Praxisadresse:

An die
Kassenärztliche Vereinigung

__.__.2021

Widerspruch gegen den
Bescheid über die Honorarkürzung infolge des nicht erfolgten
Anschlusses an die Telematikinfrastruktur für das Quartals ____/_____

Sehr geehrte Damen und Herren,

hiermit wird gegen den o.g. Bescheid für das Abrechnungsquartal __/____ vom ……2021 (Az. _____), zugegangen am ……2021,

W i d e r s p r u c h

eingelegt und beantragt,

den Honorarkürzungsbescheid für das Quartal _____/_____ aufzuheben.

B e g r ü n d u n g

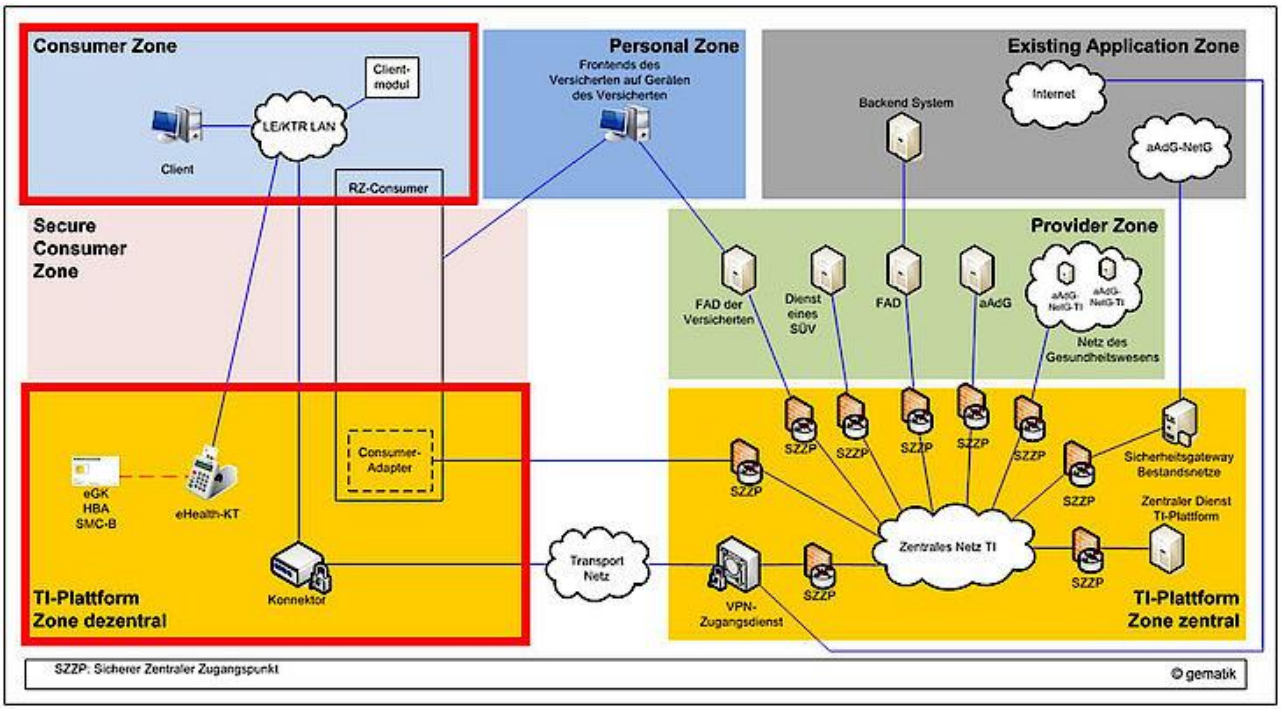
Der Widerspruch ist zulässig und begründet.

Der Honorarbescheid für das vorbezeichnete Abrechnungsquartal betreffend die Praxis des Widerspruchsführers ist – soweit es den pauschalen Abzug in Höhe von 2,5 Prozent des Gesamthonoraranspruch betrifft – aufzuheben, da die seitens des Gesetzgebers auferlegte Pflicht zur Durchführung des Versichertenstammdatenabgleichs (§ 291b Abs.2 SGB V n.F.) mit den derzeit von der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zugelassenen Telematik-Komponenten-Modellen für die verpflichteten Leistungserbringer, so auch den Widerspruchsführer, 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 Widerspruchsführer 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 Arztpraxis / psychotherapeutischen Praxis. Über die dezentrale Zone der TI, nämlich über den in der Arztpraxis / psychotherapeutischen Praxis zu installierenden Konnektor und das daran angeschlossene Kartenlesegerät, werden die auf der jeweiligen elektronischen Gesundheitskarte gespeicherten Daten eines jeden Patienten ausgelesen und an die zentrale Zone der TI zum Abgleich mit den bei der jeweiligen Krankenversicherung gespeicherten Daten weitergesandt, was eine Datenverarbeitung personenbezogener Daten im Sinne von Art.4 Ziff.2 DSGVO darstellt.



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 bereits gesundheitsbezogene Daten gespeichert und verarbeitet. Gemäß dem „Fachkonzept Versichertenstammdatenmanagement" der gematik und der „technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-L)" 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 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 bereits sogar Gesundheitsdaten in einem ganz erheblichen Umfang verarbeitet werden, ist die datenschutzrechtliche Verantwortlichkeit für die Telematikinfrastruktur nach wie vor ungeklärt:

Die fehlende Klärung der datenschutzrechtlichen Verantwortung hat entscheidende praktische Folgen: Einerseits die Unklarheit, wer für welche Bereiche der Telematikinfrastruktur die datenschutzrechtliche ex-ante-Sicherheitsbewertung in Form der Datenschutzfolgenabschätzung (Art.35 DSGVO) oder Meldungen bzw. Maßnahmen bei Datenpannen (Art.33, 34 DSGVO) vorzunehmen hat, andererseits, wer die Betroffenenrechte gemäß Art.12ff DSGVO zu erfüllen hat, z.B. anfängliche Informationspflichten bei Erhebung der Daten nach Art.13, Auskunftspflichten nach Art.15, Recht auf Löschung nach Art.17. Derzeit ist unklar, an wen sich der Patient wenden muss, wenn er erfahren will, welche Daten über ihn an welcher Stelle im Zuge der TI gespeichert werden und wenn er inhaltlich falsche Daten über sich löschen lassen möchte. Die augenblickliche tatsächliche Situation ist bezeichnend und genauso alarmierend: Obwohl es sich bei dem Versichertenstammdatenmanagement um eine der größten Datenverarbeitungen in Deutschland handelt, sind die Verantwortlichkeiten nicht rechtskonform geregelt und geklärt. Die Verletzung von datenschutzrechtlichen Vorschriften ist mit Beginn der Datenverarbeitung im Zuge des Versichertenstammdatenaustauschs seit 2019 eingetreten. Mit dem Verstoß gegen Art.5 DSGVO und gegen Art.26 Abs.1 S.2 DSGVO wird somit derzeit im Zuge des VSDM gegen höherrangiges Recht verstoßen.

Solange es keine wirksame Regelung zur datenschutzrechtlichen Verantwortlichkeit zum Versichertenstammdatenmanagement ("VDSM") gibt bzw. sich niemand als der „Verantwortliche" für eine Datenverarbeitung mit hinreichender Sicherheit bestimmen lässt, geschweige denn die daraus erwachsenden Pflichten erfüllt, läuft das gesamte Pflichtenregime der DSGVO ins Leere. Insbesondere die gematik hat diese Verantwortung bislang nicht anerkannt und auch die Pflichten des „Verantwortlichen" nicht erfüllt.

So hat die Datenschutzkonferenz (DSK - Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) einen Beschluss am 12.09.2019 dahingehend gefasst, dass sie zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematikinfrastruktur die Auffassung vertritt, dass die gematik für die zentrale Zone der Telematikinfrastruktur datenschutzrechtlich alleinverantwortlich und für die dezentrale Zone der TI datenschutzrechtlich mitverantwortlich ist. Ferner mahnte die

Datenschutzkonferenz an, dass der Umfang der Verantwortung der gematik für die dezentrale Zone einer gesetzlichen Regelung bedürfe, aber führte gleichzeitig aus, dass die gematik für die Verarbeitung verantwortlich sei, soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt sei (siehe DSK-Beschluss vom 12.09.2019, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zur_gematik.pdf).

Demgegenüber hat die Bundesregierung - entgegen der datenschutzrechtlichen Bewertung der Datenschutzkonferenz - im Zuge des Patientendatenschutzgesetzes zum 20.10.2020 eine gesetzliche Regelung in Form des § 307 SGB V n.F. dahingehend vorgenommen, dass die gematik gerade nicht als Verantwortlicher bzw. Mitverantwortlicher gelten soll. Dies ist mit Art.4 Nr.7 DSGVO nicht vereinbar.

Der Rechtsstandpunkt bezüglich der Mitverantwortlichkeit der gematik für die Datenverarbeitung über die Telematikinfrastruktur wurde auch während des Entstehungszeitraums des jetzigen Patientendatenschutzgesetzes vom Bundesdatenschutzbeauftragten in dem im Mai 2020 veröffentlichten Tätigkeitsbericht für 2019 auf den Seiten 26 und 27 wiederholt und somit aufrechterhalten. Dort heißt es:

> *"[…] Daher wurde die Klärung der Frage dringend notwendig, wer für die TI im Sinne der DSGVO datenschutzrechtlich verantwortlich ist. Diese Frage habe ich intensiv mit meinen Kolleginnen und Kollegen in den Ländern erörtert. Die DSK hat daraufhin am 12. September 2019 befunden, dass die gematik GmbH eine datenschutzrechtliche Mitverantwortung für die TI trägt, weil sie mit ihren Vorgaben und Festlegungen Mittel und Zweck für die Datenverarbeitung in der TI bestimmt […]"*

Auch wird nochmals die Mitverantwortlichkeit (Art.26 DSGVO) der gematik für die dezentrale Zone zusammen mit den Leistungserbringern ausdrücklich genannt:

> *"[…] Insbesondere für den Betrieb der Konnektoren sind aber auch die Leistungserbringer mitverantwortlich, insofern sie gewisse Sorgfaltspflichten zu erfüllen haben und auf Dauer diese Konnektoren auch für die sichere Übermittlung von Patientendaten nutzen werden […]"*

(siehe: Tätigkeitsbericht des BfDI für 2019, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/28TB_19.html)

Dass die jetzige Regelung in § 307 SGB V n.F. auch vom Bundesrat nicht für DSGVO-konform erachtet wird, zeigt die Stellungnahme des Bundesrates zum Patientendatenschutzgesetz nebst Gegenäußerung der Bundesregierung, (siehe Drucksache 19/19365 vom 20.05.2020, Seiten 4-7 und 25). Insbesondere kritisierte der Bundesrat die vorgesehene Regelung, dass die gematik nur als "*verantwortungsfreier Vermittlungsdienst*" dargestellt wird, während nach Auffassung des Bundesrats die datenschutzrechtliche Verantwortlichkeit für die Telematikinfrastruktur bei der gematik anzusiedeln ist, nämlich aufgrund der Tatsache, dass sie konkret Vorgaben erteilt, und aufgrund ihrer organisierenden und koordinierenden Funktion. Dies macht die gematik nach Auffassung des Bundesrats unter Bezugnahme auf das EuGH-Urteil vom 10.07.2018 Az. C-25/17 zum datenschutzrechtlich Verantwortlichen im Sinne von Art.4 Nr.7 DSGVO, darüber hinaus begründet dies auch eine gemeinsame datenschutzrechtliche Verantwortlichkeit der gematik mit den in § 307 SGB V genannten Anbietern.

Soweit die Bundesregierung in der vorgenannten Gegenäußerung (Drucksache 19/19365 Seite 25) dem Bundesrat widerspricht, dass kein Fall der gemeinsamen datenschutzrechtlichen Verantwortlichkeit vorläge, da ja § 4 Nr.7 DSGVO eine konkrete gesetzliche Zuweisung der Verantwortlichkeiten durch den nationalen Gesetzgeber erlaube, die nun in Form des § 307 SGB V n.F. erfolge, wird hierbei von der Bundesregierung übersehen, dass eine derartige gesetzliche Zuweisung von Verantwortlichkeiten durch nationales Recht zwar möglich ist, aber im Einklang mit der DSGVO nur dann stehen, 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).

Der Bundesrat argumentiert in seiner Stellungnahme:

"Die gematik bestimmt im Rahmen ihrer Aufgabenzuweisung sehr wohl mit über die Zwecke und Mittel der Datenverarbeitung. Durch diese wird nicht nur die Telematikinfrastruktur errichtet, sondern die Gesellschaft bestimmt auch die Maßnahmen zur Umsetzung der technischen und organisatorischen Anforderungen

nach Artikel 32 DSGVO. Durch die Zuweisung von technischen Hilfsdiensten, wie das Betreiben eines Netzes, die technische Umsetzung von Zugangsdiensten und Diensten der Anwendungsinfrastruktur an andere Stellen kann diese datenschutzrechtliche Verantwortlichkeit der Gesellschaft für Telematik nicht pauschal verneint werden. 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" (Stellungnahme des Bundesrats, Drucksache 19/19365 vom 20.05.2020, Seite 5f).

Der Bundesrat führt zudem aus:

"Es mag sein, dass die Diensteanbieter bestimmte technische Anforderungen erfüllen können. Die alleinige Setzung eigener Zwecke ist aber nicht erkennbar. Die technische Infrastrukturverantwortung ist gerade der Gesellschaft für Telematik zugewiesen. Diese würde sich jeglicher Haftung (Artikel 82 DSGVO) zum Nachteil betroffener Personen entziehen, wenn diese schlicht festlegt, dass bestimmte Dienste durch „eigenverantwortliche Diensteanbieter" erbracht werden. Die Tätigkeit der Gesellschaft für Telematik ist nicht lediglich auf einen bloßen Vermittlungsdienst beschränkt („Koordinierungsstelle"). Vorliegend kommt entgegen der Darstellung in dem Gesetzentwurf einerseits eine Auftragsverarbeitung der technischen Dienstleister für die Gesellschaft für Telematik in Betracht. Verwiesen sei dabei auf das Papier der Artikel 29-Datenschutzgruppe, Stellungnahme zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter", WP 169, Seite 13, Beispiel 1, wonach der Anbieter von Telekommunikationsdiensten allenfalls im Hinblick auf die Verarbeitung von Verkehrs- und Rechnungsdaten als Verantwortlicher eingestuft werden kann. Ferner wird im gleichen Papier WP 169, Seite 29 auf Beispiel 15 verwiesen, wonach für die Einrichtung einer Plattform für die Verwaltung von Gesundheitsdaten auch eine gemeinsame Verantwortlichkeit der Beteiligten in Betracht kommt. 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. Hierzu genügt gerade nicht die bloße Erteilung

allgemeiner Informationen (vgl. § 307 Absatz 5 SGB V) durch die Gesellschaft für Telematik und der Verweis auf andere beteiligte Stellen und „Zuständigkeiten". 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." (Stellungnahme des Bundesrats, Drucksache 19/19365 vom 20.05.2020, Seite 6)

Zwischenergebnis:
Die neue gesetzliche Regelung in § 307 SGB V zu den datenschutzrechtlichen Verantwortlichkeiten ist somit als Verstoß gegen höherrangiges EU-Recht, nämlich Art.4 Nr.7 DSGVO, gewertet werden. Somit ist weiterhin von einer fehlenden Zuweisung der datenschutzrechtlichen Verantwortlichkeiten auszugehen, was wiederum entsprechende Verstöße gegen Art. 5 Abs.1, 2, Art. 24 Abs.1 und Art. 26 Abs.1 S.2 DSGVO begründet.

Darüber hinaus sind weitere Verstöße gegen die DSGVO festzustellen:

Gemäß Art.35 DSGVO hätte eine Sicherheitsbewertung in Form einer sog. Datenschutzfolgenabschätzung („DSFA") vor Beginn der im Zuge des VSDM stattfindenden Datenverarbeitung zwingend erfolgen müssen, was auch seitens des Bundesdatenschutzbeauftragten gegenüber der gematik eingefordert wurde. Eine DSFA liegt seitens der gematik jedoch derzeit weder für die zentrale Zone der Telematikinfrastruktur vor, noch für die dezentrale Zone, also somit auch nicht für den TI-Konnektor und die Datenverarbeitung im Zuge des VSDM vor. Mit diesem Verstoß gegen Art.35 DSGVO wird derzeit im Rahmen 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 § 311 Abs.1 Ziff.1 lit.a., Abs.2 und Abs.6 SGB V n.F. (§ 291b Abs.1 S.1 Ziff.3 sowie Abs.1a S.6 SGB V a.F.) durch die bereits anfänglichen technischen Vorgaben seitens gematik und dem BSI Bundesamt für Sicherheit in der Informationstechnik („BSI") verletzt. 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.

Entgegen Art.5 Abs.1 lit.f, Art.24 Abs.1 S.2, Art.32 Abs.1 lit.d DSGVO fehlt es zudem an den gesetzlich erforderlichen Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, allein schon aufgrund des Umstands, dass es an Vorgaben für eine regelmäßige Wartung und deren Überprüfung der TI-Konnektoren fehlt, so dass bereits jetzt nachweislich veraltete, nicht gewartete Open-Source-Softwarestände in den TI-Konnektoren verwendet werden, die bekannte Sicherheitsmängel aufweisen.

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 SGB V n.F. (§ 291b Abs.1 S.4 SGB V a.F.) 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.

Auch mit der fehlenden Regulierung und Überprüfung der Installation der TI-Konnektoren wird derzeit im Zuge des VSDM gegen höherrangiges Recht, nämlich gegen Art.5 Abs.1 lit.f, Art.24 Abs.1 S.2, Art.32 Abs.1 DSGVO verstoßen, ferner gegen das verfassungsrechtliche Bestimmtheitsgebot mangels hinreichender gesetzlichen Regelungen hierzu.

Angesichts der zahlreichen datenschutzrechtlichen Verstöße kann der jeweilige Arzt / Psychologische Psychotherapeut nicht verpflichtet sein, an der Datenverarbeitung im Zuge des VSDM als datenschutzrechtlich „Mitverantwortlicher" (Art.26 DSGVO) mitzuwirken. Der Arzt / Psychologische Psychotherapeut, somit auch der Widerspruchsführer, wäre als datenschutzrechtlich Mitverantwortlicher nicht nur Teil einer rechtswidrigen Datenverarbeitung, sondern auch der finanziellen Mithaftung für datenschutzrechtliche Verstöße gemäß Art.82 Abs.4 DSGVO sowie dem Bußgeldrisiko gemäß Art.83 DSGVO mit einem Bußgeldrahmen von bis zu 4% des Jahresumsatzes bzw. € 20 Mio. ausgesetzt, denn z.B. bereits die fehlende Vereinbarung im Sinne von Art.26 Abs.1 S.2 DSGVO erfüllt den Bußgeldtatbestand.

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 gemäß §§ 311 SGB V verletzt das Grundrecht der Ärzte / Psychologischen Psychotherapeuten und somit auch des Widerspruchsführers aus Art.12 GG, weswegen der Widerspruchsführer

nicht zur Teilnahme am Versichertenstammdatenmanagement verpflichtet sein kann und für die bislang unterbliebene TI-Anbindung auch nicht sanktioniert werden darf.

Ansatzpunkt für den hiesigen Widerspruch 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 Bescheid ist demnach insoweit aufzuheben.

Mit freundlichen Grüßen