S 38 KA 190/20

Land
Freistaat Bayern
Sozialgericht
SG München (FSB)
Sachgebiet
Vertragsarztangelegenheiten
1. Instanz
SG München (FSB)
Aktenzeichen
S 38 KA 190/20
Datum
26.01.2023
2. Instanz
-
Aktenzeichen
-
Datum
-
3. Instanz
-
Aktenzeichen
-
Datum
-
Kategorie
Urteil
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).

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.

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.

I. Dem Antrag, Beweis durch Einholung eines Sachverständigengutachtens entsprechend der schriftlichen Vorlage des Prozessbevollmächtigten zu erheben, wird nicht stattgegeben.

II. Die Klage wird abgewiesen.

III. Der Kläger trägt die Kosten des Verfahrens.

T a t b e s t a n d :

Der Kläger, der als Vertragsarzt (Facharzt für Augenheilkunde) zugelassen ist, wendet sich gegen die mit dem angefochtenen Ausgangsbescheid in der Fassung des Widerspruchsbescheids vorgenommenen Honorarkürzungen in den Quartalen 1/19 - 4/19 in Höhe von 1 % (= 2.399,11€) wegen Nichtteilnahme an der Telematikinfrastruktur (TI).

Zur Begründung der Kürzung wurde auf die Rechtsgrundlage des § 291 Abs. 2b Satz 14 a.F. (Satz 9 n.F; Anmerkung: genannte §§ 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. für Vertragsärzte und Vertragszahnärzte verpflichtend. Ein Verstoß gegen höherrangiges Recht liege nicht vor. Die Beklagte setzte sich insbesondere mit den Argumenten des Klägers, die dieser im Rahmen des Vorverfahrens vortrug bzw. vortragen ließ, auseinander.

So wurde betont, eine Verletzung von Privatgeheimnissen § 203 StGB sei nicht ersichtlich, wenn die Telematikinfrastruktur eingeführt und bestimmungsgemäß betrieben werde; etwas anders stelle sich die Situation dar, wenn es aufgrund fehlender Datenschutzmaßnahmen (fehlende Absicherung der Hard-oder Software mittels Firewall, Zugriffsbeschränkung oder ähnlichem) zu einem Datenmissbrauch kommen sollte. Eine Verletzung erfordere immer ein Verschulden oder einen Vorsatz. Ferner sei ein Verstoß 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 Gefährdung 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 schütze 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 verschlüssle. Gleichzeitig schütze der Konnektor auch die TI vor beispielsweise Schadstoffsoftware in der Arztpraxis. Es sei zwar einzuräumen, dass die in § 291b Abs. 2 S. 2 SGB V vorgesehenen Stand-Alone-Lösungen (= Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer) zwar nur bis 19.12.2019 bestanden hätten. Diese Lösungen seien aber nunmehr nicht mehr vorgesehen, da sie mit Einführung des Anspruchs auf die Notfalldaten nicht mehr einsetzbar seien.

Durch das Zertifizierungsverfahren und die dafür notwendige Sicherheitsüberprüfung für die Herstellung und den Betrieb von Produkten der TI und Diensten gewährleiste die G., die die Architektur der TI maßgeblich definiere und entwickle, dass die sensiblen Gesundheitsdaten vor unbefugtem Zugriff sicher seien. Bei der 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, führe das nicht zur Rechtswidrigkeit und Unvereinbarkeit mit höherrangigem Recht. Im Übrigen hafteten die Hersteller nach Zivilrecht. Außerdem stünden diese zivilrechtlich auch in einer Gewährleistungspflicht.

Soweit der Kläger auf Klagen beim Bundeskartellamt wegen unerlaubter Preisabsprachen der Konnektor- und Kartenlesegerätehersteller hinweise, ergebe sich auch hieraus keine Rechtswidrigkeit. Insgesamt vier Hersteller böten zertifizierte Konnektoren an. Für den bundesweiten Betrieb der zentralen TI sei die Firma A. zuständig.

Auch die Finanzierung der Installation der Konnektoren und der laufenden Kosten sei rechtlich nicht zu beanstanden. Die TI-Kostenübernahme sei in § 291a Abs. 7 S. 5 SGB V geregelt. KBV und GKV-Spitzenverband hätten sich in einem Schiedsverfahren auf die Finanzierung der TI in Form von Pauschalen verständigt (Anlage 32 BMV-Ä). In dem Zusammenhang habe das SG München (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 rechtmäßig. Die Kürzung sei somit zu Recht erfolgt.

Gegen den Ausgangsbescheid in der Fassung des Widerspruchsbescheides ließ der Kläger durch seinen Prozessbevollmächtigten Klage zum Sozialgericht München einlegen. Zur Begründung führte dieser aus, es habe bis zum 19.12.2019 sog. Stand-Alone-Lösungen gegeben (§ 291 Abs. 2 SGB V; = Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer). Eine dem Schutz der Patientendaten angemessene Datensicherheit wäre nur durch eine Stand-Alone-Lösung erreichbar. Die Abschaffung sei deshalb erfolgt, weil angeblich die Stand-Alone-Lösungen nicht vereinbar seien mit der Einführung 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 bestünden massive Bedenken. So habe der Computer Chaos Club (CCC) bereits Mängel beim Vergabeprozess der Berechtigungskarten aufgedeckt. Denn es finde die Prüfung der Identität der Antragsteller nicht zuverlässig statt. Jedermann habe bis Ende 2019 eine Berechtigungskarte bestellen und diese auch an eine abweichende Anschrift schicken lassen können. 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 Stromzähler oder Tachos. Zudem werde gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen. Zwar handle es sich um keinen gezielten Eingriff in das Grundrecht, wohl aber um massive faktische Beeinträchtigungen. Der Einzelne müsse stets die Kontrolle über 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 grundsätzlichen Anforderungen an Sicherheitsmaßnahmen. Auch würden konkrete Regeln zur Gefahrenvorsorge unterlassen. Dies sei notwendig, da es hier um besonders sensible Daten im Gesundheitsbereich gehe. Außerdem seien solche Eingriffe nur dann zulässig, wenn der Gesetzgeber geeignete Sicherheitsmaßnahmen angeordnet habe. Es sei auch zu besorgen, dass die ärztliche Schweigepflicht (§ 203 StGB) tangiert werde. Unvereinbar sei auch die Beteiligung der Privaten Krankenversicherer und des Wirtschaftlichen Spitzenverbandes der Apotheker mit den Anforderungen des Bundesverfassungsgerichts. Insgesamt verstießen die Regelungen im SGB V (§§ 291 ff. SGB V) gegen die Datenschutzgrundverordnung (DSGVO), insbesondere gegen Art. 32 DSGVO, aber auch gegen Art. 26 DSGVO. Bisher sei der Praxisinhaber für die Verarbeitung von Daten alleinverantwortlich. Andere in die TI Involvierte seien dagegen nicht als (Mit-)Verantwortliche aufgeführt.

Schließlich werde auch gegen die Berufsfreiheit aus Art. 12 GG verstoßen. Der Prozessbevollmächtigte des Klägers beantragte, ein Sachverständigengutachten einzuholen.

In ihrer Replik räumte 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 Klägerseite geäußerte Befürchtung, wonach von anderen Praxen eine Gefährdung ausgehen könne, treffe nicht zu. In dem Zusammenhang werde auf die Ausführungen der G. im White Paper Datenschutz und Informationssicherheit (Stand September 2020) hingewiesen. Danach würden die IT-Systeme der Heilberufe vor Angriffen aus dem Internet, aber auch vor unberechtigten Zugriffen aus der zentralen TI-Plattform geschützt. Das Problem sei nicht der Konnektor, sondern "der richtige Umgang mit den Gegebenheiten vor Ort und das enge Zusammenspiel aller an einer Praxis-IT beteiligten Dienstleister". Zum Argument des Prozessbevollmächtigten des Klägers, die Regelungen zum Sicherheitsniveau und zu den geeigneten Sicherheitsmaßnahmen einschließlich konkreter Regelungen zur Gefahrenvorsorge müssten durch den Gesetzgeber, nicht aber durch die G. erfolgen, vertrat die Beklagte die Auffassung, hierbei müsse die rasante Entwicklung auf dem Sektor der Informationstechnologie berücksichtigt werden. Es sei fraglich, ob der Gesetzgeber dem Rechnung tragen könne. Eventuell seien die Regelungen dann bei Inkrafttreten des Gesetzes bereits überholt. Im Übrigen habe der Gesetzgeber mit dem PDSG die Regelungen in den §§ 291 ff. SGB V überarbeitet. So seien auch die Aufgaben der G. in § 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 der G. zum Thema Haftung und Datenschutz im Juli 2019 hingewiesen. Voraussetzung für eine Haftung sei ein Verschulden, das jedenfalls bei einem sachgemäßen Anschluss zu verneinen sei. Haftungsfragen seien als solche zu klären und kein Grund, eine Teilnahme an der TI von vornherein grundsätzlich abzulehnen. Ferner lägen keinerlei Grundrechtsverstöße vor, auch nicht gegen das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht aus Art. 12 Grundgesetz. Denn Eingriffe seien im überwiegenden Allgemeininteresse unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz oder aufgrund eines Gesetzes hinzunehmen und gerechtfertigt. Die Eingriffe seien durch vernünftige Belange des Gemeinwohls legitimiert. Im Übrigen werde das Grundrecht auf informationelle Selbstbestimmung in seinem Schutz der personenbezogenen Daten durch den Versichertenstammdatenabgleich nur geringfügig beschränkt, 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 könne sich der Kläger "im subjektiv geprägten Sozialgerichtsverfahren" grundsätzlich 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 mündlichen Verhandlung am 26.01.2023 wurde die Sach-und Rechtslage mit den Beteiligten besprochen. Das Gericht stellte zur weiteren Sachaufklärung zusätzliche Fragen an die anwesenden Beteiligten. Danach, so die Beigeladene (G.), sei es notwendig gewesen, die Stand-Alone-Lösung abzuschaffen. Dies sei für die Durchführung des Notfalldatenmanagements notwendig gewesen. Im Übrigen 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 außer den vom CCC gemeldeten Fällen keine weiteren konkreten Fälle gegeben. Es habe sich um kein echtes "Szenario" gehandelt, sondern nur um Demonstrationsfälle. Zur Frage nach dem laut dem Vorbringen der Klägerseite niedrigen Sicherheitsprofil (EAL3+) wird ausgeführt, aus dieser Bezeichnung sei nicht auf das tatsächliche Sicherheitsniveau zu schließen. Das eigentliche Sicherheitsniveau sei wesentlich größer. Das BSI habe auf insgesamt 155 Seiten das Schutzprofil vorgegeben. So gebe es 27 Bausteine; davon seien 25 sowohl für Konnektoren, als auch für smart meter gateway bestimmt. Lediglich bei zwei Prüfbausteinen, die sich auch nicht auf das Produkt selbst, sondern auf den Entwicklungsprozess beim Hersteller beziehen würden, sei der smart meter gateway höher eingestuft, nämlich bei insgesamt sieben Stufen, davon die siebte Stufe als die höchste Stufe, mit Stufe 4 statt mit Stufe 3. Auf Frage des Prozessbevollmächtigten des Klägers wurde durch die Beigeladene (G.) ausgeführt, 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 fünf Jahren für notwendig erachtet worden, da eine Zertifikatsverlängerung nicht stattfand. Denn einer der Hersteller von Konnektoren habe die für die Umsetzung notwendige Software nicht bereitgestellt. Zum sog. Patientenstammdatenabgleich wurde ausgeführt, es seien zu keiner Zeit Patientenstammdaten an die Krankenkassen übertragen worden. Der Konnektor frage verschlüsselt (Kartennummer) lediglich bei der Krankenkasse an, ob es ein Update gebe. Habe sich eine Änderung, beispielsweise eine Adressänderung ergeben und sei es damit zu einem Update gekommen, werde ebenfalls verschlüsselt Rückmeldung von der Krankenkasse gegeben und die Anpassung auf die Patientenkarte geschrieben.

In der mündlichen Verhandlung am 26.01.2023 übergab der Prozessbevollmächtigte des Klägers dem Gericht einen schriftlich formulierten Beweisantrag, der den Vertretern der Beklagten und den Vertretern der Beigeladenen in Kopie ausgehändigt wurde.

Der Kläger selbst trug vor, er halte seit Jahren eine Vielzahl von digitalen Plätzen in seiner Praxis vor. Daten von zig-1000 Patienten seien gespeichert. Es handle sich um äußerst sensible Daten. Da seines Erachtens der Datenschutz im Zusammenhang mit der Einführung der TI unsicher sei, bestehe die Gefahr, dass er der ärztlichen Schweigepflicht nicht genügen könne und sich letztendlich strafrechtlich verantworten müsse (§ 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 rechtskräftig 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 München (SG München, Urteile vom 09.11.2022, u.a. Az S 38 KA 5155/21; bislang nur
im Zahnarzt-Bereich). Die Klagen wurden abwiesen.

Der Prozessbevollmächtigte des Klägers stellte folgende Anträge:

Es wird beantragt, Beweis durch Sachverständigengutachten entsprechend dem in der mündlichen Verhandlung übergebenen schriftlichen Beweisantrag zu erheben (- Der Vergabeprozess für die Berechtigungskarten im Jahr 2019 war aus den auf Seite 5f. der Klagebegründung genannten Gründen 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. - 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. - Das Sicherheitsniveau EAL3+ für den Konnektor ist nicht ausreichend, weil es kein hohes Sicherheitsniveau beschreibt. Vielmehr ist EAL4+ erforderlich).

Hilfsweise stellte der Prozessbevollmächtigte des Klägers 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 mündlichen Verhandlung
war die Beklagtenakte. Im Übrigen wird auf den sonstigen Akteninhalt, insbesondere die Schriftsätze 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 ü n d e:

Das Gericht hat dem Antrag des Prozessbevollmächtigten des Klägers, Beweis durch Sachverständigengutachten entsprechend dem in der mündlichen Verhandlung übergebenen schriftlichen Beweisantrag zu erheben, nicht stattgegeben. Entsprechend hat es unter I. des Urteils tenoriert. Dies wäre an sich nicht notwendig gewesen, da es ausreicht, in den Entscheidungsgründen darauf einzugehen (Meyer-Ladewig/Keller Leitherer/ Schmidt, Kommentar zum SGG, Rn. 12c zu § 103), ist aber unschädlich. Nach § 103 Satz 2 SGG ist das Gericht an das Vorbringen und die Beweisanträge der Beteiligten nicht gebunden. Hintergrund hierfür ist, dass in sozialgerichtlichen Verfahren nach § 103 Satz 1 SGG eine sog. Amtsermittlungspflicht besteht. Der Sachverhalt ist umfassend, losgelöst von dem Vorbringen und Beweisanträgen der Beteiligten zu ermitteln. Beweisanträge sind daher grundsätzlich als Anregungen zu verstehen (Meyer-Ladewig/Keller Leitherer/ Schmidt, Kommentar zum SGG, Rn. 12c zu § 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 erübrigt und dazu führt, den Rechtsstreit als entscheidungsreif anzusehen.

Die zum Sozialgericht München eingelegte Klage ist zulässig, erweist sich jedoch als unbegründet. Der angefochtene Ausgangsbescheid in der Fassung des Widerspruchsbescheides ist rechtmäßig.
Rechtsgrundlage für die vorgenommene Kürzung (Honorarabzug) ist § 291 Abs. 2b S. 14 SGB V. Danach ist die Vergütung vertragsärztlicher Leistungen pauschal um ein Prozent zu kürzen, wenn die an der vertrags(-zahn)ärztlichen Versorgung teilnehmenden Ärzte die Prüfung nach § 291 Abs. 2b S. 2 SGB V nicht durchführen. Nach § 291 Abs. 2c S. 2 SGB V ist die Vergütung vertrags(-zahn)ärztlicher Leistungen pauschal um ein Prozent solange zu kürzen, bis der Nachweis, dass die Ärzte über die für den Zugriff auf die elektronische Patientenakte erforderlichen Komponenten und Dienste verfügen, nicht erbracht wird. Konkret hat der Kläger weder den Nachweis geführt, noch hat er den online-Datenabgleich vorgenommen, sodass die seit dem Pflegepersonalstärkungsgesetz (PpSG) gewährte Fristverlängerung zur Anbindung an die Telematikinfrastruktur und Durchführung des Versichertenstammdatenmanagements bis zum 30.06.2019 (§ 291 Abs. 2b S. 14 und 15 in der Fassung vom 11.12.2018) nicht gilt.
Die Honorarkürzung ist nur dann rechtmäßig, wenn die Verpflichtung zur Teilnahme an der Telematikinfrastruktur ihrerseits rechtmäßig ist. Dies setzt insbesondere voraus, dass die Regelungen über die Telematikinfrastruktur mit höherrangigem 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 über die Rechtmäßigkeit der Honorarkürzung wegen Nichtteilnahme von Vertragsärzten an der Telematikinfrastruktur zu entscheiden. Diese Entscheidung betraf das Quartal 1/2019. Das Gericht kam zu dem Ergebnis, §§ 291 Absatz 2b S. 3, S. 14 SGB V a.F. seien nicht wegen Verstoßes gegen höherrangiges Recht, insbesondere nicht wegen eines Verstoßes gegen die DSGVO nichtig.
Im Einzelnen setzte sich das SG Stuttgart mit der Vereinbarkeit der Regelungen der §§ 291 ff. SGB V a.F. mit Art. 6 Abs. 1 DSGVO (Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt), Art. 6 Abs. 3 S. 4 DSGVO (Verhältnismäßigkeitsgrundsatz), 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 (Datenschutzfolgenabschätzung) und Art. 12 Grundgesetz (GG) sehr ausführlich auseinander. Das Urteil ist nicht rechtskräftig (Berufung zum LSG Baden-Württemberg).
Zudem gelangte das Sozialgericht Mainz (SG Mainz, Urteil vom 27.07.2022, Az S 3 KA 84/20) zu dem Ergebnis, die erfolgte Honorarkürzung auf der Grundlage von § 291 Abs. 2b S 3, S. 14 SGB V a.F. sei rechtmäßig. Vom Gericht geprüft wurde insbesondere die Vereinbarkeit der Vorschriften des SGB V (§§ 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 führte aus, die Vorschriften würden nicht gegen die Vorgaben der DSGVO verstoßen. Insbesondere handle es sich um einen überschaubaren Datenverarbeitungsprozess. Außerdem sei eine kontinuierliche Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben durch die Gesellschaft und die Anbieter von Diensten und Anwendungen im Rahmen der TI hinreichend gewährleistet.
Ende 2022 war das SG München (SG München, Urteile vom 09.11.2022, u.a. Az S 38 KA 5155/21) mit Honorarkürzungen im Zahnarzt-Bereich wegen Nichtteilnahme an der TI (Klagen mehrerer Vertragszahnärzte) befasst. Auch hier wurden die Klagen abgewiesen.

Des Weiteren prüfte das Bundessozialgericht (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R), wenn auch in anderem Zusammenhang, die Rechtmäßigkeit und Vereinbarkeit der §§ 291 ff. SGB V mit der DSGVO. Gegenstand des dortigen Verfahrens war, ob für die beklagte Krankenkasse eine Verpflichtung bestand, einer Versicherten einen Weg zu eröffnen, ihre Berechtigung zur Inanspruchnahme von vertragsärztlichen Leistungen nachweisen zu können, ohne dabei die E-Gesundheitskarte verwenden und einen online erfolgenden Abgleich von Versichertenstammdaten dulden zu müssen. Das Bundessozialgericht hat hierzu ausgeführt, die aktuellen gesetzlichen Vorgaben zur E-Gesundheitskarte und ihre Einbeziehung in die TI stünden 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 Stabilität der gesetzlichen Krankenversicherung zugutekomme. Das Bundessozialgericht betonte auch, es gebe keine absolute Datensicherheit. Im Übrigen sprach das Bundessozialgericht (aaO) von einem hinreichend normdichten und klaren Regelungsgefüge, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler Maßnahmen der

Datensicherheit diene. Der Gesetzgeber sei auch später seiner Beobachtungs-und Nachbesserungspflicht nachgekommen.
Das Sozialgericht München nimmt auf die o.g. Entscheidungen Bezug. Zudem ist im streitgegenständlichen Verfahren wie folgt auszuführen: Was die genannte Entscheidung des Bundessozialgerichts betrifft (BSG, aaO), ist diese auf die vorliegende Rechtsstreitigkeit nicht unmittelbar übertragbar. Denn Gegenstand des hier anhängigen 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 maßgeblichen Regelungen im SGB V (§§ 291 ff SGB V) umfassend auseinandersetzt und die Regelungen für datenschutzrechtlich unbedenklich und mit der DSGVO vereinbar angesehen. Die rechtlichen Erwägungen können folglich mittelbar und ohne weiteres auch auf das streitgegenständliche Verfahren aus dem Bereich des Vertragsarztrechtes übertragen werden.
Die Teilnahme der Vertragsärzte an der Telematikinfrastruktur steht im Zusammenhang mit der Einführung der sog. elektronischen Gesundheitskarte (E-Gesundheitskarte), die den Versicherten von der Krankenkasse ausgestellt wird (§ 291a Abs. 1 SGB V). Nach § 291 Abs. 2 SGB V enthält sie verschiedene Angaben, nämlich sog. Patientenstammdaten. § 291 Abs. 2, Abs. 3 SGB V regelt die Zwecke, für die die E-Gesundheitskarte geeignet sein muss. In dem strittigen Zeitraum (Jahr 2019) stellen die an der vertragsärztlichen Versorgung teilnehmenden Ärzte/Zahnärzte bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten im Quartal die Leistungspflicht der Krankenkasse durch Nutzung der Dienste fest. Dazu ermöglichen 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 Prüfungspflicht gilt ab dem Zeitpunkt, ab dem die Dienste nach § 291 Abs. 1 SGB V sowie die Anbindung an die Telematikinfrastruktur zur Verfügung stehen (§ 291 Abs. 2b S. 4 SGB V). Nach § 291 Abs. 2b S. 6 SGB V ist die Durchführung der Prüfung auf der E-Gesundheitskarte zu speichern. Gegenüber den zuständigen Kassen(-zahn)ärztlichen Vereinigungen besteht eine Nachweispflicht durch die an der vertrags(-zahn)ärztlichen Versorgung teilnehmenden Leistungserbringer (§ 291 Abs. 2c S. 1 SGB V). Nach der Erläuterung der Beigeladenen findet ein sog. Patientenstammdatenabgleich jedenfalls in der Weise nicht statt, dass Stammdaten an die Krankenkassen übertragen werden. Vielmehr wird nach Einlesen der Versichertenkarte in der Arztpraxis über den Konnektor verschlüsselt (Kartennummer) bei der Krankenkasse angefragt, ob es ein Update gibt. Liegt ein solches vor, erfolgt eine verschlüsselte Rückmeldung von der Krankenkasse. Diese Änderung wird dann auf die Patientenkarte geschrieben.

Komponenten und Dienste der Telematikinfrastruktur werden von der G. zugelassen (§ 291 b Abs. 1 a S.1 SGB V). Die G. prüft dabei die Funktionsfähigkeit und Interoperabilität auf der Grundlage der von ihr veröffentlichen Prüfkriterien (§ 291 b Abs. 1 a S.4 SGB V). Vorgesehen ist auch eine sogenannte Sicherheitszertifizierung nach § 291b Abs. 1a S. 5 SGB V. Kommt es zu Störungen, die zu einer beträchtlichen Auswirkung auf die Sicherheit und Funktionsfähigkeit der Telematikinfrastruktur führen können oder bereits geführt haben, hat die Gesellschaft für Telematik dies dem Bundesamt für Sicherheit in der Informationstechnik zu melden (§ 291b Abs. 6 S. 4 SGB V). Bei Sicherheitsmängeln kann das Bundesamt für Sicherheit in der Informationstechnik der Gesellschaft für Telematik verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel erteilen (§ 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 § 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 ausgeführte 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 für personenbezogene Daten findet sich in Art. 4 Ziff. 1 DSGVO. Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen... Damit ist der Anwendungsbereich der DSGVO (Art. 1 DSGVO) eröffnet.
Die Regelungen des §§ 291 ff. SGB V sind mit den allgemeinen Grundsätzen der DSGVO (Art. 4, 5, 6) vereinbar. Insbesondere dient der Datenabgleich der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (Art. 6 Abs. 1 DSGVO). Ebenso wird der Grundsatz der Verhältnismäßigkeit in Art. 6 Abs. 3 S. 4 DSGVO eingehalten. Danach muss auch das Recht des Mitgliedstaats ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Die Prüfung des Verhältnismäßigkeitsgrundsatzes erfordert die Beurteilung der Eignung und Erforderlichkeit des gewählten Mittels zur Erreichung des erstrebten Zwecks sowie eine vorzunehmende Einschätzung 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 § 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 Gewährleistung der finanziellen Stabilität der GKV. Es ist nicht ersichtlich, dass es andere, gleich geeignete, weniger belastende Möglichkeiten gibt, um die legitimen Ziele zu erreichen (vgl BSG, Beschluss vom 20.01.2021, B 1 KR 7/20 ER). Vielmehr drängt sich auf, die Möglichkeiten der elektronischen Datenverarbeitung auch im gesundheitlichen Bereich, allerdings bei gleichzeitiger besonderer Wahrung des Datenschutzes zu nutzen, wie sie auch in anderen Bereichen seit längerer Zeit bereits Verwendung finden.
Zu den wichtigsten zu beachtenden Regelungen in der DSGVO gehört die Sicherheit der Daten. Damit die Ziele der DSGVO (Art. 1 Abs. 2 DSGVO), nämlich der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Rechte auf Schutz persönlicher personenbezogener Daten erreicht werden, müssen nach Art. 5 Abs. 1 Buchst. f DSGVO "die 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")".
Der Verarbeitungsprozess in den Quartalen 1/19-4/19 besteht darin, dass der an der vertragsärztlichen 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 § 291 Abs. 2b S. 2 SGB V prüft. 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 (§ 291 Abs. 2b S. 3 SGB V). Zu den Patientenstammdaten zählen die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die Kassenärztliche 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, für die Personengruppe nach § 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 Gültigkeit elektronischen Gesundheitskarte das Datum des Fristablaufs (Nr 10). Das Sozialgericht München, wohl aber auch die bisher befassten Sozialgerichte sind bisher von einem Abgleich aller sog. Patientenstammdaten

im Wege der Übermittlung von der jeweiligen Praxis an die Krankenkassen und Rückleitung ausgegangen. Wie dies im Einzelnen geschieht, wurde, soweit ersichtlich, in den vorangegangenen Entscheidungen nicht thematisiert. Nunmehr, nämlich im Rahmen der mündlichen Verhandlung am 26.01.2023 vor dem Sozialgericht München wurden Einzelheiten des sog. Online-Datenabgleich bekannt. Danach - so die Vertreter der G. - wird bei der Krankenkasse verschlüsselt angefragt, ob es ein Update gibt. Ist dies der Fall, beispielsweise, weil sich beim Patienten eine Adressänderung ergeben hat und es damit zu einem Update gekommen ist, wird ebenfalls verschlüsselt Rückmeldung 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 verschlüsselt angefragt, ob es ein update gibt, geschweige denn werden Daten über den einzelnen Gesundheitsstatus des Versicherten verarbeitet. Auch werden vom Vertrags(-zahn)arzt selbst Daten nicht erhoben, nicht erfasst, nicht angepasst oder verändert (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 "angemessene" Datensicherheit gefordert. Bei dem Begriff "angemessen" handelt es sich um einen unbestimmten Rechtsbegriff, der der Auslegung zugänglich ist. In dem Zusammenhang bekräftigt das Gericht seine Auffassung, wonach umso höhere Anforderungen an die Datensicherheit zu stellen sind, um das Risiko vor unbefugtem Zugriff Dritter möglichst gering zu halten, je umfangreicher und personenbezogener Daten sind, die verarbeitet werden. Die Anforderungen an die Datensicherheit sind somit unterschiedlich und abhängig von der Art, dem Umfang der Daten und der konkreten Datenverarbeitung. Ganz allgemein gilt, eine absolute Datensicherheit ist nicht zu fordern und wäre auch mit einem noch so großen technischen und organisatorischen Aufwand nicht darstellbar (vgl BSG, Urteil vom 20.01.2021, B 1 KR 7/20 R).

In Umsetzung dieser grundsätzlichen Erwägungen auf das streitgegenständliche Verfahren, ist zunächst 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 tatsächlich 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 der G. im Zusammenhang mit der Telematikinfrastruktur eine wesentliche Rolle zugedacht hat, kommt es darauf an, ob diese Institution den Anforderungen an eine "angemessene" Datensicherheit formell und materiell gerecht wird. Auch stellt sich die Frage, ob es der G. qua Gesetz überlassen werden kann, die wesentlichen, mit der Einführung der Telematikinfrastruktur zusammenhängenden Maßnahmen, darunter insbesondere Sicherheitsmaßnahmen zur Gewährleistung des Datenschutzes zu treffen. Als Aufgaben der G. sind die Erstellung der funktionalen und technischen Vorgaben einschließlich eines Sicherheitskonzepts (§ 291b Abs. 1 Ziff 1 SGB V), die Festlegung des Inhalts und der Struktur der Datensätze für deren Bereitstellung und Nutzung (§ 291b Abs. 1 Ziff 2 SGB V), die Erstellung und Überwachung der Vorgaben für den sicheren Betrieb der Telematikinfrastruktur (§ 291b Abs. 1 Ziff 3 SGB V), die Sicherstellung der notwendigen Test-und Zertifizierungsmaßnahmen (§ 291b Abs. 1 Ziff 4 SGB V) und die Festlegung der Verfahren einschließlich der dafür erforderlichen Authentisierungsverfahren zur Verwaltung der in § 291a Abs. 4 und 5a geregelten Zugriffsberechtigungen und der Steuerung der Zugriffe auf Daten nach § 291 Abs. 3 (§ 291b Abs. 1 Ziff 5 SGB V) genannt. Die G. wird in der Rechtsform einer GmbH geführt, bestehend aus mehreren Gesellschaftern, konkret die Bundesrepublik Deutschland und die in § 291a Abs. 7 SGB V genannten Spitzenorganisationen (Spitzenverband Bund der Krankenkassen, die Kassenärztliche Bundesvereinigung, die Kassenzahnärztliche Bundesvereinigung, die Bundesärztekammer, die Bundeszahnärztekammer, 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 übrigen Spitzenorganisationen (§ 291b Abs. 2 Ziff. 1 SGB V). Mit Gesetz vom 14.10.2020 erfolgte eine Änderung des SGB V u.a. durch Neuformulierung bestehender Vorschriften und durch Einfügung der Vorschriften der §§ 306 ff SGB V.
Der Kläger äußert Vorbehalte dahingehend, die Beteiligung der Privaten Krankenversicherer und des wirtschaftlichen Spitzenverbandes der Apotheker sei mit den Anforderungen des Bundesverfassungsgerichts unvereinbar. In dem Zusammenhang ist zunächst zu bemerken, dass in § 291a Abs. 7 SGB V eine Beteiligung der Privaten Krankenversicherer nicht vorgesehen war. Erst mit Gesetzesänderung zum 14.10.2020 wurde eine Beteiligung der Privaten Krankenversicherer fakultativ durch Beschluss der Gesellschafter der G. (§ 310 Abs. 3 SGB V) möglich; 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 überwiegend bei der Bundesrepublik Deutschland, vertreten durch das BMG (= Mehrheitsgesellschafterin mit 51 %) und den Körperschaften des öffentlichen Rechts liegen. Denn die Einbindung des Spitzenfachverbandes der Apotheker in die TI erscheint im Zusammenhang mit der Einführung des E-Rezeptes unerlässlich. 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 Erfüllung der Aufgaben der G. hat der Gesetzgeber eine Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und mit der/dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verbindlich vorgegeben. So ist, wenn bei den Festlegungen und Maßnahmen nach § 291b Abs. 1 SGB V Fragen der Datensicherheit berührt sind, ein Einvernehmen mit dem BSI herzustellen. Ferner ist in § 291b Abs. 1e S. 1 SGB V geregelt, dass die Gesellschaft für Telematik sichere Verfahren zur Übermittlung medizinischer Dokumente in Abstimmung mit dem BSI festlegt. Für die Zulassung von Komponenten und Diensten der Telematikinfrastruktur entwickelt das BSI geeignete Prüfvorschriften und veröffentlicht diese im Bundesanzeiger. Das Nähere zum Zulassungsverfahren und zu den Prüfkriterien wird von der G. in Abstimmung mit dem BSI beschlossen (§ 291 b Abs. 1a S. 6 und 7 SGB V). Nach § 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 berührt sind. Auch, soweit von Komponenten und Diensten eine Gefahr für die Funktionsfähigkeit oder Sicherheit der Telematikinfrastruktur ausgeht, ist die G. in Abstimmung mit dem BSI befugt, die erforderlichen technischen und organisatorischen Maßnahmen zur Abwehr dieser Gefahr zu treffen. Für die zugelassenen Dienste und Betreiber besteht die Pflicht, erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und Vertraulichkeit dieser Dienste unverzüglich der G. zu melden (§ 291b. Abs. 6 S. 2 SGB V). Die G. ist dann ihrerseits verpflichtet, diese Störungen unverzüglich dem BSI zu melden (§ 291b. Abs. 6 S. 4 SGB V). Auf Verlangen des BSI hat die G. die in § 291b Abs. 8 S. 1 SGB V genannten Dokumente vorzulegen. Wenn sich daraus Sicherheitsmängel ergeben sollten, kann das BSI der G. verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel erteilen (§ 291b Abs. 8 S. 2 SGB V).
Des Weiteren sieht das Gesetz in § 291b Abs. 2a SGB V die Einrichtung eines Beirats durch die Gesellschaft für Telematik vor, der diese in fachlichen Belangen berät. Der Beirat besteht zwingend aus insgesamt 17 Vertretern, nämlich aus vier Vertretern der Länder, drei Vertretern der für die Wahrnehmung der Interessen der Patienten und der Selbsthilfe chronisch kranker und behinderter Menschen maßgeblichen Organisationen, drei Vertretern der Wissenschaft, einen durch das Bundesministerium für Gesundheit im Einvernehmen mit

dem Bundesministerium für Bildung und Forschung zu benennenden Vertreter aus dem Bereich der Hochschulmedizin, drei Vertretern der für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbände aus dem Bereich der Informationstechnologie im Gesundheitswesen, einem Vertreter der für die Wahrnehmung der Interessen der hausarztzentrierten Versorgung teilnehmenden Vertragsärzte maßgeblichen Spitzenorganisationen sowie der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der oder dem Beauftragten der Bundesregierung für die Belange der Patientinnen und Patienten.
In § 291c SGB V ist ferner die verbindliche Einrichtung einer Schlichtungsstelle bei der Gesellschaft für Telematik vorgesehen, deren Entscheidungen für alle Gesellschafter, für die Leistungserbringer und Krankenkassen sowie für ihre Verbände nach diesem Buch verbindlich sind.
Die Beschlüsse der Gesellschaft für Telematik zu den Regelungen, dem Aufbau und dem Betrieb der Telematikinfrastruktur sind für die Leistungserbringer und die Krankenkassen sowie ihre Verbände nach diesem Buch verbindlich (§ 291b Abs. 4 S. 1 SGB V). Außerdem ist die G. Betreibern von Diensten gegenüber weisungsbefugt (§ 291b Abs. 8 S. 6 SGB V).
Somit verfügt die G. einerseits über umfangreiche eigene Kompetenzen, so vor allem eine eigene Kompetenz, Festlegungen und Maßnahmen der Datensicherheit (§§ 291b Abs. 1, 291b Abs. 1e SGB V), darunter auch Maßnahmen der Gefahrenabwehr zu treffen (§ 291b Abs. 6 S. 1 SGB V), Entscheidungen über die Zulassung von Diensten und Betreibern zu treffen (§ 291b Abs. 1a SGB V), auch gegebenenfalls den Zugang zur Telematikinfrastruktur zu sperren oder nur unter Auflagen zu gestatten (§ 291b Abs. 6 S. 6 SGB V).
Andererseits ist den Regelungen, insbesondere § 291b SGB V immanent, dass bei Maßnahmen und Entscheidungen, die die Datensicherheit betreffen, ein Einvernehmen bzw. eine Abstimmung mit dem BSI und/oder der/dem BfDI erforderlich ist. Für die G. besteht auch gegenüber dem BSI eine Meldepflicht bei erheblichen Störungen (§ 291b Abs. 4 S. 2 SGB V). Das BSI ist ebenfalls gegenüber der G. zu Weisungen befugt. Hinzu kommt auch die Einrichtung des Beirates nach § 291b Abs. 2a SGB V und einer Schlichtungsstelle nach § 291c SGB V, beides Einrichtungen, die ihrerseits ein zusätzliches "Mehr" an Datensicherheit garantieren. Auch wenn ein solches Procedere auf den ersten Blick raschen Entscheidungsprozessen zuwiderläuft, trägt dieses nicht unmaßgeblich zu einem "Mehr" an Datensicherheit bei. Es handelt sich also um eine nicht unerhebliche Kompetenzzuweisung an die G., in der strukturell neben der Bundesrepublik Deutschland die maßgeblichen Institutionen im Gesundheitswesen vertreten sind, diese aber begrenzt durch zahlreiche Kontrollmechanismen, die vor allem dem BSI und der/dem BfDI überantwortet wurden.
Damit zeugen die Regelungen in §§ 291 ff. SGB V von dem großen Bemühen des Gesetzgebers, ein Optimum an Datenschutz zu erreichen. Das Bundessozialgericht (aaO) spricht deshalb nicht umsonst von einem "risikobasierten Ansatz" der Regelungen der §§ 291 ff. SGB V, einem normdichten und klaren Regelungsgefüge, das durch eine Vielzahl aufeinander abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler Maßnahmen der Datensicherheit dient und eine ausreichende Datensicherheit gewährleistet. 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 der G. in der mündlichen Verhandlung so deutlich gemacht. Nicht bekannt ist auch, dass in anderen Bereichen des Wirtschaftslebens ähnliche Sicherheitsvorkehrungen bestehen.
Zudem ist festzustellen, dass der Gesetzgeber in den Regelungen, die elektronische Patientenkarte und die Telematikinfrastruktur betreffend (§§ 291ff. SGB V), umfangreich festgelegt hat, wer an der Umsetzung der Telematikinfrastruktur beteiligt ist und welche Aufgaben den einzelnen an der TI Beteiligten überantwortet sind. Das Gericht räumt aber zugleich ein, dass im SGB V keine oder kaum detaillierte Vorgaben und Regelungen zum Sicherheitsniveau und zu den geeigneten Sicherheitsmaßnahmen einschließlich konkreter Regelungen zur Gefahrenvorsorge enthalten sind (Stand: Jahr 2019). Trotzdem teilt das Gericht nicht die Auffassung des Prozessbevollmächtigten des Klägers, 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 für die Bundesrepublik Deutschland, Rn. 72 zu Art. 20). Außerdem ist den Bestimmtheitsanforderungen Rechnung zu tragen (Jarass/Pieroth, Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Rn. 72 zu Art. 20). Dabei handelt es sich nicht nur darum, dass überhaupt 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 für die Bundesrepublik Deutschland, Rn. 82 zu Art. 20). Die ausreichende Bestimmtheit hängt 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, verstoßen, sind solche Maßnahmen 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 grundsätzlich nicht auszuschließen ist. Bei der Frage, welche wesentlichen Regelungen dem Gesetzgeber hier vorbehalten sind, damit der Wesentlichkeitstheorie und dem Bestimmtheitsgrundsatz Rechnung getragen wird, ist auch zu berücksichtigen, dass die Digitalisierung auf allen Gebieten, so auch im Gesundheitsbereich weltweit rasant zunimmt und immer mehr die Lebenswirklichkeit bestimmt. In immer kürzeren zeitlichen Abständen besteht Veranlassung, solche Regelungen neu einzufügen bzw. bereits bestehende Regelungen anzupassen. Dies macht es erforderlich, dass die Sicherheitsvorkehrungen zur Einhaltung des Datenschutzes ebenfalls kurzfristig und laufend angepasst sowie nachjustiert werden müssen. Es handelt sich somit um eine Besonderheit der Materie, die schnelles Handeln verlangt. Die Befürchtung der Beklagten, es sei fraglich, ob der Gesetzgeber dem Rechnung tragen könne, weil die Regelungen bereits bei Inkrafttreten des Gesetzes bereits überholt sein könnten, erscheint deshalb nicht unbegründet, 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 Änderung nicht der Zustimmung der Bundesländer 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 Grundsätzen vereinbar, wenn in den gesetzlichen Regelungen (§§ 291 ff. SGB V) detaillierte Vorgaben und Regelungen zum Sicherheitsniveau und zu den geeigneten Sicherheitsmaßnahmen einschließlich konkreter Regelungen zur Gefahrenvorsorge nicht oder nur ungenügend enthalten sind.
Gleichwohl wird immer wieder über 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 Störung der Versichertenstammdaten bei der Telematikinfrastruktur und von konfigurationsbedingten Sicherheitsmängeln bei Konnektoren bestimmter Hersteller. Davon seien über einen Zeitraum von acht Wochen bis zu 80.000 Arzt/Zahnarztpraxen betroffen gewesen (zm 110, Nummer 15-16, 16.08.2020, (1472)). Die Einführung des sogenannten E-Rezeptes wurde gestoppt. Auch die Einführung der sogenannten elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) ist - soweit ersichtlich -noch nicht abgeschlossen. Außerdem besteht die Absicht, die Konnektoren zu tauschen, was zu erheblichen Kosten führen

dürfte. Insgesamt wird sogar zum Teil die Auffassung vertreten, "die regelmäßigen Pannen belegen, dass der gegenwärtige Ansatz der Vernetzung nicht hinreichend praxiserprobt und für die Digitalisierung im Gesundheitswesen im Ergebnis dysfunktional ist" (BZB, November 2021). Schließlich hat auch der Chaos Computer Club (CCC) auf verschiedene Sicherheitslücken hingewiesen.
Es mag sein, dass die in den Medien geschilderten Probleme mehr oder weniger auftraten. Zum Teil drängt sich allerdings der Eindruck auf, dass die Berichterstattung hierzu zu plakativ ist, dem Gerieren von Schlagzeilen geschuldet ist und als "Aufhänger" dienen soll, der Schaffung der Telematikinfrastruktur nicht nur kritisch gegenüber zu stehen, sondern diese pauschal und gänzlich abzulehnen. Aus den in den Medien geschilderten Problemen ist jedoch nicht auf mangelnde Datensicherheit zu schließen.
Zunächst kann nicht erwartet werden, dass die Einführung der Telematikinfrastruktur von Beginn an "reibungslos" verläuft. Die Telematikinfrastruktur befindet sich in einer Anfangs- und Erprobungsphase, die bis zur definitiven Umsetzung der in § 291a Abs. 3 SGB V genannten, sehr ambitionierten Ziele nicht nur Monate, sondern Jahre dauern dürfte. Denn es handelt sich um ein Novum im Gesundheitswesen, das in den fortgeschrittenen Ausbaustufen geradezu als revolutionär zu bezeichnen ist und für das nicht auf Erfahrungswerte aus der Vergangenheit zurückgegriffen werden kann. Der Chief Produktion Office der G., Herr H. hat darauf hingewiesen, "wir befinden uns in einer Einführungsphase eines der wichtigsten Massenprozesse des Gesundheitswesens, das jährlich rund 77 Millionen Mal durchgeführt wird." Vor diesem Hintergrund, dem Umstand, dass es sich um eine Anfangs- und Erprobungsphase handelt, sind gewisse Unschärfen 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 Sicherheitslücken 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 ausgeführt, nicht darstellbar. Dass der Gesetzgeber der Beobachtungs- und Nachbesserungspflicht genügt, 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 Einführung der Telematikinfrastruktur grundsätzlich infrage zu stellen. Denn der Gesetzgeber hat sich hierfür entschieden. In diesem Zusammenhang wird darauf hingewiesen, dass die Bundesrepublik Deutschland, obwohl zu einer der führenden Wirtschaftsnationen gehörend, im Ranking unter den 27 bewerteten europäischen Ländern nach dem Digital economy and society index (DESI) im Jahr 2022 lediglich einen mittleren Platz (Platz 13) einnimmt.
Was den Vortrag der Klägerseite betrifft, es gebe Schwachstellen im Vergabeprozess - angeblich fand keine zuverlässige Prüfung der Identität der Antragsteller statt; jedermann habe bis Ende 2019 eine Berechtigungskarte bestellen und diese auch an eine abweichende Anschrift schicken lassen können - ist dies auch nach dem Vortrag der Klägerseite ab Anfang 2020 nicht mehr möglich. 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 Ausmaß annehmen, die die Telematikinfrastrukur insgesamt in Frage stellt. Dies ist aber nicht der Fall, wie sich darin zeigt, dass es nach den Ausführungen der Beigeladenen außer den vom Computer-Chaos-Club (CCC) gemeldeten Fällen keine weiteren konkreten Fälle gab, es sich um kein echtes Szenario handelte, sondern nur um Demonstrationsfälle. Hinzu kommt, dass diese Schwachstellen später 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 höher eingestuft sind, bedeutet nicht zwangsläufig, dass das Sicherheitsniveau der Konnektoren zu niedrig wäre. Abgesehen davon sind nach Aussage der Beigeladenen in der mündlichen Verhandlung am 26.01.2023 smart meter gateway lediglich bei zwei Prüfbausteinen, die sich auch nicht auf das Produkt selbst, sondern auf den Entwicklungsprozess beim Hersteller beziehen, höher eingestuft, nämlich mit Stufe 4 statt mit Stufe 3. Außerdem wurde die Stufe der Schwachstellenanalyse nicht von 5 auf 3 abgesenkt. Im Übrigen spiegelt die Einstufung mit EAL3+ nicht das tatsächliche Sicherheitsniveau wieder. Dieses ergibt sich vielmehr aus dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach § 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 über den Konnektor statt. Die G. hat in ihrem White Paper Datenschutz und Informationssicherheitsstand September 2020 die Sicherheitsstruktur allgemein, aber auch im Einzelnen erläutert. Zu unterscheiden ist zwischen der TI-Plattform dezentrale Zone und der TI-Plattform zentrale Zone. Zur zentralen Zone gehören die Karten aller Beteiligten, die Kartenterminals, der sogenannte Konnektor, sowie die Gerätekarten, die den Kartenterminals und Konnektoren eine eindeutige Identität zuordnen. Dagegen enthält die zentrale TI-Plattform Zone Zentraldienste der TI-Plattform, die die Anwendungen der Telematikinfrastruktur mit grundlegenden Funktionalitäten unterstützen. In dem White Paper Datenschutz und Informationssicherheit wird zum Konnektor wie folgt ausgeführt: "Damit die Heilberufe auf die zentrale TI-Plattform zugreifen können, 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 über das Internet hergestellt. Sensible Daten, die über diese Verbindung versandt werden, sind zusätzlich auf Transportebene geschützt (Transport Layer Security)...In seiner Funktion als Firewall auf Netz-und Anwendungsebene schützt 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 geschützt." Insofern kann die von Klägerseite geäußerte Befürchtung, wonach von anderen Praxen eine Gefährdung ausgehen könne, nicht geteilt werden.
Ebenfalls nicht geteilt wird auch die Ansicht der Klägerseite, nur durch sog. Stand-Alone-Lösungen (= Nutzung der Dienste ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer) könne eine dem Schutz der Patientendaten "angemessene" Sicherheit gewährleistet werden. Diese Stand-Alone-Lösungen gab es noch bis Ende 2019, sodass der Einwand jedenfalls für die hier streitbefangenen Quartale nicht gilt. Im Übrigen ist nicht ersichtlich, dass die Aufgabe der Stand-Alone-Lösungen nicht hinnehmbare Auswirkungen auf die Datensicherheit hat. Auch zukünftig sind die Leistungserbringer, so auch der Kläger nicht gehindert, sich einen zweiten Konnektor allerdings auf eigene Kosten zu beschaffen, falls trotzdem Zweifel an der Sicherheit der Daten bestehen sollten.
Ein Verstoß der gesetzlichen Regelungen der §§ 291 ff. SGB V gegen Art. 5 Buchst. f DSGVO ist deshalb nicht festzustellen.
Die Klägerseite beanstandet ferner, dass die datenschutzrechtliche Verantwortlichkeit ganz oder jedenfalls überwiegend dem Vertrags-(zahn)arzt auferlegt ist. Es trifft zu, dass erst mit Gesetz vom 14.10.2020 (BGBl I S. 2115) datenschutzrechtliche Verantwortlichkeiten in § 307 SGB V geregelt sind. Danach (§ 307 Abs. 1 SGB V) liegt die Verantwortung für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Abs. 2 Nr 1 SGB V (insbesondere ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten) bei denjenigen, die diese Komponenten für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen. Ferner ist der Anbieter des gesicherten Netzes innerhalb des gesicherten Netzes für Übertragung von personenbezogenen Daten verantwortlich, insbesondere von Gesundheitsdaten der Versicherten, zwischen Leistungserbringern, Kostenträgern sowie Versicherten und für die Übertragung im Rahmen der Anwendungen der elektronischen Gesundheitskarte (§ 307 Abs. 3 S. 2 SGB V). Auch die G. wurde nunmehr in den Kreis der datenschutzrechtlich Verantwortlichen in § 307 Abs. 5 S. 1 SGB V mit aufgenommen. So ist sie verantwortlich für die

Verarbeitung personenbezogener Daten in der Telematikinfrastruktur, soweit sie im Rahmen ihrer Aufgaben nach § 311 Abs. 1 die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist. Es handelt sich somit um eine subsidiäre Verantwortlichkeit der G., was sich daraus ergibt, dass diese nur dann besteht, soweit nicht die in § 307 Abs. 1, 3 und 4 SGB V genannten verantwortlich sind.
Daraus, dass vor dem 14.10.2020 keine ausdrücklichen Verantwortlichkeiten im SGB V festgelegt wurden, ergibt sich allerdings kein Verstoß gegen die DSGVO. Denn, wer datenschutzrechtlicher Verantwortlicher ist, folgt bereits aus der Legaldefinition in Art. 4 Ziff 7 DSGVO. Danach ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dieser setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür zu erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (Art. 24 DSGVO). Daraus folgt zumindest indirekt die Verantwortlichkeit für die natürliche Person oder juristische Person, Behörde, Einrichtung oder andere Stelle für die Einhaltung des Datenschutzes innerhalb der eigenen Sphäre. Der Vertragszahnarzt hat keine Verantwortung für 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 für die dezentrale Zone. Eine solche Verantwortlichkeit des Vertragszahnarztes für die dezentrale Zone stellt kein Novum dar. Denn bereits vor Einführung der E-Gesundheitskarte lag es im Verantwortungsbereich des Vertrags-(zahn)arztes, die datenschutzrechtlichen Vorgaben in seiner Sphäre zu beachten. Jegliche Haftung ist außerdem verschuldensabhängig, sodass ein Haftungsrisiko für den Vertragsarzt bei bestimmungsgemäßem Anschluss an die TU, bestimmungsgemäßer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen Datenschutzmaßnahmen (zum Beispiel Absicherung der Hard-und Software) nicht besteht. Im Übrigen wurde, wie der Vertreter der G. in der mündlichen Verhandlung am 09.11.2022 in den vorausgegangenen Verfahren (aaO) ausführte, bereits Mitte 2019 ein Informationsblatt zum Datenschutz und Haftung in der Telematikinfrastruktur herausgegeben.
Außerdem 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 Verstoß gegen Art. 26 DSGVO ist nicht ersichtlich, wenn keine gemeinsame Verantwortlichkeit festgelegt wurde. Es ist bereits fraglich, ob die G. in den Quartalen des Jahres 2019 als verantwortlich im Sinne von Art. 4 Nr 7 DSGVO anzusehen ist. Allein dadurch, dass die G. Komponenten und Dienste der Telematikinfrastruktur (§ 291b Abs. 1a SGB V) zulässt und als "actus contrarius" Komponenten und Dienste für den Zugang sperren kann (§ 291b Abs. 5 S. 6 SGB V), besitzt sie zumindest eine Entscheidungsbefugnis über die Mittel der Datenverarbeitung. Dagegen ist eine Entscheidungsbefugnis der G., was den Zweck, also das ob, wofür und wie weit der Datenverarbeitung betrifft, nicht ersichtlich. Denn die Entscheidungsbefugnis müsste von einem Eigeninteresse an der Datenverarbeitung getragen sein, was aber nicht der Fall ist. Vielmehr fungiert die G. lediglich als organisatorische und koordinierende Institution und erfüllt als solche nur die ihr auferlegten gesetzlichen Pflichten (aA . Dochau in MedR 2020, 979, 985; Kühling/Sackmann, Datenschutzrecht, Rn. 538, 541).
Abgesehen davon bestimmt Art. 26 Abs. 1 S. 2 DSGVO, dass "gemeinsam Verantwortliche" in einer Vereinbarung in transparenter Form festlegen, wer von Ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt... Eine solche Vereinbarung wurde nicht geschlossen und wäre auch nicht umsetzbar, zumal jeder einzelne an der TI teilnehmende Vertrags-(zahn)arzt in einer Individualvereinbarung mit der G. die wechselseitigen Verpflichtungen festlegen müsste. Es müssten 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 wären. An sich müssten 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 über die TI weitere Anwendungen stattfinden sollen (so zum Beispiel Verarbeitung von Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation (elektronischer Arztbrief; § 291a Abs. 3 Ziff. 2 SGB V) und die Verarbeitung von Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichten sowie Impfungen für eine fall-und einrichtungsübergreifende Dokumentation über die Versicherten sowie durch von Versicherten selbst oder für Sie zur Verfügung gestellte Daten (elektronische Patientenakte; § 291a Abs. 3 Ziff. 2 SGB V), ist nicht Gegenstand im streitgegenständlichen Verfahren, sodass über deren Vereinbarkeit mit der DSGVO nicht zu befinden ist. In der Tat gehen diese Anwendungen weit über den in § 291 Abs. 2b S. 2 SGB V verpflichtenden Datenabgleich hinaus. Ohne einer späteren rechtlichen Bewertung und Entscheidung vorgreifen zu wollen, wird zu beachten sein, dass, je umfangreicher die Datenverarbeitung stattfinden soll, umso größer also das Gefährdungspotenzial ist, umso größere Anforderungen sind an die Datensicherheit zu stellen.
Zusammenfassend kommt das Gericht zu dem Ergebnis, dass die Vorschriften der §§ 291 ff. SGB V mit der DSGVO rechtlich zu vereinbaren sind.
Schließlich muss auch der mit der Nichtteilnahme an der Telematikinfrastruktur verbundene Honorarabzug seinerseits verhältnismäßig sein. Bei Verstoß gegen die Pflicht zur Fortbildung nach § 95d SGB V beträgt der Honorarabzug zunächst 10 % für die ersten vier Quartale, später dann 25 % (§ 95d Abs. 3 S. 3 SGB V). Wird der Fortbildungsnachweis nicht spätestens zwei Jahre nach dem Ablauf des Fünfjahreszeitraums geführt, steht auch die Zulassung zur vertrags(-zahn) ärztlichen Tätigkeit zur Disposition (§ 95 Abs. 6 SGB V). Gemessen daran handelt sich um einen moderaten Honorarabzug (zunächst 1 %, später 2,5 % vom Gesamthonorar) bei Nichtteilnahme an der Telematikinfrastruktur. Eine Verpflichtung des Vertrags-(zahn)arztes zur Teilnahme an der Telematikinfrastruktur ohne jegliche Sanktion würde dazu führen, dass sich ein Teil der Vertrags-(zahn)ärzte der Telematikinfrastruktur trotzdem anschließen, ein anderer Teil aber sanktionslos davon Abstand nehmen könnte. Damit könnten die Ziele der Einführung der E- Gesundheitskarte nicht erreicht werden. Der Grundsatz der Verhältnismäßigkeit in Bezug auf die Honorarkürzung ist trotz der in den Quartalen des Jahres 2019 äußerst eingeschränkten Datenverarbeitung (Online-Abgleich) gewahrt. Wenn es bei der Datenverarbeitung solcher Art und solchen Ausmaßes bliebe, dann wäre in der Tat die Verhältnismäßigkeit der Honorarkürzung grundsätzlich, zumindest aber der Höhe nach kritisch zu würdigen. Jedoch ist hier zu berücksichtigen, dass die Nutzung der Dienste in mehreren Schritten gesteigert werden und die Telematikinfrastruktur künftig zu einem Bündel unterschiedlicher Anwendungen dienen soll. Würden bereits bei den ersten Schritten der Einführung keine Sanktionen (Kürzungen) erfolgen oder würden die Sanktionen geringer sein mit der Folge, dass ein Teil der Vertrags-Ärzte keine Veranlassung sehen würden, sich an die TI anzuschließen, hätte dies weitreichende Konsequenzen für die vom Gesetzgeber in Zukunft beabsichtigte umfangreichere Nutzung der TI. Insofern ist es mit dem Verhältnismäßigkeitsgrundsatz vereinbar, dass bereits am Anfang der Einführung der TI Sanktionen (Kürzungen) in der genannten Höhe 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 tatsächliche Unmöglichkeit. In diesem Fall wäre es als unverhältnismäßig anzusehen, das Honorar zu kürzen. Allerdings wäre vom Vertrags-(zahn)arzt der Nachweis zu führen, dass eine solche Konstellation vorliegt.
Soweit wegen der verpflichtenden Teilnahme der Vertrags-(zahn)ärzte an der Telematikinfrastruktur ein Verstoß gegen Art. 12 Grundgesetz geltend gemacht wird, ist diese Auffassung nicht zu teilen. Denn es ist zu differenzieren zwischen einer Berufswahl- und einer Berufsausübungsregelung. Allenfalls könnte 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 Berufsausübungsregelung 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 Berufsausübungsregelung zulässig ist, wenn "sachlich nachvollziehbare Erwägungen des Normgebers im Hinblick auf die Gestaltungsfreiheit" 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 Verhältnismäßigkeitsgrundsatz ausgeführt, dient die Einführung 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 Gewährleistung der finanziellen Stabilität der GKV. Es handelt sich somit um sachlich nachvollziehbare Erwägungen des Normgebers, die einen Eingriff in die Berufsausübungsfreiheit nach Art. 12 GG rechtfertigen (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R).
Genausowenig ist ein Verstoß gegen Art. 2 Abs. 1 GG (allgemeine Handlungsfreiheit) ersichtlich. Es ist anerkannt, dass es sich hierbei um ein sog. Auffanggrundrecht handelt, das gegenüber dem in Art. 12 Abs. 1 GG speziellen Grundrecht zurücktritt (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). Geschützt wird der Einzelne gegen informationsbezogene Maßnahmen, die ihn betreffen und die für ihn weder überschaubar, noch beherrschbar sind. Der Einzelne ist befugt, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen 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 Verstoß 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) ausgeführt, "im subjektiv geprägten Sozialgerichtsverfahren" könne sich der Kläger grundsätzlich nicht auf die Verletzung von Rechten Dritter berufen. Selbst wenn dies zu bejahen wäre, kann nichts Anderes gelten als für den betroffenen Patienten, dessen Daten erfasst und weitergegeben werden. Denn das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos. Eine solche Grundrechtseinschränkung ist zulässig, wenn sie auf einer gesetzlichen Ermächtigung beruht, die ihrerseits einen legitimen Gemeinwohlzweck verfolgt und der Grundsatz der Verhältnismäßigkeit eingehalten wird (BSG, Urteil vom 20.01.2021, Az B 1 KR 7/20 R). Dies ist, wie wiederholt ausgeführt wurde, der Fall.
Neben der haftungsrechtlichen Fragestellung hat die Klägerseite die Befürchtung geäußert, es sei zu besorgen, dass sich der Vertragsarzt strafrechtlich (§ 203 StGB) verantworten müsse, wenn er sich an die TI anschließe und es zu einem Datenmissbrauch komme. Nach § 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs-oder Geschäftsgeheimnis offenbart das ihm als Arzt, Zahnarzt anvertraut worden oder sonst bekannt gegeben worden ist. Selbst wenn der objektive Tatbestand von § 203 StGB erfüllt wäre, ist bei bei bestimmungsgemäßem Anschluss an die TI, bestimmungsgemäßer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen Datenschutzmaßnahmen (zum Beispiel Absicherung der Hard-und Software) der subjektive Tatbestand zu verneinen. Denn dieser erfordert nämlich Vorsatz, zumindest bedingten Vorsatz (vgl Thomas Fischer, Kommentar zum StGB, Rn. 92 zu § 203).
Betroffene Personen, die der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt, haben die Möglichkeit, Rechtsbehelfe nach Art. 77 ff. DSGVO in Verbindung mit §§ 81 ff SGB X einzulegen. Im Einzelnen handelt es sich um das Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 Abs. 1 DSGVO), das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde (Art. 78 Abs. 1 DSGVO). Für den gerichtlichen Rechtsbehelf ist der Rechtsweg zu den Gerichten der Sozialgerichtsbarkeit nach § 81a Abs. 1 bzw. § 81b SGB X eröffnet.
Rechtsgrundlage für einen Schadenersatzanspruch wegen eines Verstoßes gegen diese Verordnung, die zu einem materiellen oder immateriellen Schaden geführt 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 für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Insofern kann er weder für einen Schaden haftbar gemacht werden, der nicht in seiner Sphäre entstanden ist, noch kann er für einen Schaden haftbar gemacht werden, der zwar in seiner Sphäre entstanden ist, den er aber bei bestimmungsgemäßem Anschluss an die TU, bestimmungsgemäßer Nutzung, ordentlicher Wartung und Beachtung der erforderlichen Datenschutzmaßnahmen (zum Beispiel Absicherung der Hard-und Software) nicht zu vertreten hat.
Aus den genannten Gründen sind die angefochtenen Bescheide (Honorarkürzung) als rechtmäßig anzusehen und ist die Klage abzuweisen. Ein Verstoß der Vorschriften der §§ 291ff. SGB V gegen höherrangiges Recht, insbesondere die DSGVO und das Grundgesetz ist nicht ersichtlich.
Die Kostenentscheidung beruht auf § 197a SGG in Verbindung mit § 154 VwGO.

Rechtskraft
Aus
Saved
2023-02-27