Bleibtreustraße 24
10707 Berlin (Deutschland)
Telefon (030) 887 086-36
Telefax (030) 887 086-37

E-Mail info@medi-geno-deutschland.de
www.medi-geno-deutschland.de

MEDI GENO Deutschland e.V. ● Bleibtreustr. 24 ● 10707 Berlin

An den
Bundesbeauftragten für den Datenschutz und die
Informationsfreiheit

Berlin, 12.04.2019

Eilt! Bitte sofort vorlegen!

Datenschutzrechtliche Beschwerde zur Einführung des „TI-Konnektors“ im Gesundheitswesen

Sehr geehrter Bundesbeauftragte für Datenschutz und Informationsfreiheit,

wir sind ein Landesverband des MEDI GENO Deutschland e.V., der die politischen und wirtschaftlichen Interessen seiner Mitglieder vertritt. Der MEDI GENO Deutschland e.V. und seine angeschlossenen Mitgliedsorganisationen verfügen bundesweit über ca. 15.000 Mitglieder.

Hintergrund unserer datenschutzrechtlichen Beschwerde ist die für Ärzte zwingende Einführung des sog. TI-Konnektors zum 30.06.2019, einer steuernden IT-Komponente in den Arztpraxen im Rahmen der Telematikinfrastruktur gemäß § 291a SGB V zur zentralen Kommunikationsinfrastruktur für das Gesundheitswesen. Die Telematikinfrastruktur soll eine sichere Verbindung zum Datenaustausch zwischen Krankenkassen, Arztpraxen, Krankenhäusern und Apotheken herstellen. In der ersten Ausbaustufe des zukünftigen Datenaustauschs sollen - beginnend - zum 01.07.2019 die Versichertenstammdaten zwischen der Arztpraxis und der jeweiligen Krankenversicherung abgeglichen werden (sog. Versichertenstammdatenmanagements, „VDSM“). Die technische Organisation und der Betrieb der Telematikinfrastruktur ist gemäß § 291b SGB V der gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Friedrichstraße 136, 10117 Berlin übertragen worden.

Wir stellen an dieser Stelle klar, dass sich diese datenschutzrechtliche Beschwerde nicht gegen das gesetzgeberische Vorhaben als solches oder die Tätigkeit des BSI - Bundesamt für Sicherheit in der Informationstechnik richtet, sondern gegen Einzelheiten der datenschutzrechtlichen Umsetzung, die auch die technische Umsetzung in Arztpraxen, Krankenkassen, Kliniken, Apotheken etc. im hiesigen Bundesland betrifft (weswegen wir auch von Ihrer sachlichen und örtlichen Zuständigkeit ausgehen).

Wir sind der Ansicht,

1. dass es entgegen Art. 35 DSGVO an der erforderlichen Datenschutzfolgenabschätzung für den Datenaustausch unter Nutzung der sog. TI-Konnektoren und der Telematikinfrastruktur fehlt und

2. dass entgegen Art. 26 DSGVO an den erforderlichen Vereinbarungen zwischen den gemeinsam Verantwortlichen innerhalb der Telematikinfrastruktur fehlt.

Wir fordern Sie im Rahmen dieser Beschwerde auf, die Nutzung der Telematikinfrastruktur für den Versichertenstammdatenaustausch mit Hilfe des sog. TI-Konnektors zu untersagen, solange die vorgenannten datenschutzrechtlichen Anforderungen nicht erfüllt sind.

Im Einzelnen:

1. Zum gesetzlichen Hintergrund:

Gemäß § 291 Abs.1 SGB V stellen die gesetzlichen Krankenversicherungen ihren Versicherten eine elektronische Gesundheitskarte aus, welche die Angaben gemäß § 291 Abs.2 SGB V enthält. Die Krankenkassen sind gemäß § 291a SGB V verpflichtet, Dienste anzubieten, welche es den Leistungserbringern (Ärzten, Heilpraktikern etc.) ermöglichen, die Gültigkeit und die Aktualität der auf der elektronischen Gesundheitskarte gespeicherten Daten zu überprüfen und gegebenenfalls anzupassen. Diese Überprüfung soll onlinebasiert stattfinden und wird durch die einzurichtende Telematikinfrastruktur sichergestellt (§ 291 Abs.2b SGB V). Nach der Regelung des § 291 Abs.2b S.2 SGB V sind Vertragsärzte künftig dazu verpflichtet sein, bei der erstmaligen Inanspruchnahme von Behandlungsleistungen durch den Versicherten im jeweiligen Quartal der Leistungserbringung die Angaben auf der Gesundheitskarte durch Benutzung der Telematikinfrastruktur zu überprüfen.

Um die vorgenannte Überprüfung der Leistungspflicht durchführen zu können, verpflichtet der Gesetzgeber die Vertragsärzte nach § 291 Abs.2b S.4 SGB V dazu, den Online-Abgleich und die Online-Aktualisierung der auf der elektronischen Gesundheitskarte gespeicherten Daten sicherzustellen.

Den ersten Schritt im Zusammenhang mit der Einführung der Telematikinfrastruktur stellt die Anwendung des sogenannten Versichertenstammdatenmanagements (VSDM) dar (Daten nach § 291 Abs.2 Nr.1-10 SGB V). Die Versichertenstammdaten entstehen aus dem Versicherungsverhältnis zwischen Versichertem und Kostenträger. Die Kartenpersonalisierung sowie die Ausgabe der elektronischen Versicherungskarte an den Versicherten erfolgt über die Kostenträger (§§ 284, 291 SGB V).

Zum Abgleich der Daten und zum Anschluss an die Telematikinfrastruktur muss in der Arztpraxis künftig ein sog. TI-Konnektor eingesetzt werden. Die Vertragsärzte wurden gesetzlich dazu verpflichtet, bis zum 31.03.2019 einen TI-Konnektor zu bestellen und diesen bis zum 30.06.2019 zu installieren. Zunächst wurde die Anschaffungspflicht bis zum 31.12.2018 normiert. Diese Frist wurde vom Gesetzgeber auf den 31.03.2019 verschoben.

2. Nichterfüllung datenschutzrechtlicher Anforderungen:

Es bestehen erhebliche datenschutzrechtliche Bedenken in Bezug auf den Einsatz und den Datenaustausch mit Hilfe des TI-Konnektors, weshalb wir Sie hiermit zum Tätigwerden auffordern.

a) Notwendigkeit einer Datenschutzfolgenabschätzung

Nach Art. 35 Abs. 1 DS-GVO ist eine solche Datenschutzfolgenabschätzung immer dann vorzunehmen, wenn eine *„Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“* hat. In Art. 35 Abs. 3b DS-GVO wird zudem geregelt, dass eine Datenschutzfolgenabschätzung insbesondere dann vorzunehmen ist, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten vorgenommen wird.

In der ersten Rollout-Phase (VSDM) der Telematikinfrastruktur sollen nach Angaben der gematik zunächst die gemäß § 291 SGB V auf der elektronischen Gesundheitskarte gespeicherten Daten übertragen und abgeglichen werden. Hierbei handelt es sich um folgende Daten:

aa) Die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat,

bb) den Familiennamen und Vornamen des Versicherten,

cc) das Geburtsdatum des Versicherten,

dd) das Geschlecht des Versicherten,

ee) die Anschrift des Versicherten,

ff) die Krankenversicherungsnummer des Versicherten,

gg) den Versichertenstatus, für Personengruppen nach § 264 Abs. 2 SGB V den Status der auftragsweisen Betreuung,

hh) den Zuzahlungsstatus des Versicherten,

ii) den Tag des Beginns des Versicherungsschutzes,

jj) bei befristeter Gültigkeit der elektronischen Gesundheitskarte das Datum des Fristablaufs.

In § 291 Abs.2 Nr.7 SGB V wird darüber hinaus auf den § 264 Abs.2 SGB V verwiesen, also die Vorschrift „Versichertenstatus, für Personengruppen nach § 264 Abs.2 der Status der auftragsweisen Betreuung“. Gemäß § 264 Abs.4 S.3 und 4 SGB V gilt als Versicherungsstatus die Statusbezeichnung „Mitglied“, „Rentner“ oder „Familienversicherter“. Der Status der auftragsweisen Betreuung nach § 264 Abs. 2 kann die Werte „SGB XII“, „Asylbewerberleistungsgesetz“ und „Krankenhelfer“ haben.

Die tatsächlich auf der elektronischen Gesundheitskarte speicherbaren Daten zum Versichertenstatus ergeben sich aber aus untergesetzlichen Normen, namentlich aus dem „Fachkonzept Versichertenstammdatenmanagement“ der gematik und aus der „technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-L)“. Gesetzliche Grundlage für den Erlass der technischen Normen sind § 291 b Abs.1 Nr.2 und §§ 291 Abs.3, 87 Abs.1 S.2 SGB V. In den beiden technischen

Spezifikationen ist unter anderem geregelt, dass auf der EGK ein „DMP-Kennzeichen“ gespeichert wird, das folgende Werte haben kann:

- Diabetes Mellitus Typ 2
- Brustkrebs
- Koronare Herzkrankheit
- Diabetes Mellitus Typ 1
- Asthma Bronchiale
- COPD

siehe: „Fachkonzept Versichertenstammdatenmanagement“, Seite 43, abrufbar unter

https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Fachanwendungen/gematik_VSD_Fachkonzept_VSDM_V270.pdf

Bei gespeicherten Daten zu diesen chronischen Erkrankungen handelt es sich zweifellos um besondere personenbezogene Daten im Sinne von Art.9 Abs.1 DSGVO. Gerade die vorgenannten DMP-Zeichen und die daraus ersichtlichen Informationen über chronische Erkrankungen des betroffenen Patienten können ganz eindeutig als Score-Wert gegen die Interessen des Betroffenen verwendet werden. Die Eintrittswahrscheinlichkeit und der Schaden der Rechte und Freiheiten im Sinne von Art.35 DSGVO würde in diesem Fall ein hohes Risiko für die Betroffenen bedeuten.

Aber auch aus weiteren Gründen ist eine Datenschutzfolgenabschätzung rechtlich zwingend geboten: Die Telematikinfrastruktur stellt die „Verwendung neuer Technologien“ dar, die angesichts der sensiblen Daten und der hunderttausenden von involvierten Nutzern der Telematikinfrastruktur (Ärzte, Kliniken, Krankenversicherungen, Apotheker, etc.) ein hohes Sicherheitsrisiko für die betroffenen Patienten, aber auch die Integrität der jeweiligen IT-Systeme und Datenbestände der Nutzer darstellen.

Aus den “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” (WP 248, Stand 04.04.2017) sind zahlreiche Kriterien wie “Scoring”, “Automatisierte Einzelentscheidung (mit Rechtswirkung)”, Sensitive Daten”, “Umfangreiche Daten”, “Besonders schutzwürdige Betroffene” und “Neue Technologien/Verarbeitungen” erfüllt. Nach Ansicht der Artikel-29-Gruppe reicht bereits die Erfüllung von zwei Kriterien, damit im Regelfall von einer Pflicht zur Durchführung einer Datenschutzfolgenabschätzung auszugehen ist.

Zwischenergebnis: Bereits in der ersten Ausbaustufe („Rollout-Phase“), dem Versichertenstammdatenmanagements (2019), werden umfangreiche personenbezogenen Daten im Sinne von Stammdaten und teilweise sogar besondere personenbezogene Daten im Sinne von Art.9 Abs.1 DSGVO verarbeitet werden, weshalb eine Datenschutzfolgenabschätzung bereits - auch unter diesem Gesichtspunkt - vor der Einführung der ersten Rollout-Phase notwendig ist. Die Datenschutzfolgenabschätzung erfüllt die Funktion eines „Frühwarnsystems“, in dem eine konkret beabsichtigte Verarbeitung vorab auf ihre datenschutzrechtliche Konformität überprüft wird (Ehmann/Selmayr/Baumgartner Datenschutzgrundverordnung Art. 35 Rn.2). Dem liegt auch der Gedanke

zugrunde, dass neuartige Technologien von Anfang an datenschutzfreundlich zu gestalten sind („Privacy by design“ Art. 25 DS-GVO). Sofern also sämtliche Leistungsbringer dazu verpflichtet werden, einen TI-Konnektor an ihre interne Infrastruktur anzubinden, so muss eine datenschutzkonforme Sicherheit der Infrastruktur von Anfang an gewährleistet sein.

b) Gleichwohl ist uns bislang die Durchführung einer Datenschutzfolgenabschätzung nicht bekannt. Aus unserer Sicht sind nur die gematik und die weiteren technischen Provider der Komponenten für die Telematikinfrastruktur in der Lage, die erforderliche Datenschutzfolgenabschätzung vorzunehmen. Die gemäß § 291b SGB V gesetzlich festgelegte Zuständigkeit der gematik macht sie nach unserer Rechtsauffassung auch zur datenschutzrechtlich Verantwortlichen, so dass die Verantwortung für die Durchführung der Datenschutzfolgenabschätzung in erster Linie bei der gematik liegt. Denn die gematik beschreibt sich selbst dahingehend, dass sie den Betrieb der Telematikinfrastruktur koordiniert und die Gesamtverantwortung trägt, siehe z.B. unter: **https://www.gematik.de/ueber-uns/**. An anderer Stelle spricht die gematik gar davon die „Betriebsverantwortung“ für die Telematikinfrastruktur innezuhaben, siehe **https://gmds.de/fileadmin/user_upload/.../140907_Beirat_GMDS_Vortrag_Elmer.pdf** .

Die gematik hat datenschutzrechtliche Ausführungen zur Telematikinfrastruktur und zum TI-Konnektor bereits im September 2016 veröffentlicht, siehe „White Paper-Datenschutz und Informationssicherheit“, Seite 16, abrufbar unter

https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_whitepaper_web_Stand_270916.pdf. Die gematik sieht sich also auch selbst in der datenschutzrechtlichen Verantwortung für die Telematikinfrastruktur. Die vorgenannte Veröffentlichung („White Paper“) ersetzt jedoch keine Datenschutzfolgenabschätzung und umfasst insbesondere auch nicht die datensicherheitsrechtliche Bewertung der TI-Konnektoren in den Arztpraxen.

Dass die Ärzte (bzw. die sonstigen sog. Leistungserbringer des Gesundheitswesens) keine datenschutzrechtliche Verantwortlichkeit für den TI-Konnektor und die weitere Telematikinfrastruktur haben, wird nicht nur von der gematik so gesehen, sondern auch durch den Bundesdatenschutzbeauftragten, siehe dazu veröffentlichte Schreiben der Bundesbeauftragten für Datenschutz und die Informationsfreiheit, Herr Walter Ernestus, vom 14.06.2018 und 19.07.2018 an die gematik sowie den Hartmannbund Verband der Ärzte Deutschlands e.V. , abrufbar unter:

https://www.hartmannbund.de/fileadmin/user_upload/Downloads/Sonstiges/2018-07_BDSB-DSB_DFA_TI.pdf

Übereinstimmend mit der Einschätzung des Bundesdatenschutzbeauftragten nutzt auch nach eigener Aussage der gematik jeder Leistungserbringer (Ärzte, Heilpraktiker etc.) seine betriebenen Praxissysteme in eigener Verantwortung. Die Verantwortung der Ärzte endet jedoch beim Konnektor, schließt diesen nicht ein. Dies bedeutet, dass nach Auffassung der gematik die einzelnen Ärzte ausschließlich für eine sichere IT-Infrastruktur innerhalb der Praxis zuständig sind. Alles was darüber hinaus über den TI-Konnektor an Daten verarbeitet wird, liegt also nicht mehr im Verantwortungsbereich der Ärzte. Schlussendlich bedeutet dies aber für die Ärzte, dass sie ihre internen Systeme an eine Infrastruktur anbinden müssen, auf deren Sicherheit sie keinerlei Einfluss haben. Nach unseren Recherchen gibt es zwar sog. Schutzprofile für die TI-Konnektoren, die als verbindliche Zertifizierungsvorgaben vom BSI erarbeitet wurden. Wir haben unter Hinzuziehung von Experten die aktuell einschlägigen Schutzprofile PP-0097 und -0098 auf konkrete Schutzmaßnahmen für die Arztpraxen hin überprüft, sind aber nicht fündig geworden. Auf unsere Anfrage hin erhielten wir vom BSI mit Schreiben vom 25.02.2019 die

Auskunft, dass der Schutz der Arztpraxen ganz wesentlich von der Konfiguration des Konnektors vor Ort abhinge. Ob es hierzu verbindliche Konfigurationsvorgaben für die Konnektoren-Hersteller und -Dienstleister seitens der gematik gibt, ist uns nicht bekannt. All dies sind aber Fragen, die im Rahmen einer Datenschutzfolgenabschätzung zur Bewertung der Datensicherheit zu klären wären.

Die sog. Leistungserbringer (Ärzte, Heilpraktiker etc.) verfügen in der Regel über eine große Anzahl an sog. besonderen personenbezogenen Daten im Sinne des Art.9 Abs.1 DSGVO. Daher muss ein hoher Maßstab an die Sicherheit der Verarbeitung der Daten gelegt werden. Zudem haben die Ärzte strafrechtlich gemäß § 203 StGB für die Geheimhaltung dieser Daten einzustehen. Bevor die Leistungserbringer mit dem TI-Konnektor die praxiseigenen IT-Systeme mit der Telematikinfrastruktur verbinden, muss die Sicherheit der Telematikinfrastruktur und der TI-Konnektoren geklärt sein. Hierzu gehört auch eine Datenschutzfolgenabschätzung. Nur dann können wiederum die Leistungserbringer und deren IT-Berater ihrerseits bewerten, inwieweit die Sicherheit der eigenen IT-Systeme und Datenbestände durch den TI-Konnektor gefährdet sind, also ob der TI-Konnektor überhaupt eine verlässliche „Sicherheitsschleuse“ ins Internet ist oder „Hackern“ einen schlecht geschützten Zugang zu den praxiseigenen IT-Systemen und dortigen Datenbeständen bieten. Davon hängt auch ab, ob und in welchem Umfang der jeweilige Arzt in seiner Praxis weitere interne IT-Schutzmaßnahmen vornehmen muss oder ob er auf den TI-Konnektor vertrauen darf.

Neben den gefährdeten praxiseigenen IT-Systemen und Datenbeständen der Leistungserbringer besteht auch ein erhebliches Risiko bei der Verarbeitung der direkt auf der elektronischen Gesundheitskarte zusätzlich gespeicherten Patientendaten, bei denen der jeweilige Patient nach der derzeitigen Rechtslage freiwillig entscheiden kann, ob diese auf der Karte gespeichert werden sollen.

c) Die aus unserer Sicht bislang nur unvollständige datenschutzrechtliche Bewertung der Verantwortlichkeiten sowie der Datensicherheit in Bezug auf den TI-Konnektor wird erhebliche Auswirkungen für die Praxis haben. Sofern durch einen Hacker-Angriff aus der Telematikinfrastruktur in die IT-Systeme einer Arztpraxis Patientendaten freigesetzt werden, ist nach dem derzeitigen Stand für den betroffenen Arzt völlig unklar, welche Maßnahmen er vornehmen müsste (ganz zu schweigen von der datenschutz- und strafrechtlichen Haftung für die Datenpanne und die anschließende Unterlassung eventuell notwendiger Maßnahmen). Vor allem wird für den Arzt - selbst bei Hinzuziehung von IT-Experten - in aller Regel die Überprüfung nicht möglich sein, ob der TI-Konnektor bzw. die Telematikinfrastruktur das ursächliche Sicherheitsrisiko für den Angriff darstellte.

Nach unserem Wissensstand haben weder die gematik noch die Konnektoren-Hersteller hierfür Handlungsanweisungen vorgesehen, die z.B. die Überprüfung des Vorfalls, die Trennung der Praxissysteme von der Telematikinfrastruktur oder die Änderung der Konnektoren-Konfiguration vorsehen. Derartige Notfallkonzepte sind dagegen fester Bestandteil, um die Sicherheit der Datenverarbeitung im Sinne von Art. 32 DSGVO sicherzustellen.

Da die Ärzte keinen Einfluss auf die Konfiguration der Konnektoren nehmen können und dürfen, ist es die Aufgabe der gematik, im Rahmen der Datenschutzfolgenabschätzung diese Szenarien dahingehend zu bewerten, ob und ggf. welche Handlungsanweisungen für die Bewältigung dieser Situationen gemacht werden müssen.

Ergebnis: Im Rahmen der Einführung des TI-Konnektors ist also eine durch die gematik zu erstellende Datenschutzfolgenabschätzung gemäß Art.35 DSGVO durchzuführen, um Sicherheitsrisiken für die personenbezogenen Daten eindämmen zu können. Dies ist nach unserem Kenntnisstand bisher nicht

geschehen, insbesondere trotz der unübersehbaren Aufforderung des Bundesdatenschutzbeauftragten an die gematik vom 14.06.2018 (abrufbar unter **https://www.hartmannbund.de/fileadmin/user_upload/Downloads/Sonstiges/2018-07_BDSB-DSB_DFA_TI.pdf**).

2. Gemeinsame Verarbeitung Art.26 DS-GVO

Wir sehen in der Telematikinfrastruktur mit allen involvierten Komponenten, insbesondere nun den TI-Konnektoren, eine Datenverarbeitung, deren Zwecke und Mittel von mehreren Verantwortlichen gemeinsam im Sinne von Art.26 DSGVO festgelegt werden. Neben der gematik sind die Krankenkassen sowie die technischen Provider der IT-Komponenten/Dienstleistungen involviert. Neben den TI-Konnektoren sind eine SMC-B-Karte (ausgestellt von der Bundesdruckerei), ein dazu passendes Kartenterminal zum Einlesen der Karte und als Dienstleistung ein VPN-Zugangsdienst erforderlich. Trotzdem wurden nach unserer Kenntnis entgegen Art.26 DSGVO keine entsprechenden Joint-Controllership-Vereinbarungen abgeschlossen.

Zur gemeinsamen Verantwortlichkeit ist in mehreren bedeutenden Entscheidungen des EuGH klargestellt worden, was hierunter zu verstehen ist:

In der Entscheidung des EuGH zu den Facebook-Fanpages (EuGH, Urteil vom 05.06.2018 – C-210/16) wurde für die Annahme einer „gemeinsamen Verantwortlichkeit“ für ausreichend erachtet, wenn ein Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung geleistet wird. Diesen Beitrag leisten die Fanpage-Betreiber dadurch, dass sie eine sogenannte Facebook-Fanpage einrichten und somit eine Datenverarbeitung seitens Facebook überhaupt erst ermöglichen.

Nach den Ausführungen des EuGH erfordert eine „gemeinsame Verantwortlichkeit“ keine gleichwertige Verantwortlichkeit. Es reicht also aus, dass der Fanpage-Inhaber dazu beiträgt, dass die Daten überhaupt erst erhoben werden können und auch die Möglichkeit hat, die erhobenen Daten – wenn auch anonymisiert – auszuwerten. Der EuGH stellt in der Entscheidung auch klar, dass die vorwiegende Verantwortlichkeit zwar bei Facebook zu sehen ist, dass es jedoch nicht auf eine gleichwertige Verantwortlichkeit ankommt.

Ähnlich gestalten sich die Anwendung des TI-Konnektors und die Zusammenarbeit der gematik, den technischen Providern der dazu erforderlichen Komponenten und den Krankenkassen:

Die Krankenkassen haben ein eigenes Interesse am Datenabgleich, um ihre Abrechnungsvorgänge und sonstigen Bearbeitungsprozesse zu vereinfachen, indem bei Beginn einer ärztlichen Behandlung bereits geklärt wird, inwieweit Versicherungsschutz besteht und ob eventuelle Zuzahlungspflichten bestehen. Die Krankenkassen haben zwar keine Kenntnisse von der Funktionsweise und Sicherheit des TI-Konnektors und der weiteren Telematikinfrastrukturkomponenten, allerdings kommt es entsprechend der EuGH-Rechtsprechung zu den Facebook-Fanpages hierauf gerade nicht an. Die Inhaber der Facebook-Fanpages haben noch weniger einen Einblick in die genauen technischen und organisatorischen Abläufe der Datenverarbeitung durch Facebook, als dies bei den Krankenkassen und der Telematikinfrastruktur ist.

In einem weiteren Urteil des EuGH vom 10.07.2018 – C-25/17 – „Jehovan todistajat“ (Zeugen Jehovas) stellte der EuGH erneut klar, dass eine gemeinsame Verantwortlichkeit keine gleichwertige Verantwortlichkeit der verschiedenen Akteure für dieselbe Verarbeitung voraussetzt, sondern dass vielmehr die verschiedenen Akteure in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein können. Eine solche Zusammenarbeit ist vorliegend grundsätzlich auch zwischen den Krankenkassen und der gematik gegeben, da beide gleichermaßen mit der Verarbeitung in Kontakt kommen und ein eigenes Interesse an der Durchführung der Verarbeitung haben.

Zumindest zwischen der gematik und den jeweiligen Krankenkassen muss daher ein Regelungswerk im Sinne von Art.26 DSGVO getroffen werden, aus welchem hervorgeht, wer in welcher Phase der Verarbeitung der „Verantwortliche“ nach Art.4 Nr.7 DSGVO ist. Die §§ 291 ff. SGB V treffen hierzu keine Regelung. Es fehlt an einer Klärung und verbindlichen Festlegung, welche die jeweiligen Verantwortlichkeiten in den einzelnen Verarbeitungsphasen klarstellen. Sollte es zu einer Datenpanne kommen, so muss klar geregelt sein, wer die Pflichten nach Art.33f DSGVO zu erfüllen hat, um Gefahren und Schäden schnellstmöglich beseitigen und den Betroffenenrechten nachkommen zu können.

Vor allem aber bedarf es eines Regelungswerkes, welches eine sichere Datenverarbeitung zwischen den Krankenkassen und der gematik sicherstellt. Es muss daher geregelt werden, dass die IT-Infrastrukturen der jeweiligen Krankenkassen hinreichende Sicherheitsvorkehrungen aufweisen müssen, denn Sicherheitslücken in der IT-Infrastruktur einer Krankenversicherung bieten „Hackern“ ein einfachen Zugang in die Telematikinfrastruktur und damit auch in die IT-Systeme der Arztpraxen und Kliniken. Hierzu findet sich bisher keine gesetzliche Verpflichtung, so dass in keiner Weise eine sichere Datenverarbeitung gewährleistet werden kann. Gerade bei den vielen kleineren Krankenkassen ist zu befürchten, dass sie angesichts veralteter IT-Infrastrukturen große Sicherheitslücken ausweisen. Während derartige Sicherheitslücken in der Vergangenheit „nur“ zur Gefährdung eigener Systeme und Daten der dieser Krankenkasse führten, entsteht durch die Vernetzung mit der Telematikinfrastruktur eine Gefährdung für die IT-Systeme sämtlicher Teilnehmer der Telematikinfrastruktur, also sämtlicher Ärzte, Kliniken, Apotheken, etc..

Bevor die datenschutzrechtlichen Fragen einer Datenschutzfolgenabschätzung und des Joint-Controllership nicht geklärt sind, darf nach unserer Ansicht die Telematikinfrastruktur in Bezug auf das Versichertendatenmanagements nicht genutzt werden, so dass eine Nutzung behördlich zu untersagen ist.

Wir bitten diesbezüglich um dringende Prüfung.

Mit freundlichen Grüßen

Dr. Werner Baumgärtner
Vorstandsvorsitzender
MEDI GENO Deutschland e.V.
MEDI Baden-Württemberg e.V.