Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)151

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

Vorsitzende des Ausschusses
für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz, MdB
Platz der Republik 1
11011 Berlin

Nur per Mail:
innenausschuss@bundestag.de

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-5000
TELEFAX (0228) 997799-5550
E-MAIL referat11@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 26.10.2018
GESCHÄFTSZ. **11-100/044#0126**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Entwurf eines 2. Datenschutzanpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU), BT-Drs. 19/4674**

HIER Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

ANLAGEN -1-

Sehr geehrte Frau Vorsitzende,

für Ihre Beratungen zum Entwurf eines 2. Datenschutzanpassungs- und Umsetzungsgesetzes EU, BT-Drs. 19/4674 erhalten Sie im Anhang die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Ich würde mich freuen, wenn meine Vorschläge und Anregungen im weiteren Gesetzgebungsverfahren berücksichtigt würden. Für Ihre Fragen stehen Ihnen meine Mitarbeiterinnen und Mitarbeiter sowie ich selbst gern zur Verfügung. Zu den Empfehlungen des Bundesrates zu dem o. a. Gesetzentwurf werde ich gegebenenfalls gesondert Stellung nehmen.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Ich bitte Sie, meine Stellungnahme den Ausschussmitgliedern zur Verfügung zu stellen.

Mit freundlichen Grüßen

Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 26. Oktober 2018

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Zweiten Datenschutzanpassungs- und Umsetzungsgesetzes-EU (2. DSAnpUG-EU), BR-Drs. 430/18, BT-Drs. 19/4674

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Vorbemerkung

Die Bundesregierung hat am 5. September 2018 den Entwurf eines Zweiten Datenschutzanpassungs- und Umsetzungsgesetzes-EU (2. DSAnpUG-EU) beschlossen. Dieser liegt dem Bundesrat (BR-Drs. 430/18) sowie dem Deutschen Bundestag (BT-Drs. 19/4674) zur Beratung vor.

Die folgende Darstellung enthält die wichtigsten Punkte, die aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im weiteren parlamentarischen Verfahren berücksichtigt werden sollten.

I. Artikel 8 (Änderung des BDBOS-Gesetzes)

1. Zu Nr. 2 – Änderung von § 19 Abs. 2 BDBOS-Gesetz

§ 19 Abs. 2 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(2) Wenn der Bundesanstalt tatsächliche Anhaltspunkte für eine rechtswidrige Inanspruchnahme des Digitalfunks BOS vorliegen, darf sie Verkehrsdaten auch verarbeiten, soweit dies erforderlich ist, um die rechtswidrige Inanspruchnahme des Digitalfunks BOS festzustellen und zu unterbinden; die tatsächlichen Anhaltspunkte sind aktenkundig zu machen und der behördliche Datenschutzbeauftragte ist über die beabsichtige Verarbeitung zu informieren.“

Vorschlag BfDI:

§ 19 Abs. 2 BDBOS-Gesetz wird gestrichen.

Begründung:

Der Regierungsentwurf enthält einen Erlaubnistatbestand zur Verarbeitung von Verkehrsdaten. Da der BOS-Funk kein öffentlich zugänglicher Telekommunikationsdienst ist, fällt dieser nicht unter die Richtlinie 2002/58/EG, sondern die DSGVO. Im Anwendungsbereich der DSGVO können die Mitgliedstaaten spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen dieser Rechtsgrundlage liegen hier nicht vor, weil die Verarbeitung nicht erforderlich, jedenfalls aber nicht verhältnismäßig ist. Eine rechtswidrige Inanspruchnahme des Digitalfunks BOS dürfte äußerst selten vorkommen, so dass es in diesen Fällen genügt, wenn die Strafverfolgungsbehörden tätig werden. Der Diebstahl und die Unterschlagung von Empfangsgeräten ist strafbewehrt (§§ 242, 246 StGB) ebenso wie das unerlaubte Abhören des BOS-Funks (§ 148 Abs. 1 Nr. 1 i.V.m. § 89 TKG). Zudem können abhandengekommene Endgeräte sowie die zugehörigen SIM-Karten aus der Ferne deaktiviert werden.

2. Zu Nr. 2 – Änderung von § 19 Abs. 4 BDBOS-Gesetz

§ 19 Abs. 4 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(4) [1]Zur Sicherstellung, dass die Zwecke der Absätze 1 bis 3 erfüllt werden können, dürfen Verkehrsdaten nach ihrem Entstehen 75 Tage gespeichert werden. Nach Ablauf dieser Frist, sind die Verkehrsdaten zu löschen oder zu anonymisieren, es sei denn, ihre weitere Speicherung ist zu den in Absätzen 1 bis 3 genannten Zwecken erforderlich. [2]Die weitere Speicherung ist zu begründen und zu dokumentieren. [3]In Abständen von drei Monaten ist zu überprüfen, ob eine weitere Speicherung der Verkehrsdaten für die in den Absätzen 1 bis 3 genannten Zwecke erforderlich ist. [4]Wird im Rahmen der Überprüfung festgestellt, dass eine weitere Speicherung der Verkehrsdaten nicht erforderlich ist, sind die Verkehrsdaten unverzüglich zu löschen oder zu anonymisieren.“

Vorschlag BfDI:

§ 19 Abs. 4 BDBOS-Gesetz wird wie folgt gefasst:

„Aus konkretem Anlass kann die Bundesanstalt einzelfallbezogen anordnen, dass Verkehrsdaten gespeichert werden, soweit dies erforderlich ist, um sicherzustellen, dass die Zwecke der Absätze 1 bis 3 erfüllt werden können. Eine solche Entscheidung ist zu begründen und zu dokumentieren. Die Erforderlichkeit der Speicherung ist in regelmäßigen Zeitabständen, spätestens alle drei Monate, zu überprüfen. Dient die Speicherung von Verkehrsdaten allein den in Absatz 1 Nummer 2 und Absatz 3 genannten Zwecken, sind die Verkehrsdaten unverzüglich zu pseudonymisieren.“

Begründung:

Der Regierungsentwurf führt für den BOS-Funk eine Vorratsdatenspeicherung ein.

Während bei der allgemeinen Vorratsdatenspeicherung nach § 113b Abs. 1 Nr. 1 TKG Verkehrsdaten zehn Wochen (= 70 Tage) lang auf Vorrat gespeichert werden, soll dies beim BOS-Funk sogar 75 Tage lang erlaubt sein. Die Erforderlichkeit einer so langen Speicherdauer kann nicht nachvollzogen werden. Der Umstand, dass zum Zeitpunkt der Speicherung der konkrete Verwendungszweck noch nicht feststeht, widerspricht dem datenschutzrechtlichen Grundsatz der Zweckbindung.

Die im TKG enthaltene anlasslose Vorratsdatenspeicherung ist derzeit Gegenstand mehrerer Gerichtsverfahren (BVerwG 6 C 12.18 und 6 C 13.18; BVerfG 1 BvR 141/16) und es bestehen erhebliche Zweifel an der Verhältnismäßigkeit einer so lan-

gen anlasslosen Speicherung. Zwar wird die Erforderlichkeit der im BDBOS-Gesetz vorgesehenen Speicherdauer umfangreich begründet. Auch unter Berücksichtigung des Erfordernisses, in einigen Fällen Daten rückwirkend auswerten zu müssen, scheint die lange Speicherung dennoch unverhältnismäßig. Eine Abwägung mit den datenschutzrechtlichen Interessen der Betroffenen findet nahezu nicht statt.

Die standardmäßig vorgegebene Speicherfrist sollte daher entfallen. Verkehrsdaten sollten grundsätzlich nur solange gespeichert werden, wie dies für den Betrieb des BOS-Funks erforderlich ist (bei den meiner Aufsicht unterliegenden Telekommunikationsanbietern wurde eine Speicherdauer zu betrieblichen Zwecken wie der Störungsbeseitigung von maximal sieben Tagen als angemessen angesehen), allerdings mit der Option einer anlassbezogenen Verlängerung eines bestimmten, näher einzugrenzenden Datenbestands im Rahmen eines sog. „Quick Freeze“, soweit dies zu den in Abs. 1 bis 3 genannten Zwecken erforderlich ist und eine entsprechende Begründung und Dokumentation erfolgt. Bei geplanten Großeinsätzen (z. B. G7-Gipfel), bei denen die Erforderlichkeit einer längeren Speicherdauer bereits vorab bekannt ist, kann eine Speicherung der benötigten Daten im Vorfeld einzelfallbezogen angeordnet werden.

Für die Zwecke des § 19 Abs. 1 Nr. 2 und Abs. 3 BDBOS-Gesetz genügen auch pseudonymisierte Daten, so dass eine weitere Speicherung von Verkehrsdaten, die allein diesen Zwecken dient, zum Schutz der Betroffenen ausschließlich in pseudonymisierter Form erfolgen sollte. Dies entspricht der Vorgabe des Art. 32 DSGVO, wonach Verantwortliche technische und organisatorische Maßnahmen wie Pseudonymisierung zu treffen haben, um ein dem Risiko angemessenes Schutzniveau herzustellen.

3. Zu Nr. 2 – Änderung von § 20 Abs. 2 BDBOS-Gesetz

§ 20 Abs. 2 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(2) Um das Wiederauffinden eines abhandengekommenen Endgerätes zu unterstützen, darf auf Antrag eines Nutzers die Bundesanstalt an die für diesen Nutzer verantwortliche Zuständige Stelle für den Betrieb des Digitalfunk BOS folgende Daten übermitteln:

1. *Kennung der Basisstationen, an denen sich das Endgerät seit dem Abhandenkommen eingebucht oder einzubuchen versucht hat, und*
2. *den Zeitpunkt, zu dem die jeweilige Standortinformation erfasst wurde.*

Der Antrag ist durch den Nutzer über die für ihn verantwortliche Zuständige Stelle für den Betrieb des Digitalfunk BOS zu stellen und hat Angaben zur Identifizierung des Endgeräts zu enthalten.“

Vorschlag BfDI:

§ 20 Abs. 2 BDBOS-Gesetz ist zu streichen.

Begründung:

Der Regierungsentwurf enthält einen Erlaubnistatbestand zur Verarbeitung von Verkehrsdaten, wozu auch Standortdaten zählen, zum Zwecke des Auffindens von Endgeräten des BOS-Funks. Im Anwendungsbereich der DSGVO können die Mitgliedstaaten spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen dieser Rechtsgrundlage liegen hier nicht vor, da die Verarbeitung nicht erforderlich, jedenfalls aber nicht verhältnismäßig ist.

Die Verarbeitung ist nicht verhältnismäßig. Die Endgeräte des BOS-Funks sind wesentlich günstiger als die früheren Endgeräte beim Analogfunk. Deshalb sind die Kosten einer Suchaktion nach einem verlorenen Gerät häufig kostspieliger als die Kosten eines Neuerwerbs. Zudem können verlorene Endgeräte sowie zugehörigen SIM-Karten aus der Ferne deaktiviert werden, so dass ein Verlust zu keinen Sicherheitsrisiken führt.

II. Artikel 13 (Änderung des BSI-Gesetzes)

Zu Nr. 7 - § 6f Satz 2 BSI-Gesetz

§ 6f Satz 2 des BSI-Gesetzes (BSIG-E) in der Entwurfsfassung lautet:

„Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.“

Vorschlag BfDI:

§ 6f Satz 2 des BSI-Gesetzes in der Entwurfsfassung wird gestrichen.

Begründung:

Art. 21 Abs. 1 Satz 1 DSGVO ermöglicht es der betroffenen Person, aus Gründen, die sich aus ihrer besonderen Situation ergeben, einer an sich rechtmäßigen Verarbeitung personenbezogener Daten – bspw. durch eine Behörde – zu widersprechen. Eine Verarbeitung dieser Daten ist nach einem Widerspruch gem. Art. 21 Abs. 1 Satz 2 DSGVO nur dann erlaubt, wenn der Verantwortliche dafür zwingende schutzwürdige Gründe nachweisen kann, die die Interessen der betroffenen Person überwiegen.

§ 6f Satz 2 BSIG-E setzt an dieser Stelle an und soll es dem BSI ermöglichen, während der Prüfung der o. g. zwingenden Gründe die Verarbeitung noch fortsetzen zu dürfen. Diese Beschränkung wird auf Art. 23 DSGVO gestützt. Die dem BSI damit eingeräumte Möglichkeit, die zwingenden Gründe für die Verarbeitung ohne jede zeitliche Begrenzung zu prüfen, führt allerdings dazu, dass das Widerspruchsrecht faktisch in das Belieben des BSI gestellt und weitgehend ausgehebelt wird. Art. 23 Abs. 1 DSGVO erlaubt Beschränkungen der Betroffenenrechte nur, soweit diese eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellt. Die hierzu in der Begründung genannten Aspekte vermögen eine zeitlich unbefristete Aushebelung des Widerspruchsrechts nicht zu begründen. Der Satz ist daher zu streichen, zumindest aber mit einer zeitlich engen Frist zu versehen.

III. Artikel 62 (Änderung des Soldatengesetzes)

Zu Nr. 2 – Änderung von § 58c Soldatengesetz

§ 58 c Soldatengesetz lautet:

„(1) Zum Zweck der Übersendung von Informationsmaterial nach Absatz 2 Satz 1 übermitteln die Meldebehörden dem Bundesamt für das Personalmanagement der Bundeswehr jährlich bis zum 31. März folgende Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden:

1. Familienname,

2.Vornamen,

3.gegenwärtige Anschrift.

Die Datenübermittlung unterbleibt, wenn die Betroffenen ihr nach § 36 Absatz 2 des Bundesmeldegesetzes widersprochen haben.

(2) Das Bundesamt für das Personalmanagement der Bundeswehr darf die Daten nur dazu verwenden, Informationsmaterial über Tätigkeiten in den Streitkräften zu versenden.

(3) Das Bundesamt für das Personalmanagement der Bundeswehr hat die Daten zu löschen, wenn die Betroffenen dies verlangen, spätestens jedoch nach Ablauf eines Jahres nach der erstmaligen Speicherung der Daten beim Bundesamt für das Personalmanagement der Bundeswehr.“

Vorschlag BfDI:

§ 58 c Soldatengesetz wird gestrichen.

Begründung:

§ 58 c Absatz 1 Satz 2 Soldatengesetz sieht vor, dass Meldebehörden personenbezogene Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden, an das Bundesamt für Personalmanagement der Bundeswehr übermitteln dürfen, wenn die Betroffenen der Übermittlung nicht widersprochen haben.

Die Übermittlung ist eine Form der Verarbeitung (Art. 4 Nr. 2 DSGVO). Die Mitgliedstaaten können spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO liegen nicht vor. Gründe für die Übermittlung

der Daten zur Erfüllung einer rechtlichen Verpflichtung oder aus Gründen des öffentlichen Interesses werden nicht genannt.

Der Bedarf an einer bereichsspezifischen Sonderregelung für den Bereich des Bundesministeriums der Verteidigung ist daher nicht überzeugend dargelegt.

IV. Artikel 82 (Änderung des IHK-Gesetzes)
Zu Nr. 2 lit. b) – Änderung von § 9 Abs. 5 IHK-Gesetz

§ 5 Absatz 5 des IHK-Gesetzes in der Entwurfsfassung lautet:

„(5) 1Die Industrie- und Handelskammern dürfen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken die in Absatz 1 genannten Daten an nicht-öffentliche Stellen übermitteln, sofern der betroffene Kammerzugehörige der Übermittlung nicht widersprochen hat und der Empfänger der Daten sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. 2Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die Kammerzugehörigen unbeschadet der weiteren Vorgaben der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung vor der ersten Übermittlung schriftlich oder elektronisch hinzuweisen. 3Daten über Zugehörige anderer Kammern hat die Industrie- und Handelskammer nach Übermittlung an die nicht-öffentliche Stelle unverzüglich zu löschen, soweit sie nicht zur Erfüllung der ihr nach diesem Gesetz übertragenen Aufgaben erforderlich sind.“

Vorschlag BfDI:
§ 5 Absatz 5 IHK-Gesetz wird gestrichen.

Begründung:

Der Entwurf sieht vor, dass die Industrie- und Handelskammern personenbezogene Daten ihrer Kammermitglieder an nichtöffentliche Stellen übermitteln dürfen, wenn die Kammermitglieder dem nicht widersprechen. Eine solche Widerspruchslösung ist nach der DSGVO nicht zulässig.

Die Übermittlung ist eine Form der Verarbeitung (Art. 4 Nr. 2 DSGVO). Die Mitgliedstaaten können spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO dürften in der Mehrzahl der hier geregelten Fälle nicht vorliegen. Die Übermittlung der Daten ist nicht zur Erfüllung einer rechtli-

chen Verpflichtung erforderlich und liegt auch nicht im öffentlichen Interesse, sondern im mutmaßlichen privaten Interesse der Kammermitglieder an der Förderung von Geschäftsabschlüssen. Eine mutmaßliche Einwilligung ist nach der DSGVO allerdings nicht vorgesehen. Erforderlich sind vielmehr eindeutige bestätigende Handlungen, weshalb Stillschweigen oder Untätigkeit – hier ein Nichtwidersprechen – keine Einwilligung darstellen (Erwägungsgrund 32 Satz 3 DSGVO).

Es wurde auch kein Bedarf an einer bereichsspezifischen Sonderregelung für die Industrie- und Handelskammern dargelegt. Wenn die Übermittlungen im Interesse der Kammermitglieder sind, werden diese ihre Einwilligungen erteilen. Ein solches Verfahren stellt die Kammern nicht vor große praktische Hürden, wie das Beispiel der Wirtschaftsprüferkammer belegt, bei der ein solches Verfahren bereits praktisch etabliert ist. Im Übrigen wurden die Erlaubnistatbestände für die Übermittlung personenbezogener Daten von öffentlichen an nichtöffentliche Stellen bereits allgemein in § 25 Abs. 2 und § 23 BDSG geregelt. Dies genügt, so dass bereichsspezifische Regelungen im IHK-Gesetz nicht erforderlich sind.

V. Artikel 123 (Änderung des Fünften Buches Sozialgesetzbuch)

1. Zu Nr. 38 – Änderung von § 284 SGB V

Der Gesetzentwurf enthält keine klarstellende Regelung zur Wirkung der Einwilligung im Verhältnis des Versicherten zur gesetzlichen Krankenkasse. Obwohl in den bis zum Sommer 2018 diskutierten und im Ressortkreis konsentierten Vorentwürfen eine solche Regelung enthalten war, fehlt sie bedauerlicherweise im Regierungsentwurf.

Ich rege daher an, eine ursprünglich mit den Bundesministerien inhaltlich abgestimmte Regelung in das Gesetz aufzunehmen.

Vorschlag BfDI:

In § 284 SGB V wird folgender Absatz 5 eingefügt:

„(5) Krankenkassen dürfen Sozialdaten, sofern sie besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 sind, auf Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2016/679 in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 nur verarbeiten, sofern in diesem Buch eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Dies gilt nicht für die Übermittlung für Zwecke der wissenschaftlichen Forschung und Planung Dritter.“

Begründung:

Dem Gesetzesvorbehalt nach § 30 des Vierten Buches Sozialgesetzbuch (SGB IV) folgend knüpft § 284 SGB V die dort geregelten Datenverarbeitungsbefugnisse der Krankenkassen an die Voraussetzung, dass die zu verarbeitenden Daten für die dort abschließend aufgeführten Zwecke erforderlich sind. Um auszuschließen, dass Krankenkassen allein auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 Daten für Zwecke verarbeiten, die nicht zu ihrem gesetzlich zugewiesenen Aufgabenbereich gehören, sieht § 284 Absatz 5 SGB V auf der Grundlage der Öffnungsklausel des Artikels 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 vor, dass Krankenkassen besondere Kategorien personenbezogener Sozialdaten auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 trotz Einwilligung der betroffenen Person nur dann verarbeiten dürfen, wenn im SGB V eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Damit wird der Status quo erhalten.

Eine entsprechende Klarstellung, die die seit Jahrzehnten bestehende gemeinsame Rechtsauffassung des Bundesministeriums für Gesundheit, des Bundessozialge-

richts (siehe Urt. v. 10. Dezember 2008 – B6 KA 37/07 R -, BSGE 102, S. 134 Leitsatz 1), des Bundesversicherungsamtes und mir deutlich zum Ausdruck bringen.

Eine derartige Klarstellung ist nicht zuletzt deshalb erforderlich, da eine erhebliche Anzahl von Beschwerden von Versicherten, aber auch von Ärzten vorliegen, wonach in der Praxis diese Rechtsauffassung der Aufsichtsbehörden von Krankenkassen umgangen wird, indem Versicherte veranlasst werden, Schweigepflichtentbindungserklärungen abzugeben, um hiermit von Ärzten medizinische Daten über die Versicherten zu erheben, die ihnen gesetzlich nicht zustehen. Eine derartige Klarstellung würde zudem Erwägungsgrund 43 der DSGVO präzisieren, wonach eine Einwilligung dann keine gültige Rechtsgrundlage ist, „wenn zwischen der betroffenen Person“ (Versichertem) „und dem Verantwortlichen (gesetzliche Krankenkasse) ein klares Ungleichgewicht besteht“, … „und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“. Tatsächlich erfolgt die Forderung an den Versicherten, eine Schweigepflichtentbindungserklärung abzugeben, häufig in Fällen, in denen der Versicherte auf die Zahlung von Krankengeld angewiesen ist. Über die Probleme habe ich mehrfach berichtet (u.a. in meinem 26. [Nr. 9.2.5], 25. [Nr. 13.7.1] und 22. [Nr. 11.1.8] Tätigkeitsbericht).

2. Zur Verhängung von Geldbußen

Vorschlag BfDI:

Dem § 307 wird folgender Absatz 5 angefügt:

„(5) Abweichend von § 85a Absatz 3 des Zehnten Buches Sozialgesetzbuch kann gegen eine Krankenkasse wegen eines Verstoßes nach Artikel 83 Absatz 4, 5 oder 6 der Verordnung (EU) 2016/679, der sich auf Sozialdaten bezieht, eine Geldbuße nach Artikel 58 Absatz 2 Buchtstabe i) der Verordnung (EU) 2016/679 verhängt werden. § 17 Absatz 4 des Gesetzes über Ordnungswidrigkeiten ist anzuwenden.“

Begründung:

Der vorliegende Gesetzentwurf sieht keine Möglichkeit vor, Geldbußen bei Datenschutzverstößen durch gesetzliche Krankenversicherungen zu verhängen. Ein durchgreifender Grund, die sich verstärkt als Wirtschaftsunternehmen verstehenden gesetzlichen Krankenkassen mit einem Ausgabevolumen von zum Teil mehr als 25 Mrd. Euro gegenüber einem Handwerks- oder Industrieunternehmen zu privilegieren, ist nicht ersichtlich

Bereits mit der Einführung des geltenden § 85a des Zehnten Buches Sozialgesetzbuch (SGB X) war eine deutliche Verschlechterung des Datenschutzniveaus gegenüber der früheren, bis zum 24. Mai 2018 geltenden Regelung des § 85 SGB X a.F. eingetreten, in dem nunmehr pauschal Behörden und sonstige öffentliche Stellen, und damit auch gesetzliche Krankenkassen von der Verhängung eines Bußgeldes ausgenommen werden. So war es beispielsweise nach § 85a Absatz 1 Nr. 1a) und b) SGB X a.F. möglich, ein Bußgeld zu verhängen, falls bestimmte Versäumnisse bei der Auftragsverarbeitung nach § 80 SGB X vorlagen, nach § 85a Absatz 1 Nr. 3 SGB X a. F., wenn ein Sozialleistungsträger nicht oder nicht rechtzeitig einen internen Datenschutzbeauftragten bestellte oder nach § 85 Absatz 2 Nr. 6 SGB X a.F., wenn er eine Datenschutzverletzung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig den Rechtsaufsichts- und Datenschutzbehörden nach § 83a SGB X meldete.

Ich halte es für geboten, in das 2. DSAnpUG-EU eine Regelung aufzunehmen, die die wirtschaftliche Tätigkeit und das wirtschaftliche Auftreten der gesetzlichen Krankenkassen berücksichtigt und die es ermöglichte, in diesem Rahmen bestimmte Verstöße gegen die Datenschutz-Grundverordnung nach Art. 58 Absatz 2 Buchst. i) i.V.m. Art. 83 DSGVO mit einem Bußgeld zu sanktionieren.

Gesetzliche Krankenkassen sind einerseits öffentlich-rechtliche Körperschaften (§ 29 Absatz 1 Viertes Buch Sozialgesetzbuch – SGB IV), die gesetzliche Aufgaben zu erfüllen haben. Andererseits nehmen sie als öffentliche Unternehmen am Wettbewerb teil (§ 2 Absatz 5 BDSG). Der Wettbewerb hat in der Vergangenheit z. B. zu Fusionen geführt, die die Zahl der gesetzlichen Krankenkassen von 1.147 im Jahre 1990 auf den heutigen Stand von lediglich 110 gesetzlichen Krankenkassen reduziert hat.

Auch in der Öffentlichkeit gerieren sich die gesetzlichen Krankenkassen als öffentliche Wettbewerbsunternehmen, die mit verschiedenen Angeboten – ähnlich wie privatrechtliche Krankenversicherungsunternehmen – um ihre Kundschaft werben. So bieten etwa einige Krankenkassen in Zusammenarbeit mit privaten Anbietern ihren Kunden die Nutzung von elektronischen Gesundheitsakten an, die über eine App auf dem Smartphone oder Tablet genutzt werden sollen. Die Angebote und das Datenschutzniveau unterscheiden sich dabei deutlich und dies wird von den gesetzlichen Krankenkassen auch als Wettbewerbsvorteil gegenüber anderen Krankenkassen gesehen. Der Wettbewerb der Krankenkassen erstreckt sich u. a. zudem auf das Angebot von innovativen Versorgungsformen und (Zusatz-) Leistungen innerhalb des gesetzlich eröffneten Rahmens. Im Verhältnis zu ihren Versicherten ist das Verhalten der Krankenkassen unmittelbar am UWG zu messen, soweit dieses die Richtlinie 2005/29/EG (UGP-RL) über unlautere Geschäftspraktiken umsetzt (vgl. hierzu statt vieler BGH, Urteil vom 30. April 2014 – I ZR 170/10 –; Urteil vom 18. September 2013 – I ZR 183/12 –; EuGH, Urteil vom 03. Oktober 2013 – C-59/12 –).

Schließlich ist es einem Versicherten (bei den gesetzlichen Krankenkassen intern „Kunde“ genannt) möglich, frei von einer gesetzlichen Krankenkasse zu einer anderen zu wechseln. Dies ist bei anderen Sozialversicherungsträgern (Deutsche Rentenversicherungen, gesetzliche Unfallversicherer) nicht möglich. Die gesetzlichen Renten- und Unfallversicherungsträger stehen im Gegensatz zu den gesetzlichen Krankenkassen untereinander nicht im Wettbewerb

Es gibt daher tatsächliche Gründe, die Krankenkassen im Unterschied zu anderen Sozialversicherungsträger Wirtschaftsunternehmen gleich zu stellen.

Mit dem o. a. Vorschlag wird von der Möglichkeit einer abweichenden Regelung nach Artikel 83 Absatz 7 der Verordnung (EU) 2016/679 Gebrauch gemacht.

Geahndet werden können Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 durch die genannten Stellen bei der Verarbeitung von Sozialdaten im Zusammenhang mit ihren Aufgaben. Die Höhe des Bußgeldrahmens entspricht europarechtsgemäß dem in Artikel 83 Absatz 4 bis 6 DSGVO festgelegten Rahmen.

Zuständige Aufsichtsbehörden für die Verhängung von Geldbußen sind gemäß Artikel 58 Absatz 2 Buchstabe i in Verbindung mit Artikel 83 der Verordnung (EU) 2016/679 die jeweiligen Datenschutzaufsichtsbehörden, d. h. der oder die BfDI oder

die jeweiligen Landesdatenschutzbeauftragten. Hinsichtlich der praktischen Auswirkungen einer Bußgeldregelung weise ich darauf hin, dass die Verhängung eines Bußgeldes „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein muss(Art. 83 Absatz 1 DSGVO). Bei der Bemessung des Bußgeldes ist aber auch zu berücksichtigen, dass es sich bei den Geldern der gesetzlichen Krankenkassen um Versichertenbeiträge handelt.

VI. Artikel 135 (Änderung des Postgesetzes)

1. Zu Nr. 3 – Änderung von § 41 PostG

§ 41Postgesetz (PostG-E) in der Entwurfsfassung lautet:

„Für Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung solcher Dienste mitwirken (Diensteanbieter), werden die Vorgaben der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung durch die Regelungen der §§ 41a bis 42 ergänzt.“

Vorschlag BfDI:

§ 41 PostG wird um folgenden Satz ergänzt: *„Die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen stehen personenbezogenen Daten bei der Erbringung geschäftsmäßiger Postdienste gleich.“*

Begründung:

Das zu verfolgende Ziel im postrechtlichen Datenschutz muss sein, dass das bisherige, sich aus dem PostG und der Postdienste-Datenschutzverordnung (PDSV) ergebende Datenschutzniveau beibehalten wird und durch die Berücksichtigung der Datenschutz-Grundverordnung (DSGVO) keine Absenkung erfährt. An dem bisherigen datenschutzrechtlichen Gleichlauf bei natürlichen und juristischen Personen ist daher auch weiterhin festzuhalten. Die seinerzeitigen Erwägungen für die Schaffung eines einfachgesetzlichen, auch für juristische Personen geltenden, Postgeheimnisses durch das PostG i.V.m. der PDSV tragen nach wie vor. Die Regelungen wurden im Zuge der Privatisierung der Post und der Aufgabe des Postmonopols geschaffen. Da es sich bei Postdienstleistungen um vormals hoheitlich erbrachte Leistungen der Daseinsvorsorge handelt, die ursprünglich dem Fernmeldegeheimnis (Art. 10 GG) unterlagen, hat der Bund eine einfachgesetzliche Ausprägung des Postgeheimnisses geschaffen, damit auch bei der Leistungserbringung durch Private weiterhin vergleichbare Datenschutzstandards gelten.

Die auch zukünftig notwendige Regelung zur Gleichstellung der Einzelangaben über juristische Personen ist auch unter Berücksichtigung von Erwägungsgrund 14 der

DSGVO zulässig. Erwägungsgrund 14 stellt klar, dass sich die unmittelbare Geltung der DSGVO nicht auf juristische Personen erstreckt. Daraus ergibt sich aber im Umkehrschluss, dass der nationale Gesetzgeber Regelungen erlassen kann, die auch darin bestehen können, die DSGVO-Normen für juristische Personen anwendbar zu erklären. Die EU-weite Vollharmonisierung des Schutzes personenbezogener Daten durch die DSGVO bedeutet eine Sperrwirkung für mitgliedsstaatliche Regelungen nur bezogen auf die Verarbeitung personenbezogener Daten. Die DSGVO hindert die Mitgliedstaaten jedoch nicht daran, für Bereiche außerhalb des sachlichen Anwendungsbereichs der DSGVO diese für anwendbar zu erklären. Der nationale Gesetzgeber darf nur keine Regelungen zur Verarbeitung personenbezogener Daten natürlicher Personen treffen, soweit er keine ausdrückliche Regelungsbefugnis hat..

Die Postdienstleister erleiden durch die weiterhin bestehende Berücksichtigung der Einzelangaben juristischer Personen auch keinen Wettbewerbsnachteil dadurch, dass sie, anders als in anderen EU-Mitgliedstaaten, die Daten juristischer Personen ebenso schützen müssen wie die von natürlichen Personen. Im Gegenteil ist es gerade auch im Interesse der gesamten Wirtschaft, wenn der Schutz für die Daten juristischer Personen weiterhin bestehen bleibt.

Eine Abkehr von der Gleichstellung der Einzelangaben juristischer Personen würde die Postdienstleister auch vor schwere Herausforderungen stellen, da eine unterschiedliche Behandlung von in der Praxis gleichen Sachverhalten nicht praktikabel ist. Entgegen jeder Lebensrealität müssten die Postdienstleister jederzeit ihre Prozesse nach Geschäfts- und Privatpost trennen können. Dies ist den Postdienstleistern aus meiner Erfahrung bei datenschutzrechtlichen Kontrollen im Postbereich jedoch nicht möglich.

Es sollten daher die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und der Regelungen der §§ 41a bis 42 PostG-E auf die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen entsprechend Anwendung finden.

2. Zu Nr. 3 – § 41b PostG

§ 41b Absatz 1 Postgesetz (PostG-E) in der Entwurfsfassung lautet:

„(1) Diensteanbieter können von am Postverkehr Beteiligten verlangen, sich über ihre Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere auszuweisen, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen.“

Vorschlag BfDI:

§ 41b PostG ist folgendermaßen zu ergänzen: *„(1) Diensteanbieter können von am Postverkehr Beteiligten verlangen, sich über ihre Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere auszuweisen, wenn dies erforderlich ist, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen.“*

Begründung:

In den Referentenentwürfen war der Erforderlichkeitsgrundsatz richtigerweise im Gesetzestext beachtet worden. Schon die Postdienste-Datenschutzverordnung (PDSV) geht in § 7 Abs. 1 von dem Erforderlichkeitsgrundsatz aus.

3. Zu Nr. 4 – Änderung von § 42 PostG

Die Überschrift zu § 42 Postgesetz lautet:

„Kontrolle und Durchsetzung von Verpflichtungen“

Vorschlag BfDI:

Die Überschrift zu § 42 PostG ist folgendermaßen zu ergänzen: *„Kontrolle, Aufsicht und Durchsetzung von Verpflichtungen“*

Begründung:

In der Überschrift zu § 42 PostG (und auch in der Inhaltsübersicht zu dieser Vorschrift) ist zusätzlich das Wort „Aufsicht“ aufzunehmen, da § 42 Abs. 3 PostG-E in Anpassung an die DSGVO und das BDSG die datenschutzrechtliche Aufsicht der BfDI behandelt. Auch die DSGVO und das BDSG sprechen von Aufsichtsbehörden bzw. Aufsicht.

VII. Nichtaufnahme einer Anpassung des TKG

Vorschlag BfDI:

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die seit dem 25. Mai 2018 anzuwendende Datenschutz-Grundverordnung erfordert eine Anpassung der datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

dem Deutschen Bundestag unverzüglich einen Gesetzentwurf vorzulegen, mit dem die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes an die Datenschutz-Grundverordnung angepasst werden.

Begründung:

Das Telekommunikationsgesetz enthält in seinem siebten Teil (§§ 88 ff.) auch datenschutzrechtliche Bestimmungen, die nicht auf europarechtlichen Vorgaben beruhen, insbesondere nicht der Umsetzung der Richtlinie 2002/58/EG dienen, sondern nunmehr durch die DSGVO geregelt werden.

Spätestens seit Anwendbarkeit der DSGVO (25. Mai 2018) ist die Bundesrepublik verpflichtet (§ 4 Abs. 3 EUV), das TKG an diese neue Rechtslage anzupassen. Dieser „Verpflichtung aus den Verträgen“ (Art. 258 AEUV) ist Deutschland bislang nicht nachgekommen.

Dadurch, dass das TKG im bisherigen Umfang formal weiterbesteht, ist zudem nicht klar ersichtlich, welche datenschutzrechtlichen Bestimmungen – diejenigen der DSGVO oder diejenigen des TKG – auf einen bestimmten telekommunikationsrechtlichen Sachverhalt anzuwenden sind und inwieweit das TKG von dem Anwendungsvorrang der DSGVO (vgl. Art. 95 DSGVO) verdrängt wird. Dies führt bei den Betroffenen zu erheblicher Rechtsunsicherheit.

Die im TKG angelegte Zuständigkeit der Bundesnetzagentur zur Durchsetzung datenschutzrechtlicher Vorschriften sowie die Zuständigkeit derselben zur Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten (§ 149 Abs. 1 Nr. 16 bis 17d und 18 sowie 21b, 21c, 30a und 38 bis 43 TKG) widerspricht nicht nur der DSGVO, sondern auch dem europäischen Primärrecht und ist daher dringend anzupassen. Als eine der Fach- und Rechtsaufsicht unterliegende Verwaltungsbehörde ge-

nügt die Bundesnetzagentur nicht den Anforderungen, die das europäische Recht an die Unabhängigkeit und Weisungsfreiheit der Datenschutzvorschriften kontrollierenden Stellen aufstellt (Art. 8 Abs. 3 GrCh; Art. 16 Abs. 2 S. 2 AEUV). Umgekehrt ist die BfDI zwar unabhängig, verfügt jedoch nach aktueller nationaler Rechtslage über keine Durchsetzungsbefugnisse in Bezug auf Datenschutzvorschriften des TKG. Damit wird die effektive Wahrnehmung ihrer Aufgabe als unabhängige Datenschutzbehörde konterkariert.

Das BMWi hatte deshalb ursprünglich vorgesehen, im Zuge des 2. DSAnpUG-EU auch das TKG anzupassen. Ein entsprechender Referentenentwurf wird aber nicht mehr verfolgt. Die erforderlichen datenschutzrechtlichen Anpassungen finden sich auch nicht in dem Entwurf eines Vierten Gesetzes zur Änderung des Telekommunikationsgesetzes (BR-Drs. 391/18).

Andrea Voßhoff