



BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 3/2021 Januar 2021

ZUR Evaluierung des Bundesdatenschutzgesetzes

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RA Dr. Wulf Kamlah
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

Bundesrechtsanwaltskammer

The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus

Littenstraße 9 Tel. +49.30.28 49 39 - 0
10179 Berlin Fax +49.30.28 49 39 -11
Deutschland Mail zentrale@brak.de

Büro Brüssel

Avenue des Nerviens 85/9 Tel. +32.2.743 86 46
1040 Brüssel Fax +32.2.743 86 56
Belgien Mail brak.bxl@brak.eu

Verteiler: Bundesministerium des Innern, für Bau und Heimat
Bundesministerium für Justiz und Verbraucherschutz
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 (BRAK) 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 Gelegenheit einer Stellungnahme im Rahmen der BDSG-Evaluierung. Der Evaluationsfragebogen lässt sich nur in Teilen aus gesamtanwaltlicher Perspektive beantworten. Die vorliegende Stellungnahme bezieht sich lediglich auf die Fragen, die die anwaltliche Berufsausübung und die anwaltliche Selbstverwaltung an sich betreffen.

A.

Zu Frage II. 3. Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 26 bis 31 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die in § 29 Abs. 3 BDSG zum Schutz von Berufsgeheimnissen vorgesehenen Beschränkungen der Aufsichtsbefugnisse sind zu eng gefasst, um den Schutz des verfassungsrechtlich zwingend gebotenen Mandatsgeheimnisses wirksam zu gewährleisten. § 29 Abs. 3 BDSG begrenzt die Aufsichtsbefugnisse nur für die Fälle des Art. 58 Abs. 1 lit. e und f DSGVO. Weitere Einschränkungen sind nach dem Wortlaut der zugrunde liegenden Öffnungsklausel des Art. 90 Abs. 1 DSGVO – trotz im Gesetzgebungsverfahren zur DSGVO von der Bundesregierung und der BRAK entsprechend vorgetragener Forderungen – gegenwärtig nicht vorgesehen. In der Folge haben Aufsichtsbehörden in mehreren Fällen von dem ihnen dem Wortlaut des Art. 58 Abs. 1 lit. a DSGVO zustehenden Auskunftsrecht in einer Weise Gebrauch gemacht, die zu einem Bruch des Mandatsgeheimnisses führen musste. Konkret wurden Anwälte unter Zwangsgeldandrohung zur Auskunft über Mandatsinhalte aufgefordert, obwohl diese Maßnahme angesichts der abzuwägenden Rechte und Interessen – aufseiten der Mandantschaft und der Anwaltschaft namentlich des Mandatsgeheimnisses und des Rechts, nicht sehenden Auges Standesrecht brechen und einen Straftatbestand verwirklichen zu müssen – offensichtlich nicht verhältnismäßig waren. Es bedarf daher dringend einer gesetzlichen Anordnung, die den Aufsichtsbehörden Aufsichtsbefugnisse auch in solchen und allen anderen Fällen, in denen das Mandatsgeheimnis verletzt werden würde, klar einschränkt. Dies gilt umso mehr, als die datenschutzrechtliche Aufsicht über die Anwaltschaft derzeit – systemwidrig und unter Missachtung rechtsstaatlicher und verfassungsrechtlicher Anforderungen – außerhalb der anwaltlichen Selbstverwaltung angesiedelt ist (siehe dazu unten unsere Antwort auf Frage II 2.)

Zwar mag dem Wortlaut des Art. 90 Abs. 1 DSGVO im Umkehrschluss ein Verbot des nationalen Gesetzgebers zu entnehmen sein, die Aufsichtsbefugnisse der Aufsichtsbehörden weiter als in Art. 90 Abs. 1 DSGVO vorgesehen einzuschränken. Der EU-Gesetzgeber wird mit dieser Regelung aber nicht bezweckt oder in Kauf genommen haben, dass Grundrechte und insbesondere rechtsstaatliche Grundpfeiler wie das Mandatsgeheimnis verletzt würden. Eine Grundsatzentscheidung des nationalen Gesetzgebers zur Regelung der ordnungsgemäßen Ermessensausübung und zur Wahrung des Verhältnismäßigkeitsgrundsatzes bei der Ausübung der Aufsichtsbefugnisse ist daher auch in den in Art. 90 Abs. 1 DSGVO nicht genannten Fällen zulässig.

Wir bitten die Bundesregierung vor diesem Hintergrund,

sich für eine bundesgesetzgeberische Grundsatzentscheidung zum Schutz des Mandatsgeheimnisses auch in den Fällen des Art. 58 Abs. 1 a bis d DSGVO einzusetzen.

Daneben bitten wir die Bundesregierung,

sich auch auf europäischer Ebene erneut für einen Schutz des Mandatsgeheimnisses und insbesondere für eine Erweiterung des Art. 90 Abs. 1 DSGVO auf die übrigen Fälle des Art. 58 Abs. 1 DSGVO einzusetzen.

Demgegenüber muss die gelegentlich erhobene Forderung nach einer weiteren Beschränkung der Ausnahmevorschriften des § 29 Abs. 3 BDSG aus verfassungsrechtlichen und rechtsstaatlichen Gründen klar zurückgewiesen werden.

B.

Zu den Fragen IV. 1-5 (Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden)

Zu Frage 1.: Ist die Zusammenarbeit der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Die Zusammenarbeit der Aufsichtsbehörden ist im BDSG unzureichend geregelt. Es fehlt eine Regelung, die eine schnelle Meinungsbildung der unterschiedlichen Aufsichtsbehörden bei gleichgelagerten Sachverhalten fördert. Dabei existieren bereits etliche Beispiele, die nicht nur über den Europäischen Datenschutzausschuss einheitlich interpretiert werden müssten, sondern erst recht innerhalb Deutschlands einheitlich interpretiert werden müssten – insbesondere, wenn dabei Fragen des Verhältnisses vom EU-Datenschutzrecht zu Bundesrecht betroffen sind, wie es etwa bei viel diskutierten Fragen der Verarbeitung von Fotografien von Personen der Fall ist. Auch die unterschiedlichen Bewertungen des Einsatzes z. B. von Produkten zu Videokonferenzen erschweren den rechtskonformen Einsatz bei öffentlichen und nicht-öffentlichen Stellen gleichermaßen, wenn die Einschätzung der Rechtskonformität von der Postleitzahl der einzusetzenden Stelle abhängt.

Zu Frage 2.: Sind die Zuständigkeiten der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Die Zuständigkeiten der Aufsichtsbehörden sind in mehrerlei Hinsicht nicht sachgerecht geregelt.

a) Vorschlag: Zentralisierung der Aufsicht

Um den in der Antwort auf Frage 1 beschriebenen Problemen zu begegnen, ist – unter Beachtung der verfassungsrechtlichen Zuständigkeitsanordnungen – eine bundesweit zentral organisierte Aufsicht anzustreben.

Wie große Teile der deutschen Wirtschaft leidet auch die Anwaltschaft in wirtschaftlicher und organisatorischer Hinsicht unter der föderalen Aufsichtsstruktur und der fehlenden Expertise und Sensibilität für die besonderen Belange der anwaltlichen Arbeit und ihre verfassungsmäßigen Aufgaben in unserem Rechtsstaat.

Besonders kleinere Kanzleien und Unternehmen leiden unter der Kakophonie oft verschiedener Ansichten der Landesdatenschutzbehörden sowohl auf europäischer wie auf nationaler Ebene. Ihnen fehlen die personellen und finanziellen Kapazitäten, sich mit allen Verlautbarungen und einer Vielzahl von Ansichten der Aufsichtsbehörden auseinanderzusetzen und die Risiken, die mit der Befolgung der einen oder anderen Ansicht einhergehen, zu bewerten. Ihnen bleibt nur die Wahl zwischen Entscheidungen auf völlig unsicherer Grundlage („Blindflug“) oder der Aufgabe Ihrer Vorhaben bzw. Tätigkeiten. Kanzleien und Unternehmen, die demgegenüber entsprechende Bewertungskapazitäten aufbringen können, werden hierdurch finanziell erheblich belastet. Nicht zuletzt besteht auch für sie am Ende langwieriger Befassungen mit den vielen Verlautbarungen und Ansichten oft nur die Gewissheit, dass ein rechtssicherer Weg nicht beschritten werden kann.

Die deutschen Aufsichtsbehörden beklagen selbst Vollzugsdefizite und -unterschiede auf europäischer Ebene, weil die nationalen Behörden teils (offen oder verdeckt) sehr verschiedene Ansichten zur DSGVO vertreten und umsetzen. Genau dieses Bild zeigt sich innerhalb Deutschlands, allerdings ohne, dass es dort von den deutschen Aufsichtsbehörden problematisiert wird. Zum Beleg des Gegenteils wird oft angeführt, es habe noch kein Thema gegeben, bei welchem man sich im Rahmen der Vertretung auf europäischer Ebene nicht habe einigen können. Zudem wird auf die Abstimmung und die gemeinsamen Stellungnahmen im Rahmen der Datenschutzkonferenz (DSK) verwiesen. Diese Tatsachen können aber nicht darüber hinwegtäuschen, dass in vielen für die Datenverarbeitungen in Unternehmen und Kanzleien wesentlichen Fragen keine Einigkeit erzielt werden konnte. Hinweise zum Einsatz von Microsoft 365 konnten etwa nur mit neun zu acht Stimmen beschlossen werden. Abstimmungen, die erfolgen, dauern oft zu lang, insoweit seien ebenfalls beispielhaft die Hinweise zu Microsoft 365 genannt, und sind in jedem Fall unverbindlich. Auch die Folgerungen aus dem EuGH-Urteil zum Privacy-Shield (Schrems II) sind unterschiedlichster Natur und z. B. für Anwälte, die Export-Unternehmen beraten, nicht handhabbar. Die in Kanzleien, Unternehmen und Zivilgesellschaft dringend benötigte Sicherheit über die Aufsichtspraxis der Behörden kann so nicht erzielt werden. Da es bei den Abstimmungsverfahren im Rahmen der DSK häufig Meinungsverschiedenheiten zu überwinden – und gelegentlich wohl auch zu überdecken – gilt, sind deren Ergebnisse auch nicht immer hilfreich.

Die Folgen der Auslegungsdifferenzen zwischen den Landesdatenschutzbehörden werden für die datenschutzrechtlich verantwortlichen Stellen auch nicht durch die vermeintlich klaren Zuständigkeitsvorschriften der §§ 17 BDSG ff. gemildert. Denn Rechtsanwälte beraten und vertreten regelmäßig Geschäftspartner und Mandanten in ganz Deutschland, sodass im Ergebnis doch parallele Zuständigkeiten für untrennbare Sachverhalte bestehen. Kanzleien etwa kooperieren zunehmend über Online-Plattformen bzw. -Tools und kommunizieren sowohl mit anderen Berufsträgern als auch mit Mandanten über solche. Mag dabei auch jede Partei in eigener Verantwortlichkeit handeln und damit einer klaren Zuständigkeit unterliegen, so stellt sich doch das Problem, dass eine für alle Beteiligten vertretbare Lösung gefunden werden muss. Schließlich ist auch ein Beteiligter, der weder für den Betrieb der Plattform noch für den Betrieb eines dort angelegten Nutzerkontos verantwortlich ist, verpflichtet zu prüfen, ob die personenbezogenen Daten bei einer Kommunikation über den jeweiligen Dienst einem angemessenen Schutzniveau unterliegen. Dies müsste er verneinen, wenn die für ihn zuständige Aufsichtsbehörde einen vom Mandanten oder Kooperationspartner gewünschten oder bereitgestellten Dienst für nicht datenschutzkonform nutzbar erachtet. Unterschiedliche Ansichten der Berliner und Baden-Württembergischen Aufsichtsbehörden werden etwa im Hinblick auf die Nutzung des Videodienstanbieters Zoom vertreten.

Gelegentlich wird vertreten, dass divergierende Ansichten der deutschen Aufsichtsbehörden der von der DSGVO vorgegebenen Umsetzungs- und Technologieoffenheit geschuldet sei und dass den datenschutzrechtlich verantwortlichen Stellen in Deutschland dadurch Gestaltungsspielräume eröffnet würden. Dabei seien unterschiedliche Auslegungen für die Verantwortlichen von Vorteil, denn sie müssten in der Praxis kein Bußgeld befürchten, wenn wenigstens eine deutsche Aufsichtsbehörde die vorgenommene Datenverarbeitung für rechtmäßig erachte. Diese Argumentation überzeugt nicht, weil sie

außer Acht lässt, dass Verantwortliche in solchen Fällen weiter dem Risiko von Unterlassungs- und Schadensersatzansprüchen sowie Unterlassungsanordnungen ausgesetzt sind. Auf einer solchen Grundlage können Entscheidungen über Verarbeitungsabläufe und insbesondere über oft kostenträchtige Einsätze von IT-Produkten nicht getroffen werden. Dadurch wird die technische und wirtschaftliche Fortentwicklung sowohl der Wirtschaft als auch der Anwaltschaft gehemmt.

In einem Rechtsstaat sollte für jeden Normadressaten so klar wie irgend möglich ersichtlich sein, welche rechtlichen Folgen sein Handeln haben kann. Schon im Volkszählungsurteil (BVerfGE 65, ff.) wurden normenklare und bestimmte Regelungen gefordert. Die derzeitige Aufsichtsstruktur in Deutschland steht dem diametral entgegen.

b) Vorschlag: Sektorale Aufsichtsstruktur

Um den Belangen und Anforderungen unterschiedlicher Sektoren besser gerecht werden zu können und um den durch Datenverarbeitungen in den jeweiligen Sektoren Betroffenen einen bestmöglichen Schutz ihrer Rechte ermöglichen zu können, sollten sektorspezifische Zuständigkeiten geschaffen werden.

Bislang wird ein Bedürfnis nach einer bereichsspezifischeren Aufsichtsausrichtung vor allem unter den Gesichtspunkten technischer Spezialisierung und branchenspezifischer Verarbeitungsvorgänge diskutiert. Allerdings lassen sich daneben – insbesondere im anwaltlichen Bereich (siehe dazu unten) – auch organisatorische und rechtliche Besonderheiten der unterschiedlichen Bereiche hierfür ins Feld führen. Sämtliche derart bereichsspezifische Besonderheiten angemessen zu berücksichtigen, fällt den damit nicht vertrauten Landesdatenschutzbehörden naturgemäß schwer (siehe dazu ebenfalls unten).

Anders als die regionale Aufteilung der Aufsicht in Deutschland haben sich die bereits bestehenden sektoralen Strukturen in den Bereichen Post und Telekommunikation sowie Finanzwesen (BfDI), Kirche (Kirchliche BfD) und Medien (Senderbeauftragte, Presserat) bewährt.

c) Forderung: Unabhängige Datenschutzaufsicht aus der und für die Anwaltschaft

Um den verfassungsrechtlich gebotenen Schutz der anwaltlichen Verschwiegenheit (Mandatsgeheimnis) zu gewährleisten und zugleich die (Datenschutz-)Rechte der durch anwaltliche Datenverarbeitungen Betroffenen wirksam zu schützen, ist die Schaffung einer unabhängigen, zentralen und selbstverwalteten anwaltlichen Datenschutzaufsicht erforderlich.

Die Aufsicht über die Rechtsanwaltschaft obliegt in Deutschland aus verfassungsrechtlichen wie rechtsstaatlichen Gründen der anwaltlichen Selbstverwaltung – bestehend aus 28 Rechtsanwaltskammern. Diese selbst sind Ausdruck anwaltlicher Staatsferne. Sie werden durch die Bundesrechtsanwaltskammer als Dachorganisation repräsentiert.

In datenschutzrechtlicher Hinsicht sind daneben 17 Landesdatenschutzbehörden für die Aufsicht über die Anwälte und Rechtsanwaltskammern zuständig. Allerdings 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.).

Die anwaltliche Verschwiegenheit dient der Gewährleistung einer ganzen Reihe von Grund- und Verfassungsrechten (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, 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG) und ist in einem Rechtsstaat schlicht unabdingbar. Eine Verletzung der Verschwiegenheitsverpflichtungen des Anwalts unterliegt daher aus guten Gründen strengen berufs- und strafrechtlichen Sanktionen, was auch für die Offenbarung von Mandatsgeheimnissen gegenüber den für den Datenschutz zuständigen Aufsichtsbehörden gilt (vgl. KG, NJW 2011, 324 f.).

Allein die vom Bewusstsein anwaltlicher Rechte und Pflichten sowie der gebotenen Praxisnähe und sektorspezifischen Expertise geprägte anwaltliche Selbstverwaltung ist daher Garant der anwaltlichen Unabhängigkeit und Verschwiegenheit, und dies im Interesse des Rechtsuchenden wie der Rechtspflege.

Die datenschutzrechtliche Aufsicht über die Anwaltschaft durch Landesdatenschutzbehörden ist damit weder dogmatisch noch praktisch in Einklang zu bringen. Wie die Vergangenheit zeigt, interpretieren die Landesdatenschutzbehörden die anwaltliche Verschwiegenheitspflicht, je nach Konstellation, zu eng oder zu weit, und dies, obwohl sie für die Auslegung des anwaltlichen Berufsrechts gar nicht zuständig sind.

Wie bereits oben in der Antwort auf Frage II. 3. beschrieben üben einige Aufsichtsbehörden ihre Aufsichtsbefugnisse in einer Weise aus, die das Mandatsgeheimnis verletzt.

Zunehmend häufiger kommt es zudem vor, dass Landesdatenschutzbehörden sich anmaßen, anwaltliches Berufsrecht auszulegen und daraus datenschutzrechtliche Verpflichtungen abzuleiten. Nicht selten wird dabei das anwaltliche Berufsrecht falsch ausgelegt und es werden in der Folge unter Berufung auf eine vermeintlich bestehende Verschwiegenheitspflicht in Wahrheit nicht bestehende besondere datenschutzrechtliche Anforderungen für den anwaltlichen Bereich bzw. die Datenverarbeitung durch Berufsgeheimnisträger formuliert. Jüngere Beispiele hierfür sind die [Empfehlungen der Berliner Landesdatenschutzbeauftragten \(Bln LfDI\) zur Durchführung von Videokonferenzen](#) (Version 1.2 vom 3. Juli 2020) und die [Orientierungshilfe der Datenschutzkonferenz \(DSK\) zu den Anforderungen an Datenübermittlungen per E-Mail](#) vom 13. März 2020 (dort Ziffer 4.2.3). Im erstgenannten Fall wurde behauptet, Berufsgeheimnisträger dürften allein solche Auftragsverarbeiter beauftragen, die im Falle einer Vertraulichkeitsverpflichtung strafrechtlich belangt werden könnten. Dies trifft weder berufs-, noch strafrechtlich zu und würde in Ermangelung der Unternehmensstrafbarkeit de facto dazu führen, dass eine Inanspruchnahme externer Dienstleister entgegen der in § 203 Abs. 3 Satz 2 StGB und § 43e Abs. 1 BRAO vorgesehenen Möglichkeit dies zu tun, nicht erfolgen könnte. Im Falle der Orientierungshilfe der DSK wurde unter Berufung auf die angeblich so bestehende Verschwiegenheitspflicht formuliert, dass die E-Mail-Korrespondenz von Berufsgeheimnisträgern ausschließlich inhaltsverschlüsselt erfolgen dürfe und dass dabei durch zusätzliche Maßnahmen (welche sollten das neben einer Inhaltsverschlüsselung sein?) sichergestellt werden müsse, dass die Korrespondenz ausschließlich Befugten zur Kenntnis gelangen könne. Die BRAK hat hierzu bereits gesondert Stellung genommen ([BRAK-Stellungnahme 47/2020](#)).

Die BRAK fordert vor diesem Hintergrund seit langem die Einführung einer selbstverwalteten und unabhängigen Datenschutzaufsichtsstelle aus der und für die Rechtsanwaltschaft (so etwa in der [BRAK-Stellungnahme 41/2016](#) – auf die dortigen, ausführlichen Begründungen wird ergänzend verwiesen). Diese Forderung nach einer sektoralen Datenschutzaufsicht muss an dieser Stelle bekräftigt werden. Es ist nicht nachvollziehbar, warum Kirchen und öffentlich-rechtlichen Rundfunkanstalten eine eigene

Aufsichtsstelle zugestanden, der Rechtsanwaltschaft aber, die aus rechtsstaatlichen Gründen auf eine solche angewiesen ist, diese bislang versagt wird.

Die BRAK steht mit ihrer bereichsspezifischen und (datenschutz-) rechtlichen Expertise für den Aufbau einer solchen Stelle bereit (siehe auch König in der BRAK-Schriftenreihe, Band 21: „Sektorale Datenschutzkontrolle bei Rechtsanwälten“). Auf die hier vorhandenen Erfahrungen aus der Einrichtung der sehr erfolgreich arbeitenden unabhängigen Schlichtungsstelle der Anwaltschaft kann dabei zurückgegriffen werden.

d) Zusammenspiel der Zuständigkeiten nach BDSG, TMG und TKG verbesserungswürdig

Von dem vorstehend beschriebenen Verbesserungsbedarf abgesehen, erscheinen uns die Zuständigkeitsregelungen innerhalb des BDSG in der Tat sachgerecht, praktikabel und normenklar. Im Zusammenspiel mit anderen Normen mit datenschutzrechtlichen Regelungen wie dem TMG und dem TKG erscheinen die Zuständigkeitsregelungen indes nicht immer konsistent und teils schwer nachvollziehbar.

Zu Frage 3.: Hat sich aus Ihrer Sicht die Regelung in § 40 Absatz 2 BDSG bewährt, wonach sich, wenn der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen hat, die zuständige Aufsichtsbehörde entsprechend Artikel 4 Nummer 16 DSGVO nach der Hauptniederlassung bestimmt?

Aus unserer Sicht hat sich die Regelung in § 40 Absatz 2 BDSG im Hinblick auf unterschiedliche Niederlassungen bewährt. Unabhängig davon ist die Frage des Prozesses zu einer gemeinsamen Entscheidungsfindung der Aufsichtsbehörden. Die mit § 40 Abs. 2 BDSG im Hinblick auf unterschiedliche Niederlassungen erzielte Rechtssicherheit fehlt in den zahlreichen Fällen der länderübergreifenden Zusammenarbeit und Kommunikation mit Kunden, Geschäftspartnern und – für die Anwaltschaft besonders bedeutsam – Behörden, Mandanten, Gerichten und Anwaltskollegen.

Zu Frage 4. Sind die Befugnisse der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Aus unserer Sicht sind die Befugnisse der Aufsichtsbehörden mit Ausnahme des § 29 Abs. 3 (siehe dazu oben unsere Antwort Frage II. 3.) im BDSG ausreichend geregelt.

Zu Frage 5.: Gibt es aus Ihrer Sicht neben den in den Fragen 1 bis 3 angesprochenen Aspekten Änderungsbedarf bei der Regelung der Datenschutzaufsicht im BDSG und wenn ja, worin besteht er?

Sofern und soweit unsere Vorschläge bzw. Forderungen nach einer zentralen, sektoralen und – mit Blick auf die anwaltliche Selbstverwaltung – eigene und unabhängige Datenschutzaufsicht nicht umgesetzt bzw. erfüllt werden sollten, sollte wenigstens auf eine über das bereits erreichte Maß hinausgehende beschleunigte und rechtsverbindliche Abstimmung zwischen den Aufsichtsbehörden hingewirkt werden. Die Geschäftsordnung der DSK – namentlich die in deren Ziffer 3 vorgesehene Struktur zur Meinungsbildung – ist insoweit zwar ein Schritt in die richtige Richtung. Bei interner Unstimmigkeit gibt

es aber weiterhin die Möglichkeit, festgelegte Interpretationen nicht umsetzen zu müssen. Dies wirkt sich nachteilig auf die Rechtssicherheit für Verantwortliche aber auch für die betroffenen Personen aus. Dass die Abstimmungen immer noch viel zu lange dauern, hat sich zuletzt bei der Bewertung von Microsoft-Produkten gezeigt.

* * *