ist bei bei bestimmungsgemÃ¤Ãem Anschluss an die TI, bestimmungsgemÃ¤Ãer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen DatenschutzmaÃnahmen (zum Beispiel Absicherung der Hard-und Software) der subjektive Tatbestand zu verneinen. Denn dieser erfordert nÃ¤mlich Vorsatz, zumindest bedingten Vorsatz ( vgl Thomas Fischer, Kommentar zum StGB, Rn. 92 zu Â§ 203).
Betroffene Personen, die der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstÃ¶Ãt, haben die MÃ¶glichkeit, Rechtsbehelfe nach Art. 77 ff. DSGVO in Verbindung mit Â§Â§ 81 ff SGB X einzulegen. Im Einzelnen handelt es sich um das Recht auf Beschwerde bei einer AufsichtsbehÃ¶rde (Art. 77 Abs. 1 DSGVO), das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer AufsichtsbehÃ¶rde (Art. 78 Abs. 1 DSGVO). FÃ¼r den gerichtlichen Rechtsbehelf ist der Rechtsweg zu den Gerichten der Sozialgerichtsbarkeit nach Â§ 81a Abs. 1 bzw. Â§ 81b SGB X erÃ¶ffnet.

Rechtsgrundlage fÃ¼r einen Schadenersatzanspruch wegen eines VerstoÃes gegen diese Verordnung, die zu einem materiellen oder immateriellen Schaden gefÃ¼hrt hat, ist Art. 82 Abs. 1 DSGVO. Der Schadensersatzanspruch richtet sich gegen den/die Verantwortlichen oder gegen den/die Auftragsverarbeiter (Art. 82 Abs. 1, 2 DSGVO). Wenn der Vertragszahnarzt als Verantwortlicher in Anspruch genommen wird, ist er seinerseits mit Einwendungen nicht abgeschnitten. So kann er sich nach Art. 82 Abs. 3 DSGVO exkulpieren, wenn er nachweist, dass er in keinerlei Hinsicht fÃ¼r den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Insofern kann er weder fÃ¼r einen Schaden haftbar gemacht werden, der nicht in seiner SphÃ¤re entstanden ist, noch kann er fÃ¼r einen Schaden haftbar gemacht werden, der zwar in seiner SphÃ¤re entstanden ist, den er aber bei bestimmungsgemÃ¤Ãem Anschluss an die TU, bestimmungsgemÃ¤Ãer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen DatenschutzmaÃnahmen (zum Beispiel Absicherung der Hard-und Software) nicht zu vertreten hat.
Aus den genannten GrÃ¼nden sind die angefochtenen Bescheide (HonorarkÃ¼rzung) als rechtmÃ¤Ãig anzusehen und ist die Klage abzuweisen. Ein VerstoÃ der Vorschriften der Â§Â§ 291ff. SGB V gegen hÃ¶herrangiges Recht, insbesondere die DSGVO und das Grundgesetz ist nicht ersichtlich.
Die Kostenentscheidung beruht auf Â§ 197a SGG in Verbindung mit Â§ 154 VwGO.

Â

Â

Erstellt am: 27.02.2023

Zuletzt verändert am: 23.12.2024