Wichtige Hinweise / Haftungsausschluss:

Bitte beachten Sie, dass der nachfolgende Text ein unverbindliches Muster darstellt; es wird kein Anspruch auf Vollständigkeit und/oder Richtigkeit erhoben. Das Muster dient lediglich als Anregung und Hilfestellung im Zusammenhang mit der Formulierung.
Im konkreten Einzelfall bedarf das Muster gegebenenfalls weiterer Ergänzungen sachlicher und/oder rechtlicher Art. Insoweit wird nicht ausgeschlossen, dass das Muster im Einzelfall nicht geeignet ist, den beabsichtigten Zweck zu erreichen.

Im Verfahren vor dem Sozialgericht besteht kein Anwaltszwang. Die vorliegende Musterdarstellung soll die anwaltliche Rechtsberatung nicht ersetzen. Soweit rechtliche Fragen bestehen, wenden Sie sich unbedingt an einen Rechtsanwalt Ihrer Wahl. Der Medi Geno e.V. übernimmt keine Haftung für tatsächliche und/oder rechtliche Folgen, welche sich aus der Verwendung des Musters ergeben können; gleiches gilt hinsichtlich jeglicher Rechtspositionen der am Verfahren Beteiligten.

Wir weisen Sie darauf hin, dass im gerichtlichen Verfahren Fristen laufen können, welche beachtet werden müssen. Soweit Sie die Fristen versäumen, wird dies regelmäßig zu Nachteilen für Sie führen.

Sollte in einem gerichtlichen Verfahren ein Termin zur mündlichen Verhandlung terminiert werden, so wollen Sie uns dies im Einzelfall gerne zur Kenntnis bringen.

Erläuterungen:

Nachfolgend wollen wir Ihnen einige wenige Erläuterungen zu dem unverbindlichen Mustertext geben, welche sich allesamt auf formelle Aspekte im Zusammenhang mit der Verwendung beziehen.

Eine Klage muss bei dem **zuständigen Sozialgericht** erhoben werden. Der Widerspruchsbescheid, der mit der Klage angegriffen werden soll, enthält eine **Rechtsbehelfsbelehrung**. Dieser Rechtsbehelfsbelehrung ist zu entnehmen, bei welchem Gericht innerhalb welcher Frist Klage erhoben werden muss.

Die Klageschrift muss mit einem **Datum** versehen und **von dem Kläger unterzeichnet** werden; erfolgt dies nicht, ist die Klage nicht wirksam erhoben.

Der (Gebühren-)Streitwert orientiert sich an dem wirtschaftlichen Interesse des Klägers und stellt den finanziellen Wert des Streitgegenstandes dar. Beträgt die pauschale Honorarkürzung bspw. 500,00 €, so beträgt auch der Streitwert 500,00 €.

Im **Klageantrag** wird der Gegenstand Ihres Anliegens genau bezeichnet. Damit ist gemeint, dass Sie angeben müssen, welches Ziel Sie mit der Klage verfolgen. Das Gericht muss wissen, was Sie von der Beklagten wollen. Notieren Sie, wann genau Ihnen der angegriffene Widerspruchsbescheid zugegangen ist. Wird mit der Klage die Aufhebung oder Änderung eines Bescheides und Widerspruchsbescheides verfolgt, so fügen Sie **Kopien** des von Ihnen **angegriffenen Bescheides** und des **Widerspruchsbescheides** in Anlage bei. Dies ermöglicht es dem Gericht, Ihr Anliegen zu erfassen und erspart Nachfragen.

An das Sozialgericht _____

_____

_____

__.__.2023

K l a g e

des / der _____
_____

- Kläger –

g e g e n

Kassenärztliche Vereinigung _____,
vertreten durch den Vorstand, dieser vertreten durch dessen Vorsitzenden des Vorstands, _____

- Beklagte –

WEGEN: Widerspruch gegen Bescheid
STREITWERT: _____ €

Es wird

K l a g e

zum zuständigen Sozialgericht _____ erhoben und beantragt,

den Bescheid der Beklagten vom _____ in Gestalt des Widerspruchsbescheides vom _____ aufzuheben.

Dem Kläger ist bekannt, dass zu der Frage der Rechtmäßigkeit des pauschalen Honorarabzugs bei Nicht-Anschluss einer Praxis an die Telematikinfrastruktur sowie Nichtdurchführung des Versichertenstammdatenmanagements (VDSM) mehrere gleichgelagerte Musterverfahren gegen Kassenärztliche Vereinigungen geführt werden, welche derzeit bei den Gerichten anhängig sind. Die entsprechenden Aktenzeichen lauten:

- BSG B 6 KA 23/22 R (KV Rheinland-Pfalz)
- LSG Baden-Württemberg L 5 KA 620/22 (KV Baden-Württemberg).

Gegenstand dieser Musterverfahren werden zum überwiegenden Teil auch jene Rechtsfragen betreffen, die Gegenstand dieses Klageverfahrens sein sollten. Die Klage wird somit (auch) zur Wahrung der klägerischen Rechte und Rechtspositionen eingelegt.

Es wird daher weiterhin beantragt,

das streitgegenständliche Klageverfahren bis zum rechtskräftigen Abschluss der vorbezeichneten Klageverfahren ruhend zu stellen

Den Bescheid der Beklagten vom _____ sowie den streitgegenständlichen Widerspruchsbescheid vom _____ – zugegangen am _____ – überlassen wir dem erkennenden Gericht in Kopie als

Anlage K1 und **K2.**

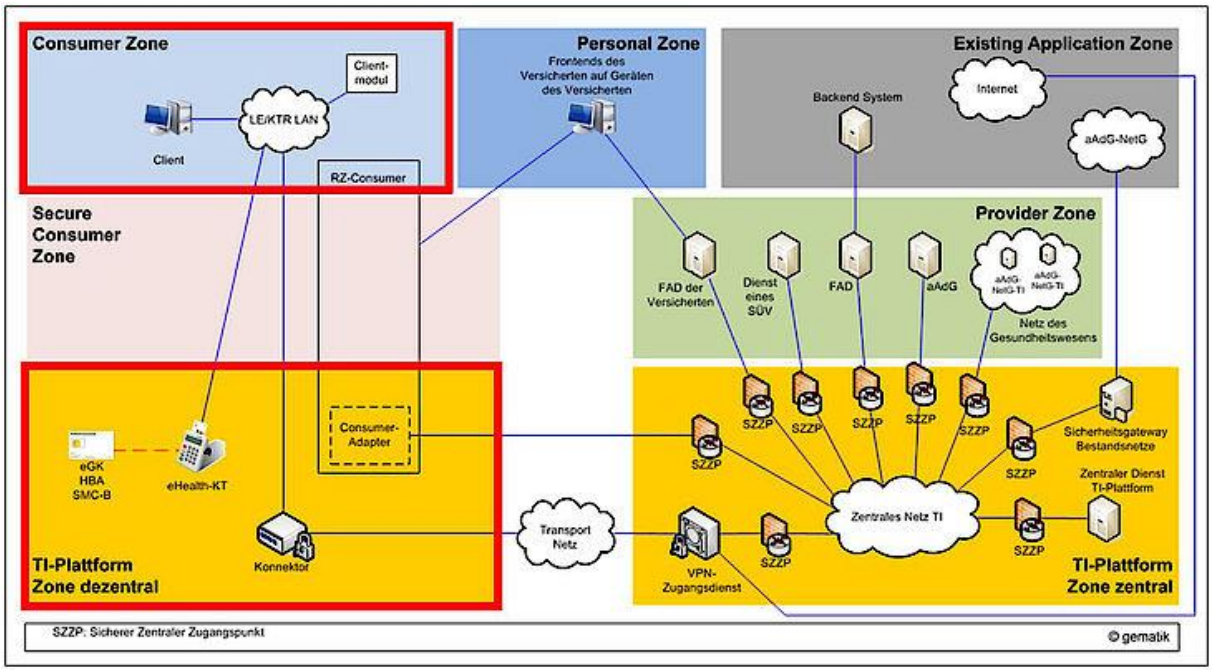
B e g r ü n d u n g

Die Klage ist zulässig und begründet.

Der Honorarbescheid in der Gestalt des beklagten Widerspruchsbescheids für das streitgegenständliche Abrechnungsquartal betreffend die Praxis des Klägers ist – soweit es den pauschalen Abzug in Höhe von 2,5 Prozent des Gesamthonoraranspruch für die Nichtinstallation des Konnektors betrifft – aufzuheben, da die seitens des Gesetzgebers auferlegte Pflicht zur Durchführung des Versichertenstammdatenabgleichs (§ 291b Abs.2 S.1-2 SGB V) mit den derzeit von der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zugelassenen Telematik-Komponenten-Modellen für die verpflichteten Leistungserbringer, so auch den Kläger, nur unter Verstoß gegen höherrangiges Recht möglich wäre. Die Nutzung der TI-Komponente „Konnektor“ verstößt zumindest in Form der derzeitigen rechtlichen und tatsächlichen Ausgestaltung gegen Vorschriften der Datenschutzgrundverordnung (DSGVO). Zudem führen diese Datenschutzverstöße sowie die konkret nachweisbaren Sicherheitsmängel der Telematik-Komponente „Konnektor“ im Ergebnis zu einem vom Kläger nicht hinzunehmenden, unverhältnismäßigen Eingriff in seine Berufsausübungsfreiheit gemäß Art.12 GG.

1. Verstöße gegen die DSGVO

Die derzeitige tatsächliche und regulatorische Ausgestaltung des Versichertenstammdatenmanagements („VSDM“) verstößt in mehrfacher Hinsicht gegen höherrangiges Gesetzesrecht in Form der Datenschutzgrundverordnung: Zur technischen Durchführung des VSDM dient die sog. Telematikinfrastruktur, bestehend aus zwei Zonen, der sog. zentralen Zone einerseits, also die zentrale Vernetzung zwischen allen Beteiligten, und der sog. dezentralen Zone andererseits, nämlich die notwendige technische Ausstattung und Anbindung des jeweils Beteiligten, z.B. in einer (Zahn)Arztpraxis / psychotherapeutischen Praxis. Über die dezentrale Zone der TI, nämlich über den in der (Zahn)Arztpraxis / psychotherapeutischen Praxis zu installierenden Konnektor und das daran angeschlossene Kartenlesegerät, werden die auf der jeweiligen elektronischen Gesundheitskarte gespeicherten Daten eines jeden Patienten ausgelesen. Anschließend wird eine Aufforderung zum Datenabgleich mit den bei der jeweiligen Krankenversicherung gespeicherten Daten gesandt. Sofern dieser Datenabgleich ergibt, dass es gegenüber dem auf der Versichertenkarte gespeicherten Datenbestand eine Neuerung gibt, wird dieser neue Datenstand direkt auf die Versichertenkarte gespielt und dort gespeichert, also noch während sich die Versichertenkarte im Kartenlesegerät der Arztpraxis befindet. Insgesamt stellt dies eine Datenverarbeitung personenbezogener Daten im Sinne von Art.4 Ziff.2 DSGVO dar, so dass die Vorgaben der DSGVO eingehalten werden müssen.



Quelle: https://www.gematik.de/news/news/ti-anschluss-gematik-aktualisiert-ueberblick-fuer-dienstleister-vor-ort/

Neben den eigentlichen Stammdaten des Versicherten (wie z.B. Name, Anschrift, Geburtsdatum, Krankenversicherung) werden auch gesundheitsbezogene Daten gespeichert und verarbeitet. Gemäß dem „Fachkonzept Versichertenstammdatenmanagement“ der gematik und der „technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-Ä)“ wird auf der elektronischen Gesundheitskarte ein „DMP-Kennzeichen“ zu folgenden chronischen Erkrankungen gespeichert: Diabetes mellitus Typ 2, Brustkrebs, Koronare Herzkrankheit, Diabetes mellitus Typ 1, Asthma bronchiale und/oder COPD. Hierbei handelt es sich zweifellos um Gesundheitsdaten und somit um eine Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne von Art.9 Abs.1 DSGVO.

Eine Datenverarbeitung ist bereits im Ansatz rechtlich überhaupt nur zulässig, wenn ein „Verantwortlicher“ der Datenverarbeitung im Sinne von Art.4 Nr.7 DSGVO feststeht, denn die Pflichten aus Art.5 DSGVO setzen zum großen Teil der Datenverarbeitung zeitlich vorgelagerte Maßnahmen voraus, so z.B. die Prüfung der Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs.1 lit.a DSGVO), die Festlegung des Verarbeitungszwecks (Art. 5 Abs.1 lit.b DSGVO) und Gewährleistung der Datensicherheit durch geeignete technische und organisatorische Maßnahmen (Art. 5 Abs.1 lit.f DSGVO) sowie Art.24 Abs.1, Art.32 DSGVO.

Trotz dieser eindeutigen gesetzlichen Vorgaben und trotz des Umstands, dass über den TI-Konnektor beim VSDM sogar Gesundheitsdaten in einem ganz erheblichen Umfang verarbeitet werden, war die datenschutzrechtliche Verantwortlichkeit für die

Telematikinfrastruktur zunächst lange Zeit gänzlich ungeklärt bzw. niemand hat sich zu dieser Verantwortung bekannt, geschweige denn die daraus erwachsenden Pflichten erfüllt, so dass das gesamte Pflichtenregime der DSGVO ins Leere lief, solange sich der „Verantwortliche“ für eine Datenverarbeitung nicht bestimmen ließ.

Die fehlende gesetzliche Regelung hatte die Datenschutzkonferenz (DSK - Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) bereits in einem Beschluss vom 12.09.2019 dahingehend gerügt und hat in diesem Beschluss sie zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematikinfrastruktur den Rechtsstandpunkt eingenommen, dass die gematik für die zentrale Zone der Telematikinfrastruktur datenschutzrechtlich alleinverantwortlich und für die dezentrale Zone der TI datenschutzrechtlich mitverantwortlich ist (siehe Beschluss unter https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zur_gematik.pdf).

Hierauf hat der Gesetzgeber erst im Herbst 2020 reagiert, im Ergebnis jedoch mit einer Regelung, die gegen Art.4 Nr.7 DSGVO verstößt:

Mit Inkrafttreten des Patientendatenschutzgesetzes (PDSG) zum 20.10.2020 hat der Gesetzgeber in § 307 SGB V n.F. Regelungen getroffen, die datenschutzrechtliche Verantwortung aller Beteiligten regeln und voneinander abgrenzen soll. In § 307 Abs.1 S.1 SGB V wird die datenschutzrechtliche Verantwortung für die TI-Komponenten in der sog. "dezentralen Zone" geregelt, wozu derzeit das Kartenlesegerät und der TI-Konnektor vor Ort beim Leistungsträger, also z.B. innerhalb einer Arztpraxis gehören (siehe obiges Bild, die dezentrale Zone ist dort links unten eingerahmt). Nach § 307 Abs.1 S.1 SGB V soll die datenschutzrechtliche Verantwortung dafür bei denjenigen liegen, die diese Komponenten "nutzen, soweit sie über die Mittel der Datenverarbeitung mitentscheiden". Nach Ansicht des Gesetzgebers fallen unter diesen abstrakten Regelungswortlaut die Leistungsträger, also die datenschutzrechtliche Verantwortung für die Datenverarbeitung über das Kartenlesegerät und die TI-Konnektoren wird den Ärzten und Psychotherapeuten zugeschrieben. Der Gesetzgeber schreibt ferner in den folgenden Absätzen 2 bis 4 des § 307 SGB V den jeweiligen Anbietern der sog. Zugangsdienste, Netze und Infrastrukturdienste die datenschutzrechtliche Verantwortung zu. Lediglich für danach eventuell noch verbleibende Bereiche der Telematikinfrastruktur wird der gematik in § 307 Abs.5 SGB V noch eine datenschutzrechtliche Verantwortung zugeordnet ("insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist"). Im Ergebnis entbindet der Gesetzgeber mit der gesetzlichen Neuregelung (§ 307 SGB V) die gematik von jeder maßgeblichen datenschutzrechtlichen Verantwortung, obwohl die gematik aufgrund der gesetzlichen Kompetenzen und auch in rein tatsächlicher Hinsicht die zentrale Steuerung der Telematikinfrastruktur übernimmt und für alle sonstigen Beteiligten die einschlägigen Regelwerke erstellt und Zulassungen prüft und erteilt. Die gesetzlichen Regelungskompetenzen der gematik

und die Realität werden damit auf den Kopf gestellt, indem die gematik von ihrer datenschutzrechtlichen Verantwortung entbunden wird. Da die Gesellschaftsanteile an der gematik GmbH zu 51% von dem Bundesministerium für Gesundheit gehalten werden, muss man hier leider eine interessensgeleitete, politische Entscheidung unterstellen, die jedoch unter Missachtung der Vorgaben aus Art. 4 Nr.7 DSGVO erfolgte. Dabei wurde sogar der oben bereits erwähnte Beschluss der Datenschutzkonferenz ignoriert, wonach der gematik für die zentrale Zone der TI die alleinige datenschutzrechtliche Verantwortung und für die dezentrale Zone zumindest eine datenschutzrechtliche Mitverantwortung zugeschrieben wurde.

Der Gesetzgeber ist aufgrund der Vorgabe aus Art.4 Nr.7 DSGVO nicht frei in seiner Zuordnung von datenschutzrechtlichen Verantwortlichkeiten. So darf danach zwar der nationale Gesetzgeber Verantwortlichkeiten gesetzlich zuordnen, jedoch nur "wenn die Festlegungen die jeweiligen tatsächlichen Funktionen und Beziehungen der verarbeitenden Stellen gebührend widerspiegeln und die betroffenen Personen nicht der Möglichkeit beraubt werden, ihre Rechte gegenüber denjenigen Stellen geltend zu machen, die den faktisch größten Einfluss auf die Datenverarbeitung haben (Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO, 1. Aufl. 2019, Artikel 4 Nummer 7, Rn. 26). Dieser Standpunkt wurde auch während des Gesetzgebungsverfahrens des Patientendatenschutzgesetzes vom Bundesdatenschutzbeauftragten in dem im Mai 2020 veröffentlichten Tätigkeitsbericht für 2019 auf den Seiten 26 und 27 wiederholt und aufrechterhalten. Auch der Bundesrat hat die jetzige Regelung der Verantwortlichkeiten in § 307 SGB V, insbesondere die Entbindung der gematik von der datenschutzrechtlichen Mitverantwortung für unvereinbar mit Art.4 Nr.7 und Art.26 DSGVO erachtet (siehe Drucksache 19/19365 vom 20.05.2020 mit der Stellungnahme des Bundesrates zum Patientendatenschutzgesetz nebst Gegenäußerung der Bundesregierung, Seiten 1, 4-7 und 25). So heißt es insbesondere auf Seite 6 und 7:

> "Soweit die Gesellschaft für Telematik die Zwecke und Mittel der Datenverarbeitung bestimmt, kann von diesem Faktum nicht durch eine gesetzliche Festlegung abgewichen werden beziehungsweise darf durch eine nationale Gesetzgebung nicht eine Stelle als allein verantwortlich bezeichnet werden, die faktisch nicht vollumfänglich die Zwecke und Mittel der Datenverarbeitung bestimmt […] Dies führt auch zu der Erkenntnis, dass für die Verarbeitung von Gesundheitsdaten durch die Gesellschaft für Telematik und die Unternehmen, welche technische Hilfsdienste umsetzen, wie das Betreiben eines Netzes, die technische Bereitstellung von Zugangsdiensten und der Anwendungsinfrastruktur eine gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO vorliegen wird. Nach Artikel 26 Absatz 2 DSGVO müssen die jeweiligen tatsächlichen Funktionen und Beziehungen der Verantwortlichen gegenüber den betroffenen Personen gebührend berücksichtigt werden […] Vielmehr muss nach Artikel 26 Absatz 1 DSGVO konkret festgelegt werden, welcher der

gemeinsam Verantwortlichen welche konkreten Aufgaben übernimmt. Dies umfasst neben der Festlegung der technisch-organisatorischen Vorgaben (Artikel 32 DSGVO), insbesondere die Wahrnehmung und Umsetzung der Rechte betroffener Personen nach Artikel 12 ff. DSGVO. Da dieser Punkt bisher kaum zum Ausdruck kommt, bleibt offen, wie der mit dem Gesetzentwurf intendierte Zweck des Patientendatenschutzes erreicht werden kann. In dem Gesetzentwurf müssen die Vorgaben und die Umsetzung der gemeinsamen Verantwortung gebührend zum Ausdruck kommen."

Die gematik bestimmt nach § 311 SGB V die technischen und funktionalen Vorgaben der Telematikinfrastruktur und somit auch die grundlegenden Vorgaben der Datenverarbeitung personenbezogener Daten, soll jedoch andererseits gemäß § 307 SGB V datenschutzrechtlich nicht verantwortlich sein, obwohl sie durch die ihr zugeordneten Aufgaben gemäß § 311 SGB V nach Art.4 Nr.7 DSGVO in Bezug auf die dezentrale Zone zumindest gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet und somit Verantwortliche i.S.d. DSGVO ist.

Aus der Sicht der Ärzte und Psychotherapeuten liegt die in § 311 Abs.1 SGB V vorgenommene gesetzliche Zuordnung der datenschutzrechtlichen Verantwortung in der dezentralen Zone neben der Realität: Wie sollen die Ärzte die Funktionalität der ihnen gesetzlich vorgeschriebenen TI-Konnektoren und Kartenlesegeräte überblicken, als dass sie dazu gegenüber Ihren Patienten die Betroffenenrechte aus der DSGVO wie z.B. die Auskunft und Informationen erfüllen könnten?

Obwohl die gematik, an der die Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit, zu 51% die Gesellschaftsanteile hält, die konzeptionellen und regulatorischen Vorgaben für die TI vornimmt und die zentralen Maßnahmen für deren Steuerung vornimmt, wird sie von nach der gesetzlichen Neuregelung von der datenschutzrechtlichen (Mit-)Verantwortung entbunden.

Die gesetzliche Regelung des § 307 SGB V zur datenschutzrechtlichen Verantwortung ohne Berücksichtigung der gematik verstößt somit gegen die DSGVO und damit gegen höherrangiges Recht. Vielmehr ist – entsprechend dem Beschluss der Datenschutzkonferenz vom 12.09.2019 von einer datenschutzrechtlichen Mitverantwortung der gematik im Sinne von Art.26 DSGVO für die dezentrale Zone auszugehen.

Auch wenn gemäß des Beschlusses der Datenschutzkonferenz vom 12.09.2019 anzunehmen ist, dass in Bezug auf die dezentrale Zone der Telematikinfrastruktur, also z.B. der TI-Anbindung in der jeweiligen Arztpraxis / psychotherapeutischen Praxis, die Konstellation der datenschutzrechtlichen Mitverantwortlichkeit, Art.26 DSGVO, vorliegt, fehlt ein Regelungswerk im Sinne von Art.26 Abs.1 S.2 DSGVO, aus welchem hervorgeht, wer die Mitverantwortlichen sind und wer von ihnen welche Pflicht aus der

DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen – also der gesetzlich krankenversicherten Patienten der Praxis des Klägers – angeht (Art.13 bis 21 DSGVO). Eine Vereinbarung bzw. gesetzliche Regelung im Sinne von Art.26 Abs.1 DSGVO müsste zumindest in Bezug auf die dezentrale Zone der TI im Verhältnis zwischen gematik und den jeweiligen Praxisinhabern vorgenommen werden, denn die Ärzte sind „Mitverantwortliche“ im Sinne von Art.26 DSGVO. Sie treffen als Hausherren ihrer Praxis die Entscheidung darüber, ob bspw. ein TI-Konnektor an die zentrale Zone der Telematikinfrastruktur angeschlossen wird bzw. ob er anschließend zum Zwecke des VSDM genutzt wird. Mit dem Verstoß gegen Art.26 Abs.1 S.2 DSGVO wird somit derzeit im Zuge des VSDM gegen höherrangiges Recht verstoßen.

Ferner werden Art.5 Abs.1 lit.f, Art.24 Abs.1 S.2, Art.32 Abs.1 lit.d DSGVO sowie § 306 Abs.3 und § 311 Abs.3 S.4 SGB V durch die bereits anfänglichen technischen Vorgaben seitens gematik und dem BSI Bundesamt für Sicherheit in der Informationstechnik („BSI“) verletzt. So heißt es insbesondere in § 306 Abs.3 SGB V in der seit dem 20.10.2020 geltenden Fassung:

> *" Für die Verarbeitung der zu den besonderen Kategorien im Sinne von Artikel 9 der Verordnung (EU) 679/2016 gehörenden personenbezogenen Daten in der Telematikinfrastruktur* ***gilt ein dem besonderen Schutzbedarf entsprechendes hohes Schutzniveau****, dem durch entsprechende technische und organisatorische Maßnahmen im Sinne des Artikels 32 der Verordnung (EU) 679/2016 Rechnung zu tragen ist."*

Ferner heißt es in § 311 Abs.3 S.4 SGB V:

> *"Die Datensicherheit ist dabei* ***nach dem Stand der Technik*** *zu gewährleisten."*

Für die Zertifizierung der TI-Konnektoren wurden in Bezug auf das VSDM bislang zwei sog. Schutzprofile von der gematik in der Zusammenarbeit mit dem BSI entwickelt, nämlich BSI-CC-PP-0047-2015 sowie BSI-CC-PP-0097-2018, in denen die technischen Vorgaben für die TI-Konnektoren gemacht werden. Das vom BSI angewandte Prüf- und Zertifizierungssystem „Common Criteria“ (ISO/IEC 15408) für die Schutzprofile der TI-Konnektoren sieht Sicherheitsstufen beginnend mit der niedrigsten Stufe EAL1 und der höchsten Stufe EAL7 vor. Die für die TI-Konnektoren geltenden Schutzprofile BSI-CC-PP-0047-2015 und BSI-CC-PP-0097-2018 sehen jeweils die Stufe EAL3 vor. Diese Einstufung ist im Ergebnis zu niedrig und kann nur darauf zurückzuführen sein, dass das BSI bei der Einstufung nicht berücksichtigt hat, dass auch bereits im Rahmen des VSDM Gesundheitsdaten (Art.9 DSGVO) verarbeitet werden. Bei Gesundheitsdaten ist mindestens die Sicherheitsstufe EAL4 angemessen und erforderlich. Der Gesetzgeber hat mit der vorgenannten gesetzlichen Neuregelung (§ 306 Abs.3 und § 311 Abs.3 S.4 SGB V) zum 20.10.2020

nachgesteuert und auf das gesetzliche Defizit reagiert, dass gemäß der Rechtsprechung des Bundesverfassungsgerichts z.B. in seinem Urteil zur Vorratsdatenspeicherung aus (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08; NJW 2010, 833, Rn. 222-225) bei einer umfassenden Datenverarbeitung sensibler Daten der Gesetzgeber selbst bereits "ein besonders hohen Sicherheitsstandard" "in qualifizierter Weise" vorgeben muss. Das BSG hat in seiner aktuellen Entscheidung zur Telematikinfrastruktur und elektronischen Gesundheitskarte (Urteil vom 20.01.2021, B 1 KR 7/20 R) unter der dortigen Rz. 102/103 genau diese Rechtsprechung des BVerfG als Prüfungsmaßstab herangezogen und speziell das Vorratsdatenspeicherungs-Entscheidung des BVerfG zitiert. Auch nach Ansicht des BSG bedarf es somit insbesondere:

- *"Erforderlich sind **gesetzliche Regelungen**, die einen ausreichend **hohen Sicherheitsstandard in qualifizierter Weise** jedenfalls dem Grunde nach **normenklar und verbindlich** vorgeben." (Rz. 103)*

- *"Dabei ist sicherzustellen, dass sich dieser Standard - etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den **Stand der Technik** (vgl hierzu allgemein Ekrot/Fischer/Müller in Kipker, Cybersecurity, 1. Aufl 2020, Kap 3) - an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt." (Rz. 102)*

Unter Rz. 104 kam das BSG zum Ergebnis, dass die mit dem Patienten-Datenschutz-Gesetz ("PDSG") zum 20.10.2020 in Kraft getretenen Vorschriften zur Telematikinfrastruktur diesen verfassungsgerichtlichen Anforderungen gerecht werden. So heißt es:

> *"Die **mit dem PDSG neu gefassten und inhaltlich überarbeiteten Neuregelungen der §§ 291 ff SGB V** enthalten ein hinreichend normdichtes und klares Regelungsgefüge, das durch eine Vielzahl aufeinander und insbesondere auch mit den Vorgaben der DSGVO abgestimmter materiell-rechtlicher, organisatorischer und prozeduraler Maßnahmen der Datensicherheit dient (s dazu im Einzelnen oben 3. c), der der Gesetzgeber beim Auf- und Ausbau der TI eine "herausragende Rolle" beimisst (s oben bb <1>)."*

Auch der amtliche Leitsatz Ziff.2 zur vorgenannten BSG-Entscheidung stellt ausschließlich nur auf die neueren Vorschriften im Zuge des PDSG ab:

> *"2. Der Gesetzgeber hat **mit den durch das Patientendaten-Schutz-Gesetz (PDSG) neu gefassten Regelungen des SGB V** zur elektronischen Gesundheitskarte und zur Telematikinfrastruktur ausreichende Vorkehrungen zur Gewährleistung einer angemessenen Datensicherheit getroffen und ist*

dabei auch seiner Beobachtungs- und Nachbesserungspflicht nachgekommen."

Allerdings gehen diese gesetzlichen Sicherheitsvorgaben ins Leere, wenn die gematik und das BSI die TI-Konnektoren nicht nach einem hohen, sondern nur mittleren Sicherheitsstandard prüfen und zertifizieren. Diese geringen Sicherheitsanforderungen spiegeln sich auch in dem Schutzprofil inhaltlich konkret wider:

Das Schutzprofil BSI-CC-PP-0047-2015, Seite 25, erlaubt einen externen Fernwartungszugang auf den TI-Konnektor. Dort werden gleich zwei wesentliche Sicherheitsanforderungen, die heute für Fernwartungszugänge Stand der Technik sind, nicht gestellt, nämlich eine 2-Faktor-Authentisierung sowie einen VPN-Tunnel. Angesichts dieser zu niedrigen Sicherheitsanforderungen wäre die Zertifizierung eines TI-Konnektors nach dem Schutzprofil BSI-CC-PP-0047-2015 möglich, wenn ein Fernwartungszugang durch das freie Internet (ohne VPN-Tunnel) erfolgt und der Fernzugriff auf den Konnektor in der Arztpraxis / psychotherapeutischen Praxis dabei nur mit einem einfachen Passwort oder PIN (ohne Zwei-Faktor-Authentisierung) abgesichert ist. Dies entspricht nicht dem Stand der Technik und stellt einen Sicherheitsmangel dar.

Der Einsatz von Verschlüsselungstechniken ist für die Verarbeitung personenbezogener Daten allgemein in Art.32 Abs.1 lit.a DSGVO und vom deutschen Gesetzgeber insbesondere für Gesundheitsdaten in § 22 Abs.2 Ziff.7 BDSG vorgeschrieben. Die im Schutzprofil BSI-CC-PP-0047-2015 vorgesehenen Verschlüsselungstechniken („SHA-1“ sowie eine Entropie von 100 bit) genügen diesen Anforderungen nach heutigem Stand der Technik nicht mehr.
In dem Schutzprofil BSI-CC-PP-0047-2015 finden sich entgegen § 311 Abs.4 S.1 SGB V keine technischen Anforderungen zum Schutz der Patientendaten im IT-System der Arztpraxis / psychotherapeutischen Praxis. Das Schutzprofil adressiert ausschließlich den Schutz der Telematikinfrastruktur und des dortigen Datenverkehrs von außen, nicht aber den Schutz des Datenbestands in der Arztpraxis / psychotherapeutischen Praxis gegen IT-Angriffe aus bzw. über die Telematikinfrastruktur, obwohl der Schutz der in der Arztpraxis / psychotherapeutischen Praxis gespeicherten Patientendaten (Befunde, Krankheitsgeschichten, etc.) wesentlich wichtiger ist als die bloßen Versichertenstammdaten.

Angesichts der zahlreichen datenschutzrechtlichen Verstöße kann der jeweilige Arzt / Psychologische Psychotherapeut nicht verpflichtet sein, an der Datenverarbeitung im Zuge des VSDM als datenschutzrechtlich „Verantwortlicher“ (§ 307 Abs.1 SGB V) mitzuwirken. Der Arzt / Psychologische Psychotherapeut, somit auch der Kläger, wäre als datenschutzrechtlich Verantwortlicher nicht nur Teil einer rechtswidrigen Datenverarbeitung, sondern auch der finanziellen Haftung für

datenschutzrechtliche Verstöße gemäß Art.82 DSGVO sowie dem Bußgeldrisiko gemäß Art.83 DSGVO mit einem Bußgeldrahmen von bis zu 4% des Jahresumsatzes bzw. € 20 Mio. ausgesetzt. Das dieses Haftungsszenario nicht nur ein Scheinargument bzw. eine Schutzbehauptung der Ärzte ist, um den Aufwand einer Installation des TI-Konnektors in ihren Praxen zu umgehen, zeigt ein aktueller Fall vom März 2022. Der Bundesdatenschutzbeauftragte ("BfDI") musste im März 2022 im Rahmen des in Deutschland seit 2019 umfangreich eingesetzten TI-Konnektoren-Modells des Herstellers SECUNET eine Datenschutzrechtsverletzung dahingehend feststellen, dass Seriennummern der elektronischen Gesundheitskarten der jeweiligen Patienten in bestimmten Fällen innerhalb des TI-Konnektor-Geräts in Fehlerprotokollen gespeichert wurden, obwohl die einschlägigen Gerätespezifikationen der Gematik besagen, dass personenbezogene Daten in Protokolleinträgen innerhalb der Geräte nicht gespeichert werden dürfen. Die TI-Konnektoren dürfen diese Seriennummern nur lesen, nicht aber im Gerät speichern. Der BfDI bewertet in einer Veröffentlichung vom 09.03.2022 den Vorfall ausdrücklich als "Datenschutzrechtsverletzung":

> *"Liegt ein Datenschutzverstoß vor?*
> *Bei den gespeicherten Seriennummern der eGK-Zertifikate von gesperrten elektronischen Gesundheitskarten handelt es sich um personenbezogene Daten. Die Speicherung dieser Daten erfolgte ohne Rechtsgrund und ist somit unzulässig. Zudem ermöglicht allein die Speicherung im Konnektor einen (unbefugten) Zugang der Nutzenden beziehungsweise der von ihnen beauftragten Administratoren zu den gespeicherten Seriennummern der eGK-Zertifikate gesperrter Gesundheitskarten. Auf diese Weise wird die Möglichkeit eröffnet, dass diese Daten an Dritte weitergegeben werden können.* ***Somit liegt eine Datenschutzverletzung im Sinne des Art. 4 Nr. 12 DSGVO vor."***

BEWEIS: Inaugenscheinnahme der BfDI-Online-Veröffentlichung unter https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/01_FAQ-TI-Konnektoren.html

Der Vorfall schlug große Wellen, da bei einem Zusammenführen mit weiteren Daten konkrete Arztbesuche der jeweiligen Patienten hergeleitet werden können, so dass alle führenden Medien der Ärztebranche wie z.B. das Ärzteblatt und Medical Tribune, aber auch sonstige Medien wie z.B. das Handelsblatt hierüber berichteten. Der Aufschrei aus der Ärzteschaft galt dabei vor allem der Bewertung seitens des BfDI hinsichtlich der rechtlichen Verantwortlichkeit für die Datenschutzverletzung:

> *"Wer ist datenschutzrechtlich verantwortlich?*
> *Gemäß § 307 SGB V hat der Gesetzgeber festgelegt, dass die Datenverarbeitung in der Verantwortung derjenigen liegt, 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. ***Dabei handelt es sich um die Leistungserbringer, also beispielsweise die Praxen.***
Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hatte im Zuge des Gesetzgebungsverfahrens eine andere Lösung bevorzugt. Dazu hat die DSK am 12. September 2019 einen Beschluss veröffentlicht. Mit dem sogenannten Patientendatenschutzgesetz (PDSG) hat der Gesetzgeber aber seine durch Art.4 Nr.7 2. Halbsatz DSGVO eingeräumte Möglichkeit genutzt, die datenschutzrechtliche Verantwortung gesetzlich festzulegen. Diese Festlegung erfolgte abweichend vom Beschluss der DSK. Nach dem PDSG (§ 307 Abs.1 SGB V) sind daher die Nutzer der Komponenten der dezentralen Infrastruktur, also die Nutzer der Konnektoren, datenschutzrechtlich verantwortlich."

BEWEIS: Inaugenscheinnahme der BfDI-Online-Veröffentlichung unter https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/01_FAQ-TI-Konnektoren.html

Dieser Vorfall ist nun auch ein realer Beispielsfall für die klägerische Kritik, dass die TI-Infrastruktur, insbesondere die TI-Konnektoren und deren Anschluss an die Datensysteme der Arztpraxen nicht hinreichend reguliert und überwacht werden, und dass zu allem Überfluss die Ärzte nun auch noch von den Datenschutzbehörden für derartige datenschutzrechtliche Verstöße rechtlich verantwortlich gemacht werden, obwohl sie zur Benutzung der TI-Konnektoren gesetzlich verpflichtet wurden und diese Technologie im Vergleich zu der Gematik oder den jeweiligen Geräteherstellern am wenigsten überblicken können.

2. Verstoß gegen das Grundrecht auf Berufsfreiheit, Art.12 GG

Die derzeitige rechtliche und tatsächliche Umsetzung der gesetzlichen Vorschriften zur elektronischen Gesundheitskarte und zum TI-Konnektor insbesondere gemäß §§ 291b, 307 und 311 SGB V verletzt das Grundrecht der Ärzte / Psychologischen Psychotherapeuten und somit auch des Klägers aus Art.12 GG, weswegen der Kläger nicht zur Teilnahme am Versichertenstammdatenmanagement verpflichtet sein kann und für die bislang unterbliebene TI-Anbindung auch nicht sanktioniert werden darf.

Ansatzpunkt für des hiesigen Klageverfahrens ist nicht die Rechtsverteidigung gegen die Pflicht zum Versichertenstammdatenmanagement an sich, sondern die Rechtsverteidigung gegen die derzeitige konkrete datenschutzrechtliche und technische Umsetzung durch die gematik. Wie in Abschnitt 1 dieses Schriftsatzes konkret dargelegt wurde, begründet die jetzige rechtliche, organisatorische und technische Umsetzung zahlreiche datenschutzrechtliche Verstöße und es gibt umfangreiche konkrete Sicherheitsmängel.

Der derzeitige Zustand führt bei den Ärzten / Psychologischen Psychotherapeuten zu einem datenschutzrechtlich rechtswidrigen Zustand und zu erheblichen Gefährdungen der auf der elektronischen Gesundheitskarte gespeicherten Patientendaten und der im Praxisinformationssystem der Ärzte / Psychologischen Psychotherapeuten gespeicherten weiteren Gesundheitsdaten.

Der angegriffene Honorarbescheid in Gestalt des streitgegenständlichen Widerspruchsbescheids ist demnach insoweit aufzuheben.

_____

(- Unterschrift Kläger -)