BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 21/2022
Mai 2022
Registernummer: 25412265365-88

zum

Vorschlag eines EU-Datengesetzes
(Vorschlag der Europäischen Kommission (COM(2022) 68 final))

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.
RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK

Mitglieder des Ausschusses Europarecht

RAuN a.D. Kay-Thomas Pohl (Vorsitzender)
RA Dr. Hans-Joachim Fritz
RAin Dr. Margarete Gräfin von Galen
RA Marc André Gimmy
RA Andreas Max Haak
RA Dr. Frank J. Hospach
RA Guido Imfeld
RA Maximilian Müller
RAin Dr. Kerstin Niethammer-Jürgens
RA Dr. Christian Lemke
RA Jan K. Schäfer, LL.M.
RAin Stefanie Schott
Prof. Dr. Gerson Trüg
RA Dr. Hans-Michael Pott
RA Andreas von Máriássy
RA Dr. Thomas Westphal
RAuN Dr. Thomas Remmers, Vizepräsident, Bundesrechtsanwaltskammer
RAin Dr. Heike Lörcher, Bundesrechtsanwaltskammer, Brüssel
RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. Jur. Sarah Pratscher, Bundesrechtsanwaltskammer, Brüssel

Verteiler: Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Innenausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Bundesrechtsanwaltskammer bedankt sich für die Möglichkeit einer Stellungnahme und gibt Nachstehendes zu bedenken.

Zusammenfassung

Der Entwurf ist umfassend und ambitioniert. Seine Umsetzung wäre mit erheblichen Auswirkungen auf alle Nutzer und Anbieter von alltäglich eingesetzten Produkten und damit verbundenen Diensten in einer Vielzahl von Situationen verbunden. Es sollte vermieden werden, dass der Einsatz dieser Produkte hierdurch erschwert wird. Es dürfte vielen nach dem Entwurf Verpflichteten aus organisatorischen, wirtschaftlichen oder rechtlichen Gründen nicht möglich sein, die vorgesehenen Daten- bzw. Zugangsbereitstellungspflichten in zumutbarer Weise zu erfüllen, wodurch diese am Einsatz der Produkte bzw. Dienste gehindert wären. Auch könnte der mit den Pflichten verbundene Aufwand die Betroffenen davon abhalten, solche Produkte einzusetzen oder anzubieten. Hierdurch könnte der mit dem Gesetzentwurf bezweckte und in einiger Hinsicht voraussichtlich auch beförderte soziale, wirtschaftliche und technische Fortschritt an anderer Stelle zugleich behindert werden. Besonders gravierend könnten derart nachteilige Auswirkungen in Sektoren zum Tragen kommen, die, wie die Anwaltschaft, besonderen Verpflichtungen im Umgang mit Daten unterliegen – insbesondere also in Bereichen, in denen Berufsgeheimnisse existieren. Es wäre wenig gewonnen, wenn gerade in so gewichtigen und grundlegenden Bereichen wie dem Zugang zum Recht, der Rechtsberatung, der Justiz oder der Gesundheitsversorgung der soziale, wirtschaftliche und technische Fortschritt durch zu weitreichende Verpflichtungen ausgebremst würde. Dies sollte vermieden werden. Erreicht werden könnte dies durch genauere und engere horizontale Begriffsdefinitionen – insbesondere der Begriffe *Dateninhaber* und *verbundener Dienst* – sowie Ausnahmen für bestimmte Bereiche oder Sektoren. Entsprechende Regelungsvorschläge finden sich in *Abschnitt 1. Übermäßiger Anwendungs- und Regelungsbereich*.

In jedem Fall und insbesondere, soweit diese nicht durch Bereichsausnahmen im vorgenannten Sinne ausgeschlossen werden können, müssen Verletzungen der anwaltlichen Verschwiegenheit und Beeinträchtigungen der anwaltlichen Unabhängigkeit ausgeschlossen werden. Es darf insbesondere für Anwältinnen und Anwälte sowie für die Rechtsanwaltskammern keinerlei Pflicht geschaffen werden, über Mandatshinhalte oder auch nur Umstände einer Mandatierung Auskunft zu erteilen. Entsprechende Regelungsvorschläge finden sich daher unter *2.1 Regelungsvorschläge zum Schutz der anwaltlichen Verschwiegenheit*.

Die Aufsicht über die Anwendung der Verordnung im anwaltlichen Bereich muss, wie in anderen Mandatsinformationen betreffenden Regelungsbereichen, wie etwa dem Datenschutzrecht oder der KI-Regulierung auch, der anwaltlichen Selbstverwaltung vorbehalten bleiben. Ein Regelungsvorschlag hierzu findet sich unter *2.2 Regelung betreffend den Schutz der anwaltlichen Unabhängigkeit und Selbstverwaltung*.

Das Verhältnis der Verordnung zum bestehenden Datenschutzrecht bedarf einer Klarstellung, für welche unter *3. Verhältnis der Verordnung zum Bestehenden Datenschutzregime* ebenfalls ein Regelungsvorschlag unterbereitet wird.

Im Einzelnen

Inhalt

1. Übermäßiger Anwendungs- und Regelungsbereich

Der Verordnungsentwurf erfasst aufgrund seines weiten Anwendungsbereichs und des insgesamt breiten horizontalen Regelungsansatzes eine Vielzahl potentieller Sachverhalte und Adressaten.

Der persönliche und sachliche Anwendungsbereich des Verordnungsentwurfs ist zu weit gefasst (Art. 1 Abs. 1 und 2). Insbesondere die auf Dateninhaber oder -empfänger bezogenen Verpflichtungen zur Zugänglichmachung (Art. 3 Abs. 1) bzw. Bereitstellung von Daten (Art. 4 Abs. 1) können nahezu jedermann treffen, da kaum Eingrenzungen des Kreises der Dateninhaber, der Produkte, damit verbundenen Dienste oder der Art der Daten erfolgen. Die diesbezüglichen Begriffsdefinitionen in Art. 2 sind übermäßig weit gefasst (zur Definition des Dateninhabers: siehe unten). Dass hinsichtlich von Produkten und verbundenen Dienstleistungen bestehende Verpflichtungen gemäß Art. 7 Abs. 2 auch für virtuelle Assistenten gelten sollen, erweitert den Anwendungsbereich zusätzlich und legt mit Blick auf die Definition des verbundenen Dienstes im Sinne von Art. 2 Nr. 3 insgesamt ein weites, nur noch lose an die Erforderlichkeit zum Betrieb des Produkts anknüpfendes Verständnis der Verbundenheit des Dienstes mit dem Produkt nahe. Auch nicht im strengeren Sinne zum Betrieb des Produkts erforderliche Dienste, wie etwa Textverarbeitungsprogramme, könnten bei einem solch weiten Verständnis den Verpflichtungstatbeständen zugeordnet werden mit der Folge, dass nahezu jede Software dem Anwendungsbereich unterfiele. Die in Art. 7 Abs. 2 enthaltene einschränkende Formulierung *„soweit diese für den Zugang zu einem Produkt oder verbundenen Dienst oder dessen Steuerung benutzt werden“* erscheint zur Begren-

zung des Anwendungsbereichs wenig geeignet, weil damit nahezu der gesamte denkbare Einsatzbereich eines virtuellen Assistenten erfasst wird. Einzig der sehr überschaubare Kreis der Kleinst- und Kleinunternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG ist gemäß Art. 7 Abs. 1 von Verpflichtungen zur Zugänglichmachung bzw. Zurverfügungstellung von Daten ausgenommen. Allerdings knüpft diese Ausnahme daran an, dass diese Unternehmen die Produkte bzw. Dienstleistungen herstellen bzw. erbringen. Die genannten Verpflichtungen gelten jedoch unabhängig von der Herstellung oder Erbringung für alle Dateninhaber. Damit könnten Kleinunternehmen gerade in Bereichen, in denen sie auf die Datenerhebung keinen Einfluss haben, weiter zur Zurverfügungstellung verpflichtet bleiben. Eine nennenswerte Entlastung von Kleinunternehmen würde so nicht geschaffen.

1.1 Insbesondere: Definition Dateninhaber

Insbesondere soweit die im Entwurf vorgesehenen Verpflichtungen und Berechtigungen – etwa in Art. 4 Abs. 1 – an die Eigenschaft als Dateninhaber anknüpfen, erscheint der Anwendungsbereich zu weit und unklar gefasst. Als Dateninhaber werden in Art. 2 Nr. 6 juristische oder natürliche Personen definiert,

> *„die nach dieser Verordnung, nach anwendbarem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen.“*

Zunächst ist unklar, wie die Wendung *„bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption“* in diesem Zusammenhang zu verstehen ist. Der Wortlaut legt ein Verständnis nahe, wonach die einschränkende Bedingung der Kontrolle über die technische Konzeption nur für nicht personenbezogene Daten gelten soll, sodass die Verpflichtungen und Berechtigungen hinsichtlich des wohl überwiegenden und kritischeren Teils der Daten – nämlich der personenbezogenen – bestehen bliebe.

Ferner erscheint die Definition des Dateninhabers in Teilen zirkelschlüssig. Denn einige Verpflichtungen nach der Verordnung setzen die Eigenschaft als Dateninhaber voraus. Zugleich wird aber als Dateninhaber u. a. definiert, wer nach der Verordnung verpflichtet ist. Es fragt sich daher, ob, zur Vermeidung des Zirkelschlusses auch lediglich potentiell nach der Verordnung Verpflichtete als Dateninhaber anzusehen sind. Dass, bei gegenteiliger Auslegung, gerade Adressaten, die nach keiner anderen Vorschrift zu Datenbereitstellung verpflichtet sind, von der diesbezüglichen Verpflichtung nach dieser Verordnung ausgenommen werden, dürfte kaum beabsichtigt sein. Rechtsanwender dürften daher geneigt sein, das Tatbestandsmerkmal „nach dieser Verordnung … verpflichtet“ in dem Sinne weit zu verstehen, dass auch die potenzielle Verpflichtung nach der Verordnung ausreicht.

Damit erscheint der Regelungsbereich der Verordnung – bei allen Unklarheiten – auch insoweit zu weitgehend gefasst als er durch die Eigenschaft des Dateninhabers definiert wird. Es erscheint erwägenswert, den Regelungsbereich durch eine engere Definition des Dateninhabers einzugrenzen, um überbordende, Arbeitsabläufe und Innovationen potentiell beeinträchtigende Regulierung zu vermeiden.

Im Interesse der Normenklarheit sollten zudem die angesprochenen Unklarheiten bei der Definition des Dateninhabers beseitigt werden.

1.2 Folge: Unzumutbar weitreichende Verpflichtungen

Der bislang intendierte und weit gefasste Regelungsbereich wird zwangsläufig Sachverhalte erfassen, in denen die Befolgung insbesondere der Pflicht zur Bereitstellung von Daten nicht sachgerecht oder zumutbar ist. Neben wirtschaftlichen oder organisatorischen Gründen wird es einigen Normadressaten

vor allem aus rechtlichen Gründen nicht zumutbar sein, diese Verpflichtung zu erfüllen. Dies gilt insbesondere für Berufsgeheimnisträger. Die in dem Entwurf vorgesehenen Ausnahmen etwa für Kleinunternehmen oder mit Blick auf Geschäftsgeheimnisse erscheinen unzureichend, um Härtefälle zu vermeiden. Es fehlen insbesondere Ausnahmen für Berufsgeheimnisträger.

1.3 Empfehlung: Einschränkende Definitionen und bereichsspezifische Ausnahmen

Die Bundesrechtsanwaltskammer empfiehlt, den Regelungsbereich der Verordnung durch klarere und eingrenzende Formulierungen zu konturieren bzw. einzuschränken. Neben der angesprochenen Überarbeitung der Definition des Dateninhabers sollten insbesondere strengere Anforderungen an die Erforderlichkeit eines Dienstes zum Betrieb eines Produktes erwogen werden.

1.3.1 Regelungsvorschlag Kleinunternehmen

Die Ausnahme des Art. 7 Abs. 1 sollte auch auf solche Kleinunternehmen ausgedehnt werden, die keine Produkte herstellen bzw. erbringen. Art. 7 Abs. 1 sollte daher lauten:

> *„Die Pflichten dieses Kapitels gelten nicht für* ~~***Daten, die bei der Nutzung von Produkten oder verbundenen Diensten erzeugt werden, die von Unternehmen hergestellt bzw. erbracht werden, die als***~~ *Kleinst- oder Kleinunternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG* ~~***gelten***~~*, sofern diese Unternehmen keine Partnerunternehmen oder verbundenen Unternehmen im Sinne des Artikels 3 des Anhangs der Empfehlung 2003/361/EG haben, die nicht als Kleinst- oder Kleinunternehmen gelten.“*
>
> *(Änderungen hervorgehoben)*

1.3.2 Regelungsvorschlag Bereichsausnahmen

Weitere Ausnahmen sollten für Bereiche vorgesehen werden, in denen die vorgesehenen Pflichten aus organisatorischen, wirtschaftlichen oder rechtlichen Gründen nicht oder nicht in zumutbarer Weise erfüllt werden können. Sektoren, die einem Berufsgeheimnis unterliegen, sollten vom Anwendungsbereich der Verordnung, jedenfalls aber von der Pflicht zur Bereitstellung von Informationen, ausgenommen werden.

In Art. 1 Abs. 2 sollte daher ein neuer Satz 2 aufgenommen werden:

> *„Diese Verordnung begründet keine Verpflichtungen für Berufsgeheimnisträger.“*

In diesem Satz könnten weitere Gruppen bzw. Sektoren aufgeführt werden, von denen zu erwarten steht, dass sie die Verpflichtungen aus organisatorischen, wirtschaftlichen oder rechtlichen Gründen regelmäßig nicht in zumutbarer Weise erfüllen könnten.

2. Schutz der anwaltlichen Verschwiegenheit und Unabhängigkeit

Jedenfalls soweit Verletzungen der anwaltlichen Verschwiegenheit und Beeinträchtigungen der anwaltlichen Unabhängigkeit nicht durch die vorgeschlagenen Beschränkungen und Bereichsausnahmen ausgeschlossen werden, bedarf es zudem effektiver Schutzklauseln. Es muss sichergestellt werden, dass für Anwältinnen und Anwälte sowie für die Rechtsanwaltskammern keinerlei Pflicht aus der Verordnung abgeleitet werden kann, über Mandatshinhalte oder auch nur Umstände einer Mandatierung Auskunft zu erteilen. Die derzeit im Verordnungsentwurf vorgesehenen Vorschriften zum Schutz personenbezogener Daten und von Geschäftsgeheimnissen sind nicht ausreichend, um zugleich einen verfassungs-, konventions- und unionsrechtlichen Anforderungen genügenden Schutz des Mandatsgeheimnisses zu gewährleisten. Denn dem Mandatsgeheimnis können auch Daten unterfallen, die weder personenbezogen sind noch einem Geschäftsgeheimnis unterliegen. Zudem sind mit Blick auf das Mandatsgeheimnis strengere unions-, verfassungs- und konventionsrechtliche Anforderungen zu beachten.

2.1 Regelungsvorschläge zum Schutz der anwaltlichen Verschwiegenheit

Die anwaltliche Verschwiegenheit ist eine Voraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit ein Grundpfeiler eines jeden Rechtsstaats. Sie unterfällt dem Schutz der europäischen wie nationalen Rechtsstaatsgarantien aus Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK sowie Art. 20 Abs. 2 GG, Art. 103 Abs. 1 GG. Zugleich ist sie im Kontext anwaltlicher Beratung Voraussetzung für die Verwirklichung europäischer wie nationaler Grundrechte aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG. Sie dient in erster Linie dem Schutz des Mandanten und seines Zugangs zum Recht. Das Mandatsgeheimnis schützt Opfer, Täter und sonstige Rechtsuchende gleichermaßen. Wird sein Schutz nicht gewährleistet und können Mandanten daher keinen Rechtsrat in Anspruch nehmen, wird dadurch zugleich die Anwaltschaft in ihrer Berufsausübungsfreiheit beeinträchtigt.

2.1.1 Regelung des allgemeinen Verschwiegenheitsschutzes und des Verhältnisses zu mitgliedstaatlichem Recht

Für einen angemessenen Schutz des Mandatsgeheimnisses bedarf es zunächst in Artikel 1 einer grundlegenden Klarstellung, dass neben den Regelungen zum Schutz personenbezogener Daten auch solche zum Schutz von Berufsgeheimnissen und namentlich des Mandatsgeheimnisses unberührt bleiben. Da diese im Wesentlichen durch nationales Recht bestimmt werden, muss auch auf dieses verwiesen und dessen ausnahmsweiser Anwendungsvorrang sichergestellt werden.

Es wird vorgeschlagen, zu diesem Zweck in Artikel 1 als neuen Absatz 5 die folgende Formulierung aufzunehmen:

> *„(5) Nationale sowie unions- und konventionsrechtliche Regelungen betreffend die Ausübung freier Berufe und namentlich zum Schutz von Berufsgeheimnissen bleiben unberührt. Keine Vorschrift dieser Verordnung darf so verstanden werden, dass der Bruch eines Berufsgeheimnisses verlangt werden kann. Träger von Berufsgeheimnissen unterliegen den Verpflichtungen nach dieser Verordnung nicht, soweit eine getrennte Verarbeitung von dem Berufsgeheimnis unterliegenden Daten und solchen, bei denen das nicht der Fall ist, nicht in zumutbarer Weise möglich ist.“*

2.1.2 Spezifische Regelungen zum Schutz der Verschwiegenheit

Ferner sollte der Schutz von Berufsgeheimnissen und weiteren Vertraulichkeitstatbeständen wie folgt gewährleistet werden:

2.1.2.1 Zur Zugänglichkeit gemäß Art. 3 Abs. 1

Gemäß Art. 3 Abs. 1 sind Produkte und verbundene Dienste so zu konzipieren, herzustellen bzw. zu erbringen, dass die bei ihrer Nutzung erzeugten Daten standardmäßig direkt zugänglich sind.

Die ferner in Art. 3 Abs. 1 angeordnete Sicherheit der Datenzugänglichkeit ist nicht ausreichend, um insbesondere in Fällen gemischter Datenhaltungen die Vertraulichkeit personenbezogener oder einem Berufs- oder Geschäftsgeheimnis unterliegender Daten im erforderlichen Umfang zu gewährleisten. Die Vorschrift sollte daher wie folgt ergänzt werden:

> *(1) Produkte werden so konzipiert und hergestellt und verbundene Dienste so erbracht, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind.* ***Ein Zugang zu personenbezogenen oder einem Berufs- oder Geschäftsgeheimnis unterliegenden Daten, auf die der Nutzer nicht zugreifen darf, darf nicht eröffnet werden.***
>
> *(Hinzufügung hervorgehoben)*

2.1.2.2 Zur Bereitstellung gemäß Art. 4 Abs. 1

Gemäß Art. 4 Abs. 1 können Nutzer eine Datenbereitstellung gegenüber Dritten verlangen.

Mit Blick auf die in Art. 4 Abs. 1 vorgesehene Datenbereitstellung enthält der Entwurf begrüßenswerter Weise Sicherungen zum Schutz personenbezogener bzw. einem Geschäftsgeheimnis unterliegender Daten. Für Daten, die einem Berufsgeheimnis unterliegen, fehlt ein entsprechender Schutz indes. Art. 4 muss daher wie folgt um einen siebten Absatz ergänzt werden:

> *„(7) Einem Berufsgeheimnis unterliegende Daten dürfen nicht bereitgestellt werden."*

2.1.2.3 Zur Bereitstellung gegenüber Dritten gemäß Art. 5

Gemäß Art. 5 Abs. 1 können Nutzer eine Datenbereitstellung gegenüber Dritten verlangen.

Art. 8 regelt die bei dieser Datenbereitstellung gegenüber Dritten zu beachtenden Bedingungen. Auch insoweit wurde zwar der Schutz personenbezogener sowie Geschäftsgeheimnissen unterliegender Daten bedacht; Anordnungen zum Schutz von Berufsgeheimnissen fehlen jedoch. Auch Art. 8 bedarf daher der folgenden Ergänzung eines siebten Absatzes:

> *„(7) Einem Berufsgeheimnis unterliegende Daten dürfen nicht bereitgestellt werden."*

2.1.2.4 Zu Datenzugriffen durch öffentliche Stellen

Gemäß Art. 14 Abs. 1 können öffentliche Stellen sowie Organe, Einrichtungen oder sonstige Stellen der Union vom Dateninhaber bei Vorliegen einer außergewöhnlichen Notwendigkeit die Bereitstellung der Daten verlangen.

Insoweit enthält der Entwurf in Art. 17 Abs. 2 lit. c und d, Art. 18 Abs. 5 und Art. 19 Abs. 2 vertraulichkeitsschützende Klauseln. Indes wird auch in diesem Zusammenhang ein Schutz von Berufsgeheimnissen unterliegenden Daten nicht gewährleistet. Dieser ist wie nachstehend dargestellt zu ergänzen. Dabei ist zu beachten, dass für Zugriffe auf dem Mandatsgeheimnis unterliegende Daten primär-, konventions- und verfassungsrechtlich höhere Anforderungen gelten als etwa mit Blick auf personenbezogene Daten und Geschäftsgeheimnisse.

2.1.2.4.1 Anforderungen an das Datenzugangsverlangen der öffentlichen Stelle gemäß Art. 17 Abs. 2

Gemäß Art. 17 Abs. 2 lit. c des Entwurfs müssen die die rechtmäßigen Ziele des Dateninhabers u. a. unter Berücksichtigung des Schutzes von Geschäftsgeheimnissen berücksichtigt werden; gemäß Art. 17 Abs. 2 lit. d dürfen Datenzugangsverlangen, soweit möglich, nur nicht personenbezogene Daten betreffen. Es fehlen indes eine allgemeine Anordnung zum Schutz der Interessen potentiell betroffener Dritter sowie von Berufsgeheimnissen unterliegenden Daten. Art. 17 Abs. b lit. c sollte daher wie folgt ergänzt werden:

(2) Ein Datenverlangen nach Absatz 1 muss

a) in klarer, prägnanter, einfacher und für den Dateninhaber verständlicher Sprache abgefasst sein;

b) im Hinblick auf die Granularität und den Umfang der verlangten Daten sowie die Häufigkeit des Zugangs zu den verlangten Daten in einem angemessenen Verhältnis zu der außergewöhnlichen Notwendigkeit stehen;

c) die rechtmäßigen Ziele des Dateninhabers unter Berücksichtigung des Schutzes von Geschäftsgeheimnissen und der Kosten und des nötigen Aufwands der Datenbereitstellung achten ***sowie die Interessen betroffener Dritter berücksichtigen****;*

d) soweit wie möglich nur nicht personenbezogene Daten betreffen;

e) ***den Schutz von Berufsgeheimnissen und insbesondere des Mandatsgeheimnisses achten***

f) ~~***e)***~~ *dem Dateninhaber Aufschluss über die Sanktionen geben, die nach Artikel 33 von einer nach Artikel 31 zuständigen Behörde verhängt werden, wenn er dem Verlangen nicht nachkommt;*

g) ~~***f)***~~ *ohne ungebührliche Verzögerung online veröffentlicht werden.*

(Änderungen hervorgehoben)

2.1.2.4.2 Anforderungen an die Erfüllung des Datenzugangsverlangens gemäß Art. 18

In Art. 18 werden Anforderungen an die Erfüllung des Datenzugangsverlangens formuliert. Diese reichen zur Wahrung des Mandatsgeheimnisses nicht aus. Insbesondere die in Art. 18 Abs. 5 unter einem Möglichkeitsvorbehalt vorgesehene Pseudonymisierung personenbezogener Daten reicht hierzu nicht aus. Zum Schutz des Mandatsgeheimnisses sollte daher wie folgt ein neuer Artikel 6 eingefügt werden:

(6) Einem Berufsgeheimnis unterliegende Daten dürfen der anfragenden Stelle nicht offenbart werden.

~~***(6)***~~***7*** *Möchte die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union der Ablehnung eines Dateninhabers, die verlangten Daten bereitzustellen, oder der von ihm beantragten Änderung des Verlangens widersprechen oder möchte der Dateninhaber Einspruch gegen das Verlangen einlegen, so wird die in Artikel 31 genannte zuständige Behörde mit der Angelegenheit befasst.*

(Änderungen hervorgehoben)

2.1.2.4.3 Pflichten öffentlicher Stellen im Umgang mit erhaltenen Daten gemäß Art. 19

Art. 19 regelt die beim Umgang mit erhaltenen Daten von öffentlichen Stellen zu beachtenden Pflichten. Auch an dieser Stelle fehlen ergänzend zu dem in Art. 19 Abs. 1 lit. b bzw. Abs. 2 Satz vorgesehenen Schutz von personenbezogenen Daten bzw. Geschäftsgeheimnissen Anordnungen zum Schutz von Berufsgeheimnissen. Art. 19 sollte daher um den folgenden dritten Absatz ergänzt werden:

(3) Sofern der anfragenden Stelle Daten offenbart werden, die einem Berufsgeheimnis unterliegen,

a) ist sie im mitgliedstaatlich für den Berufsträger vorgesehenen Umfang ihrerseits zur Verschwiegenheit hinsichtlich der betroffenen Informationen verpflichtet

b) vernichtet bzw. löscht sie, soweit möglich, die erlangten Daten, oder trifft übrigenfalls hinreichende technisch-organisatorische Maßnahmen, um Offenbarungen der Informationen an Dritte sowie bei der Stelle selbst tätiges Personal zu verhindern

2.1.2.4.4 Weitergabe an Forschungsorganisationen oder statistische Ämter gemäß Art. 21

Art. 21 Abs. 1 ermöglicht öffentlichen Stellen eine Datenweitergabe an Forschungsorganisationen. Art. 21 Abs. 3 erklärt in diesem Zusammenhang die in Art. 17 Abs. 3 und Art. 19 vorgesehenen Sicherheitsmaßgaben auf die empfangenden Stellen für anwendbar. Die in dieser Stellungnahme zu Art. 19 enthaltenen Ausführungen gelten insoweit entsprechend. Im Übrigen reicht der Verweis auf Art. 17 Abs. 3 und Art. 19 nicht aus, um einen hinreichenden Schutz des Mandatsgeheimnisses zu gewährleisten. Es bedarf ergänzend eines Verweises auf Art. 18 inklusive des darin zum Schutz von Berufsgeheimnissen neu aufzunehmenden Absatzes 6 (siehe dazu oben 2.1.2.4.2 Anforderungen an die Erfüllung des Datenzugangsverlangens gemäß Art. 18). Alternativ könnte der Schutz von Berufsgeheimnissen auch direkt in Art. 21 angeordnet werden.

2.1.2.5 Grenzüberschreitender Datenaustausch

Die Verordnung findet auch auf grenzüberscheitende Sachverhalte Anwendung. Mit Blick auf Datenzugriffsanforderungen durch öffentliche Stellen trägt Art. 22 Abs. 3 diesem Umstand in Teilen Rechnung.

2.1.2.5.1 Regelung zum Ausgleich und zum Schutz divergierender Vertraulichkeitsanforderungen

Es fehlt indes eine Regelung, mit der die zwischen den Mitgliedstaaten teils divergierenden Vertraulichkeitsanforderungen zu einem Ausgleich gebracht und ein hinreichender Schutz von Berufsgeheimnissen und insbesondere des Mandatsgeheimnisses gewährleistet wird. Art. 22 Abs. 3 sollte daher wie folgt ergänzt werden:

(3) Beabsichtigt eine öffentliche Stelle, von einem Dateninhaber, der in einem anderen Mitgliedstaat niedergelassen ist, die Bereitstellung von Daten zu verlangen, so teilt sie diese Absicht zunächst der in Artikel 31 genannten zuständigen Behörde des betreffenden Mitgliedstaats mit. Dies gilt auch für Zugangsverlangen von Organen, Einrichtungen und sonstigen Stellen der Union. ***In dem Mitgliedstaat des Dateninhabers geltende Vertraulichkeitsanforderungen wie etwa dort bestehende Berufsgeheimnisse werden in vollem Umfang auch durch die aus einem anderen Mitgliedstaat abrufende Stelle geachtet. Sofern gleichwohl ein Abruf geschützter Informationen erfolgt, gilt Art. 19 Abs. 3; maßgeblich bleibt dabei das Recht des Mitgliedstaats des Dateninhabers.***

2.1.2.5.2 Schutz von Berufsgeheimnissen bei Drittstaatsbezug

Kapitel VII des Entwurfs enthält in Art. 27 Maßgaben zum Schutz nicht personenbezogener Daten im internationalen Umfeld und bezieht sich dabei im Wesentlichen auf Drittstaatskonstellationen (Art. 27 Abs. 2 – 5). Hierbei sind – vergleichbar den Regelungen in der DSGVO – besondere und zusätzliche Anforderungen zu stellen.

Die Ausklammerung personenbezogener Daten in diesem Kapitel dürfte der zutreffenden Erwägung geschuldet sein, dass diese Drittstaatstransfers personenbezogener Daten in den datenschutzrechtlichen Rechtsakten der Union abschließend geregelt sind bzw., soweit Verbesserungsbedarf erkannt wird, zu regeln sind.

Indes bedarf es nach Ansicht der Bundesrechtsanwaltskammer mit Blick auf das Mandatsgeheimnis ergänzender Schutzvorschriften in Art. 27 – dies ungeachtet eines etwaig bestehenden Personenbezuges. Denn aufgrund der divergierenden Schutzbereiche und Schutzziele des Mandatsgeheimnisses einerseits und des Datenschutzrechts und des Schutzes von Geschäftsgeheimnissen andererseits sowie in Ermangelung einer unionsrechtlichen Regelungskompetenz kann weder den bestehenden Vorschriften zum Schutz personenbezogener Daten noch den vorgeschlagenen Vorschriften zum Schutz nicht personenbezogener Daten bei Drittstaatsverarbeitungen mit Blick auf das Mandatsgeheimnis eine abschließende Regelung entnommen werden. Der durch diese Vorschriften vermittelte Schutz wäre auch nicht ausreichend.

Als neuer Art. 4 sollte daher in Art. 27 die nachfolgende Formulierung aufgenommen werden:

> *(4) Berufsgeheimnissen und namentlich dem Mandatsgeheimnis unterliegende Informationen dürfen nur nach Maßgabe und im Umfang der hierfür im Ausgangsstaat geltenden Regeln offenbart werden.*

Die gegenwärtigen Art. 4 und 5 müssten entsprechend neu in Art. 5 bzw. 6 nummeriert werden. Um den erweiterten Regelungsgehalt abzubilden, sollte ferner die Kapitelüberschrift wie folgt neu gefasst werden:

> *Kapitel VII*
>
> *Schutzvorkehrungen für nicht personenbezogene **und Berufsgeheimnissen unterliegende** Daten im internationalen Umfeld*
>
> *(Hinzufügungen hervorgehoben)*

2.2 Regelung betreffend den Schutz der anwaltlichen Unabhängigkeit und Selbstverwaltung in Art. 31

Die anwaltliche Unabhängigkeit ist gemäß Art. 47 Abs. 2 der Grundrechtecharta zu garantieren und als Rechtsgrundsatz in allen Mitgliedstaaten anerkannt. In Deutschland gewährleistet das Grundgesetz dem Rechtsanwalt eine von staatlicher Kontrolle und Bevormundung freie Berufsausübung und schützt dazu insbesondere das Vertrauensverhältnis zwischen Anwalt und Mandant (vgl. BVerfGE 113, 29 [49]). Integrität und Zuverlässigkeit des einzelnen Berufsangehörigen (vgl. BVerfGE 63, 266 [286] sowie das Recht und die Pflicht zur Verschwiegenheit (vgl. BVerfGE 76, 171 [190]) sind die Grundbedingungen dafür, dass dieses Vertrauen entstehen kann. Maßnahmen, die geeignet sind, das Entstehen des Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant auch nur im Ansatz zu stören oder gar auszuschließen, greifen nicht nur in die Subjektstellung des Mandanten, sondern auch in die Berufsausübungsfreiheit des Rechtsanwalts ein. Die Tätigkeit des Rechtsanwalts liegt dabei auch im Interesse

der Allgemeinheit an einer wirksamen und geordneten Rechtspflege (zu allem vgl. BVerfG NJW 2010, 1740 m.w.N.). Aus diesen Gründen muss auch die Aufsicht über die Berufsausübung eine unabhängige und selbstverwaltete sein. In Deutschland obliegt die Aufsicht über die Rechtsanwaltschaft daher der anwaltlichen Selbstverwaltung bestehend aus 28 Rechtsanwaltskammern. Diese selbst sind Ausdruck anwaltlicher Staatsferne und Unabhängigkeit. Sie werden durch die Bundesrechtsanwaltskammer als Dachorganisation repräsentiert.

Art. 31 Abs. 1 lit. a des Entwurfs weist die Aufsicht über die Anwendung der Verordnung mit Blick auf personenbezogene Daten – und damit des wohl überwiegenden Anwendungsbereichs – jedoch den derzeit zuständigen Datenschutzaufsichtsbehörden zu, deren Zuständigkeit im anwaltlichen Bereich bereits auf dem früheren Versäumnis des EU-Gesetzgebers beruht, in der Datenschutz-Grundverordnung eine Öffnungsklausel für eine selbstverwaltete Aufsicht zu schaffen.

Die Bundesrechtsanwaltskammer erneuert daher in diesem Zusammenhang ihre Forderung, die Voraussetzungen zur Einrichtung einer selbstverwalteten und unabhängigen Datenschutzaufsicht der Anwaltschaft zu schaffen und zu diesem Zweck insbesondere eine entsprechende Öffnungsklausel in der Datenschutz-Grundverordnung einzuführen (siehe hierzu bereits BRAK-Stellungnahmen 52/2021, 3/2021, 16/2020, 41/2016). Es ist unabdingbar, dass Rechtsanwältinnen und Rechtsanwälte ihre Tätigkeit auch und gerade mit Blick auf in ihrer Sphäre entstehende oder verarbeitete Daten in völliger Unabhängigkeit ausüben und über die im Rahmen ihrer Tätigkeit erfolgenden Datenverarbeitungen frei und einzig am Mandatsinteresse sowie ihren rechtsstaatlich vorgegebenen Berufspflichten orientiert entscheiden.

Begrüßenswert ist zwar, dass der Entwurf in Art. 31 Abs. 2. lit. b vorsieht, dass bei spezifisch sektoralen Problemen des Datenaustauschs die Zuständigkeit der sektoralen Fachbehörde – im Falle anwaltlicher Datenverarbeitungen also der Rechtsanwaltskammer – respektiert werden soll. Diese Vorschrift muss im Mindesten beibehalten werden. Sie ist jedoch aus den genannten rechtlichen Gründen nicht ausreichend. Hinzu kommt, dass die derzeit zuständigen Datenschutzaufsichtsbehörden die Zuständigkeiten der Rechtsanwaltskammern nicht immer respektieren (vgl. bereits BRAK-Stellungnahme 3/2021), sodass die hinreichende Eignung von Art. 31 Abs. 2. lit. b, eine Berücksichtigung sektoraler Belange herbeizuführen, auch in praktischer Hinsicht infrage steht.

Im Interesse der Wahrung der gemäß Art. 47 Abs. GRCh zu gewährleistenden anwaltlichen Unabhängigkeit sollte Art. 31 Abs. 2 lit. b des Entwurfs daher wie folgt ergänzt werden:

> *b) bei besonderen sektoralen Problemen des Datenaustauschs im Zusammenhang mit der Anwendung dieser Verordnung bleibt die Zuständigkeit der Fachbehörden gewahrt;* ***die Überwachung der Einhaltung der Verordnung durch Rechtsanwälte und Rechtsanwaltskanzleien bleibt der anwaltlichen Selbstverwaltung vorbehalten;***

3. Verhältnis der Verordnung zum bestehenden Datenschutzregime

Das Verhältnis zwischen dem bestehenden Datenschutzrechtsregime, insbesondere der DS-GVO, und der hier angestrebten Verordnung ist klärungsbedürftig. Denn zunächst wird in Art. 1 Abs. 3 des Entwurfs diesbezüglich angeordnet, dass die bestehenden Vorschriften und namentlich die DS-GVO auch auf Datenverarbeitungen nach der Verordnung anwendbar seien. Allerdings besagen Art. 4 Abs. 5 und Art. 5 Abs. 6 des Entwurfs, dass unter den dort genannten Voraussetzungen die Art. 6 Abs. 1 und 9 der DS-GVO anwendbar seien. Damit fragt sich für den Rechtsanwender, was in Fällen gelten soll, in denen diese Voraussetzungen nicht erfüllt sind. Es ist nicht ersichtlich, ob der Verweis auf Art. 6 Abs. 1 DS-GVO lediglich klarstellend zu verstehen ist, oder die Verordnung in diesem – sowie möglicherweise weiteren Punkten – einen eigenen datenschutzrechtlichen Erlaubnistatbestand schaffen will. Zu letzterer Annahme könnten sich Rechtsanwender etwa durch einen Umkehrschluss veranlasst sehen. Für einen lediglich klarstellenden Charakter spricht demgegenüber Art. 1 Abs. 3. Hier sollte Rechtsklarheit geschafften werden. Falls lediglich eine Klarstellung beabsichtigt ist, sollte entweder in Art. 1 Abs. 3 der klarstellende Charakter der Bezugnahmen aus Art. 4 Abs. 5 und Art. 5 Abs. 6 erläutert oder die dortigen Bezugnahmen gestrichen werden. Sofern demgegenüber die Anwendbarkeit von Art. 6 Abs. 1 und Art. 9 der DS-GVO tatsächlich vom Vorliegen der Voraussetzungen der Artt. 4 Abs. 5 bzw. 5 Abs. 6 abhängig gemacht, im Übrigen jedoch an der Geltung der DS-GVO festgehalten werden soll, sollte dies ebenfalls in Art. 1 Abs. 3 klargestellt werden – z. B. durch den Zusatz

> *„Sofern die Anwendbarkeit der genannten Bestimmungen in dieser Verordnung in Einzelfällen vom Vorliegen weiterer Voraussetzungen abhängig gemacht wird, wird deren Anwendung im Übrigen hierdurch nicht berührt.“*

* * *