

NICOLAS BAUM

Rechtsanwalt

An den
Anwaltsgerichtshof Berlin
Eißholzstraße 30-33
D-10781 Berlin

Rechtsanwalt Baum, Görlitzer Straße 74, 10997 Berlin

15. Juni 2018

Görlitzer Straße 74
10997 Berlin
Tel +49(0)30 6112021
Fax +49(0)30 6112315
baum@ra-baum.com

in Bürogemeinschaft mit
Johannes Eisenberg,
Prof. Dr. Stefan König,
Dr. Stefanie Schork
Rechtsanwälte

K L A G E

- 1) des Rechtsanwalts Stefan Conen
- 2) des Rechtsanwalts und Syndikusrechtsanwalts Karl Jägen
- 3) des Rechtsanwalts Professor Dr. Remo Klinger
- 4) des Rechtsanwalts Christoph R. Müller
- 5) des Rechtsanwalts Daniel Rink
- 6) des Rechtsanwalts Michael Schinagl
- 7) der Rechtsanwältin Halina Wawzyniak

– Klägerin und Kläger –

Prozessbevollmächtigter: Rechtsanwalt Nicolas Baum, Görlitzer Straße 74,
10997 Berlin,

g e g e n

die Bundesrechtsanwaltskammer, Körperschaft des öffentlichen Rechts, vertreten durch ihren Präsidenten Rechtsanwalt Ekkehart Schäfer

– Beklagte –

w e g e n

Einrichtung eines besonderen elektronischen Anwaltspostfaches mit Ende-zu-Ende-Verschlüsselung

Namens und in Vollmacht der Klägerin und der Kläger wird Klage erhoben und beantragt,

1. die Beklagte zu verurteilen es zu unterlassen, für die Klägerin und die Kläger ein besonderes elektronisches Anwaltspostfach im Sinne des § 31a BRAO ohne eine Ende-zu-Ende-Verschlüsselung empfangsbereit einzurichten, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden,

2. die Beklagte zu verpflichten, für die Klägerin und die Kläger ein besonderes elektronisches Anwaltspostfach im Sinne des § 31a BRAO mit einer Ende-zu-Ende-Verschlüsselung empfangsbereit einzurichten, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden.

GLIEDERUNG

I. Sachverhalt	7
1. Die Klärgemeinschaft.....	7
2. Die Unterstützerinnen und Unterstützer	10
3. Das besondere elektronische Anwaltspostfach (beA).....	11
a) Zweckänderung: Von der elektronischen Kommunikation mit den Gerichten zur Zugangseröffnung für jedermann.....	11
b) Ausnahmslose anwaltliche Nutzungspflicht.....	12
c) Technische Umsetzung	13
aa) Offenkundig gewordene gravierende Sicherheitsmängel.....	14
bb) Im Besonderen: Grundkonzeption ohne Ende-zu-Ende-Verschlüsselung.....	16
(1) Wesenselement einer Ende-zu-Ende-Verschlüsselung	17
(2) Verstoß der beA-System-Architektur gegen das Prinzip der Ende-zu-Ende- Verschlüsselung	19
(a) Erstellung und Speicherung der privaten Schlüssel im HSM sowie Speicherung der privaten Schlüssel in einer Datenbank.....	21
(b) Umschlüsselung im HSM	22
4. Weigerung der Beklagten zur Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung.....	23
II. Rechtliche Würdigung.....	26

1. Zulässigkeit.....	26
a) Eröffnung des Rechtsweges zum Anwaltsgerichtshof Berlin.....	26
b) Sachliche Zuständigkeit.....	27
c) Örtliche Zuständigkeit.....	27
d) Streitgenossenschaft.....	28
e) Statthafte Klageart.....	29
f) Klagebefugnis.....	29
g) Rechtsschutzbedürfnis	32
aa) Begründete Besorgnis der baldigen Inbetriebnahme des beAs ohne Ende-zu-Ende- Verschlüsselung.....	32
bb) Drohende Verletzung des Mandatsgeheimnisses	33
cc) Drohender Verlust des Mandantenstamms	34
dd) Vermeidung von Sanktionen bei Weigerung der Nutzung des beAs ohne Ende-zu-Ende- Verschlüsselung.....	34
2. Begründetheit.....	35
a) Rechtswidrigkeit der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung	35
aa) Verstoß gegen § 31a Absatz 1 BRAO i. V. m. § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO	36
bb) Verstoß gegen § 31a Absatz 1 i. V. m. § 31c Nr. 3 Buchstabe b BRAO i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV.....	38

(1) Grammatik	39
(2) Systematik	39
(3) Historie	40
(4) Telos	41
(5) Verfassungskonforme Auslegung	43
cc) Zwischenergebnis: Rechtswidrigkeit der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung	46
b) Verletzung der Berufsausübungsfreiheit der Klägerin und der Kläger durch rechtswidrige Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung	47
aa) Eingriff in den Schutzbereich	47
bb) Rechtswidrigkeit des Eingriffs	48
c) Anspruch auf Unterlassung der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung ..	49
d) Anspruch auf Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung	49
aa) Schutzzweck: Gewährleistung einer sicheren elektronischen anwaltlichen Kommunikation mit den Gerichten unter Wahrung anwaltlicher Verschwiegenheit.....	50
bb) Schutz des anwaltlichen Individualinteresses an einer sicheren, vertraulichen elektronischen Kommunikation über das beA.....	51
cc) Recht auf Einhaltung der Schutznormen	52
(1) Recht auf rechtmäßiges Handeln der Kammer als der Pflichtmitgliedschaft inhärenter Antagonismus	52
(2) Grundrechtlicher Anspruch auf Rechtmäßigkeit staatlichen Handelns	53

c) Spruchreihe	54
----------------------	----

BEGRÜNDUNG

I. SACHVERHALT

1. DIE KLÄGERGEMEINSCHAFT

Der Kläger zu 1), **Rechtsanwalt Stefan Conen** ist Mitglied der Rechtsanwaltskammer Berlin. Er ist ausschließlich im **Strafrecht** tätig und damit in einem Bereich, in dem es für seine Mandanten nicht nur um **einschneidende Rechtsfolgen**, sondern auch um **sensible Lebenssachverhalte** geht. Der Gesetzgeber hatte daher etwa auch ursprünglich in § 160a Absatz 1 StPO a. F. Strafverteidigern einen herausgehobenen Schutzbereich gegenüber anderen Rechtsanwälten zugebilligt; mittlerweile sind – zu recht – alle Anwälte in § 160a StPO gleichgestellt. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat die **besondere Bedeutung des Schutzes der vertraulichen Kommunikation zwischen Strafverteidiger und Mandant** in ständiger Rechtsprechung betont und einen Verstoß gegen § 160a StPO als Verletzung des **Rechts auf Achtung der beruflichen Verschwiegenheitspflicht nach Artikel 8 EMRK** (Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04. November 1950, zuletzt geändert durch Protokoll Nr. 14 vom 13. Mai 2004 m. W. v. 01. Juni 2010) geahndet (EGMR, Urteil vom 27. April 2017 – 73607/13 Sommer vs. Deutschland). Der Kläger vertritt teilweise **prominente Mandanten in strafrechtlichen Angelegenheiten**, über die durch Indiskretionen gegebenenfalls in der Presse berichtet wird. Entsprechende Verfahren werden innerhalb der Staatsanwaltschaft dann auch regelmäßig als sog. **Vollschutzverfahren** geführt, bei dem auch nur bestimmte Ermittlungsorgane Zugriff erhalten.

Der Kläger zu 2), **Rechtsanwalt Karl Jägen**, gehört der Rechtsanwaltskammer Düsseldorf an und arbeitet neben seiner Tätigkeit als **Rechtsanwalt** auch als **Syndikus-**

rechtsanwalt eines mittelständischen Telekommunikationsdienstleisters. In seiner Tätigkeit als Syndikus kommt er häufig mit **Betriebs- und Geschäftsgeheimnissen** in Berührung, die zwingend geheim zu halten sind, beispielsweise im Rahmen (auch internationaler) Verhandlungen. In Anbetracht der latenten Gefahr einer möglichen **Industriespionage** besteht die zwingende Notwendigkeit vertraulicher Kommunikation.

Der Kläger zu 3), **Rechtsanwalt Remo Klinger**, ist Mitglied der Rechtsanwaltskammer Berlin und Partner der Kanzlei Geulen & Klinger Rechtsanwälte. Die Kanzlei ist in **prominenten öffentlich-rechtlichen Mandaten**, insbesondere des Umwelt- und Planungsrechts, sowie in Verfahren des **internationalen Menschenrechtsschutzes** tätig. Sie vertritt sowohl öffentlich-rechtliche Auftraggeber, wie Bundesministerien und Landesministerien, als auch Nichtregierungsorganisationen, die Klagerechte als Umweltschutzverbände oder Verbraucherschutzverbände wahrnehmen. Eine erhebliche Zahl von Mandaten betrifft die rechtlichen Auseinandersetzungen zum sog. „**Dieselskandal**“ bei großen deutschen Kraftfahrzeugherstellern. Der durch den Kläger vertretene Umweltschutzverband wurde im Zuge dieser Auseinandersetzungen mehrfach zum Gegenstand von **Spähattacken**, die sich sowohl gegen die Internetseite des Verbandes als auch gegen Mobilfunkverbindungen von Mitarbeitern richteten.

Der Kläger zu 4), **Rechtsanwalt Christoph R. Müller**, ist Rechtsanwalt in Leipzig und Mitglied der Rechtsanwaltskammer Sachsen. Sein Tätigkeitsfeld umfasst hauptsächlich das **Wirtschaftsrecht**, insbesondere in Bezug auf das Handels- und Gesellschaftsrecht. Zudem bearbeitet er auch **wirtschaftsstrafrechtliche Mandate**. Er berät und vertritt sowohl außergerichtlich als auch gerichtlich einen **internationalen Mandantenstamm**. Einige seiner Mandanten wurden und werden **von Sicherheitsbehörden oder Geheimdiensten überwacht**. Für die vertrauliche Mandantenkommunikation nutzt er bereits Verfahren der **Ende-zu-Ende-Verschlüsselung**. Die verpflichtende Nutzung des nicht Ende zu Ende verschlüsselten beAs würde für ihn einen

erzwungenen Systembruch bedeuten, der seine vertrauliche Mandantenkommunikation konterkarieren und ein erhebliches **Risiko für die Rechte seiner Mandanten** begründen würde.

Der Kläger zu 5), **Rechtsanwalt Daniel Rink**, ist **Syndikusrechtsanwalt** der Profilhost AG, **Rechtsanwalt** und **Geschäftsführer der Rink Rechtsanwalts-gesellschaft mbH** sowie Mitglied des **Aufsichtsrates der DENIC eG** (Vergabestelle für .DE Domainnamen). Er berät nationale und internationale Unternehmen jeder Größenordnung in allen Fragen des Schutzes von Informationen (**Informationssicherheit**), sowie des **Schutzes personenbezogener Daten**, welche in Unternehmen verarbeitet werden. Einen Schwerpunkt bildet u. a. die **Beratung von Anwaltskanzleien und Gesundheitseinrichtungen**, welche **besonders sensitive Daten** verarbeiten. Seit vielen Jahren ist es für ihn daher **zwingend erforderlich**, mit seinen **Mandanten sicher zu kommunizieren**. Hierfür verwendet er die **Ende zu Ende Verschlüsselung S/MIME** für die sichere Kommunikation. Im Rahmen seiner Tätigkeit als Aufsichtsrat bei der DENIC eG setzt er sich für ein freies, offenes und **sicheres Internet** ein. Dabei treibt er die Entwicklung eines sicheren, offenen und dezentralen **Standards zur Authentifizierung von Nutzern** voran.

Der Kläger zu 6), **Rechtsanwalt Michael Schinagl**, ist Mitglied der Rechtsanwaltskammer Berlin. Schwerpunkte seiner anwaltlichen Tätigkeit sind der **Persönlichkeitsrechtsschutz** und der **Schutz des geistigen Eigentums**, insbesondere im Bereich **freier Software**. Zum Mandantenkreis gehören **investigative Medien** und **Whistleblower** sowie „Medien-Opfer“, darunter **exponierte Persönlichkeiten des öffentlichen Lebens** wie u. a. Bundestagsabgeordnete. Seine Mandanten haben ein gesteigertes Interesse an einem hohen Schutz der anwaltlichen Kommunikation in ihren Angelegenheiten. Dies betrifft freilich nicht nur, aber insbesondere jene, die sich gegen **Eingriffe in ihre Privat- und Intimsphäre** zur Wehr setzen müssen. Zudem verfügen seine **Mandanten aus dem IT-Bereich** ihrerseits über qualifizierte Kenntnisse

und Fähigkeiten im Umgang mit sicherer elektronischer Kommunikation. Sie stellen daher entsprechend **hohe Anforderungen** auch an die von ihnen nicht weiter beeinflussbare anwaltlich-gerichtliche sowie anwaltlich-anwaltliche Kommunikation in ihren Rechtssachen. So nutzt auch der Kläger selbst bereits seit über einer Dekade eine **qualifizierte digitale Signaturkarte** und kommuniziert mit Mandanten über das **freie Kryptographiesystem GPG**. Im Übrigen ist er Initiator der schon auf mehreren Kammerversammlungen erfolgreich beschlossenen sog. „**Transparenzanträge**“ zum beA, die auf die Veröffentlichung der Quelltexte, offene Schnittstellen und hohe Sicherheitsstandards abzielen.

Die Klägerin zu 7), **Rechtsanwältin Halina Wawzyniak**, ist Mitglied der Rechtsanwaltskammer Berlin. Sie ist zudem **ehemaliges Mitglied des Deutschen Bundestages**. In der 17. Wahlperiode war sie **netzpolitische Sprecherin ihrer Fraktion, Obfrau der Enquête-Kommission Internet und digitale Gesellschaft des Bundestages** sowie **stellvertretende Vorsitzende des Rechtsausschusses**. Während ihrer Abgeordnetenzeit stand sie als eine von mehreren Bundestagsabgeordneten ihrer Fraktion zeitweise unter einer im Nachhinein parteiübergreifend **hochumstrittenen Beobachtung durch das Bundesamt für Verfassungsschutz**. Vor diesem Hintergrund hat für sie eine vertrauliche Kommunikation, bei der ausgeschlossen ist, dass diese **staatlicherseits abgehört** werden kann, einen ganz besonderen Stellenwert. Nur eine Ende-zu-Ende-verschlüsselte Kommunikation – **ohne zwischengeschaltete Instanz** – kann eben dies gewährleisten.

2. DIE UNTERSTÜTZERINNEN UND UNTERSTÜTZER

Die Zielrichtung der hiesigen Klage wird **von einer Vielzahl weiterer Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälte unterstützt**, darunter auch **Mitgliedern des Bundestages** verschiedener parteipolitischer Couleur.

Bei dem von der **Gesellschaft für Freiheitsrechte (GFF)** initiierten **Crowdfunding** zur Finanzierung des Klageverfahrens wurde ein Betrag von über 30 000 Euro erzielt. Beteiligt haben sich **mehr als 200 Spenderinnen und Spender**, darunter nicht nur Rechtsanwältinnen und Rechtsanwälte. Denn die **Wahrung der anwaltlichen Verschwiegenheit zum Schutze des Mandatsgeheimnisses** ist eine **Säule des demokratischen Rechtsstaates** und betrifft damit **potentiell jede Bürgerin und jeden Bürger**.

Zudem wird die Initiative unterstützt von der **Stiftung Datenschutz**, die sich als unabhängige Einrichtung zuvörderst der **Förderung des Privatsphärenschutzes** widmet.

3. DAS BESONDERE ELEKTRONISCHE ANWALTSPOSTFACH (beA)

Das sog. besondere elektronische Anwaltspostfach (kurz: **beA**) wurde durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I 3786) eingeführt. Dem Titel des Gesetzes entsprechend sollte es **ursprünglich der elektronischen Kommunikation zwischen Anwaltschaft und Gerichtsbarkeit** dienen.

A) ZWECKÄNDERUNG: VON DER ELEKTRONISCHEN KOMMUNIKATION MIT DEN GERICHTEN ZUR ZUGANGSERÖFFNUNG FÜR JEDERMANN

In der Folge wurde dieser **Zweck allerdings erweitert**. Inzwischen soll das beA auch der Kommunikation **„der Rechtsanwaltskammern und der Bundesrechtsanwaltskammer mit den Gerichten“** sowie **„der Mitglieder der Rechtsanwaltskammern, der Rechtsanwaltskammern und der Bundesrechtsanwaltskammer untereinander“** dienen, § 19 Absatz 1 RAVPV (Rechtsanwaltsverzeichnis- und -postfachverordnung vom 23. September 2016 <BGBl. I S. 2167>, zuletzt geändert durch Artikel 19

des Gesetzes vom 12. Mai 2017 <BGBl. I S. 1121>). Darüber hinaus erlaubt § 19 Absatz 2 RAVPV, dass das beA „**auch der elektronischen Kommunikation mit anderen Personen oder Stellen dienen**“ kann. Und in der Tat wurde das beA von der Beklagten so konzipiert, dass es **für jedermann adressierbar** ist.

„Dem beA wurde die Rolle „**buerger_rueck**“ zugewiesen. Rechtsanwältinnen und Rechtsanwälte können demnach über ihre beA-Postfächer **insbesondere** mit Rechtsanwältinnen und Rechtsanwälten, Gerichten, Behörden, Notaren, dem Schutzschriftenregister, Rechtsanwaltskammern sowie **EGVP-Bürger-Postfächern** kommunizieren“.

BRAK, Teilnehmer am elektronischen Rechtsverkehr ERV (Anlage K 1).

B) AUSNAHMSLOSE ANWALTliche NUTZUNGSPFLICHT

Nachdem der **Anwaltsgerichtshof im Jahre 2016** feststellen musste, dass die **Beklagte zum damaligen Zeitpunkt nicht berechtigt war, das beA empfangsbereit einzurichten „und damit alle Rechtsanwälte faktisch zu zwingen, dieses zu nutzen“** (AGH Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15), wurde durch das Gesetz zur Umsetzung der Berufsanerkenntnisrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Berufe vom 12. Mai 2017 (BGBl. I S. 1121) mit Wirkung ab dem 01. Januar 2018 in **§ 31a Absatz 6 BRAO** (Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 des Gesetzes vom 30. Oktober 2017 <BGBl. I S. 3618>) eine **ausdrückliche, ausnahmslose anwaltliche Pflicht zur Nutzung des beAs** statuiert:

§ 31a Absatz 6 BRAO

Der Inhaber des besonderen elektronischen Anwaltspostfachs ist verpflichtet, die für dessen Nutzung erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das besondere elektronische Anwaltspostfach zur Kenntnis zu nehmen.

Seit dem **01. Januar 2018** sind damit alle zugelassenen Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälte verpflichtet, den **Gerichten gegenüber einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen** (sog. **passive Nutzungspflicht**), § 174 Absatz 3 Sätze 3 und 4 ZPO (Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 <BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781>, zuletzt geändert durch Artikel 11 Absatz 15 des Gesetzes vom 18. Juli 2017 <BGBl. I S. 2745>). In Verbindung mit § 130a Absatz 4 Nr. 2 ZPO und § 31a Absätze 1 und 6 BRAO verstärkt sich diese Pflicht dahingehend, **hierfür das beA zu nutzen**.

Ab dem **01. Januar 2022** sollen Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälte darüber hinaus verpflichtet sein, **nur noch auf elektronischem Wege mit den Gerichten zu kommunizieren** (sog. **aktive Nutzungspflicht**), Artikel 1 Nr. 4, 2 Nr. 4, 3 Nr. 5, 4 Nr. 4, 5 Nr. 4, 6 Nr. 4 i. V. m. Artikel 26 Absatz 7 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786, 3787).

c) TECHNISCHE UMSETZUNG

Die **Beklagte** ist verantwortlich für die **technische Umsetzung und den Betrieb des beAs**, § 31a Absatz 1 Satz 1 BRAO i. V. m. §§ 20 f. RAVPV (Rechtsanwaltsverzeichnis- und -postfachverordnung vom 23. September 2016 <BGBl. I S. 2167>, zuletzt geändert durch Artikel 19 des Gesetzes vom 12. Mai 2017 <BGBl. I S. 1121>).

Finanziert wird das beA von den **Mitgliedern der Rechtsanwaltskammern**. Laut eigener Angaben der Beklagten wurden für die bisherige „Realisierung des beA seit 2015 **Beiträge von insgesamt rund 32,5 Millionen Euro**“ geleistet.

BRAK, BRAK-Präsidentenkonferenz in Berlin, Presseerklärung Nr. 2 vom 18. Januar 2018 (**Anlage K 2**)

AA) OFFENKUNDIG GEWORDENE GRAVIERENDE SICHERHEITSMÄNGEL

Kurz vor Beginn der anwaltlichen Pflicht zur Nutzung des beAs, wurde am 22. Dezember 2017 offenkundig, dass die Beklagte die beA-Inhaberinnen und -Inhaber einem „**gravierenden Sicherheitsrisiko**“ ausgesetzt hatte:

„Ein Man-in-the-Middle-Angreifer hätte durch manipulierte DNS-Antworten Anfragen nach bealocalhost.de auf seinen eigenen Server umleiten und dort **eine falsche Version der BeA-Software präsentieren** können“.

Böck, Bundesrechtsanwaltskammer verteilt HTTPS-Hintertüre, Beitrag vom 23.12.2018, golem.de (**Anlage K 3**); Hervorhebungen sind hier und im Folgenden solche des Unterzeichners, sofern nicht anders gekennzeichnet.

Die Beklagte selbst beschreibt das Risiko, dem die Nutzerinnen und Nutzer durch die Sicherheitsmängel des beAs ausgesetzt wurden, wie folgt:

„Mit Hilfe dieses Zertifikats ist es Hackern möglich, eigene Webseiten als vertrauenswürdig zu präsentieren, obwohl diese nicht vertrauenswürdig sind. Der **Hacker könnte zudem einen weiteren IT-Sicherheitsangriff durchführen**. Dieses Vorgehen würde den Angreifer in die Lage versetzen, Anwenderinnen und Anwender **auf eigene Webseiten umzuleiten und im äußersten Fall den Rechner mit Schadsoftware zu infizieren**“.

BRAK, F. beA muss vorerst offline bleiben, 2. Worin genau besteht das Sicherheitsrisiko, das aus dem am 22. Dezember online gestellten Zertifikat resultieren soll? (**Anlage K 4**).

Nachdem die Beklagte auf den Sicherheitsmangel hingewiesen wurde, forderte sie die Postfachinhaberinnen und -inhaber zur Installation eines neuen Zertifikates auf.

Damit verschlimmerte die Beklagte die Situation indes nur: Ein Angreifer konnte nun "nach Belieben Man-in-the-Middle-Angriffe gegen die Internetverbindungen der betroffenen Rechtsanwälte durchführen - und dabei **Passwörter ausspionieren, Daten manipulieren und vieles mehr**".

Böck, Bundesrechtsanwaltskammer verteilt HTTPS-Hintertüre, Beitrag vom 23.12.2018, golem.de.

Danach wurden weitere, ebenfalls schwerwiegende Sicherheitsrisiken bekannt: So war das beA von einer sog. „Java-Deserialisierungslücke“ betroffen, die es erlaubte, dass „ein Angreifer (...) **nach Belieben Software auf dem Rechner des Anwalts starten und beispielsweise vorhandene Daten kopieren oder verändern**“ konnte.

Böck, Anwälte sollen BeA sofort deinstallieren, Beitrag vom 26.01.2018, golem.de (**Anlage K 5**).

Die Beklagte selbst stellt hierzu fest:

„Nach Auffassung des Chaos Computer Clubs ist die beA-Client Security von einer sogenannten Java-Deserialisierungslücke betroffen. Die beA-Software soll lokal auf dem Rechner einen HTTPS-Server öffnen, zu dem dann auch Webseiten über Websockets eine Verbindung aufbauen könnten. Der lokale HTTPS-Server soll empfangene Objekte mit der Java-Bibliothek Jackson verarbeiten, die von der genannten Sicherheitslücke betroffen ist. Durch eine trickreiche Konstruktion einer Anfrage soll es so möglich sein, die **beA-Software dazu zu bringen, Code auszuführen**. Damit könnte ein **Angreifer nach Belieben Software auf dem Rechner des Anwalts starten**.

Die BRAK empfiehlt darüber hinaus allen Rechtsanwältinnen und Rechtsanwälten, die **beA-Client Security auf ihren PCs zu deaktivieren**. Dies kann auf zwei Weisen geschehen: Entweder durch Deinstallation der Client Security oder durch Schließen der Client Security auf dem Rechner und das anschließende Entfernen der Client Security aus dem Autostart des Rechners“.

BRAK, F. beA muss vorerst offline bleiben, 3. Worin genau besteht das Sicherheitsrisiko, das mit der Nutzung veralteter Java-Bibliotheken zusammenhängen soll und auf das der Chaos Computer Club auf dem sogenannten beA-thon aufmerksam gemacht hat? (**Anlage K 6**).

Der Beklagten wurde diese Sicherheitslücke ebenfalls bereits am 22. Dezember 2018 mitgeteilt, jedoch wurde ihr die Tragweite offenbar erst am 29. Januar 2018 bei einem Termin mit externen Sachverständigen bewusst, die den anwesenden Vertretern der Beklagten den Sicherheitsmangel nochmals verdeutlichten, woraufhin die Beklagte

die Rechtsanwältinnen und Rechtsanwälte aufforderte, die **beA-„Client Security“** **vollständig zu deinstallieren**.

Böck, So geht es mit dem Anwaltspostfach weiter, Beitrag vom 29.01.2018, golem.de (**Anlage K 7**).

Aufgrund der **vielfachen, gravierenden Sicherheitsmängel** ist das **beA** seit dem **22. Dezember 2017 „offline“**.

egvp.de, Aktuelle Meldungen, Hinweis vom 22. Dezember 2017 (**Anlage K 8**).

Zudem musste auch das **Anwaltsverzeichnis vom Netz** genommen werden, da eine **Sicherheitslücke die Manipulation** der dort eingetragenen Daten sämtlicher Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälte erlaubte. Das Anwaltsverzeichnis ist die **Grundlage für die Einrichtung der beA-Postfächer**. Manipulationen konnten somit offenbar **auch am beA-System** vorgenommen werden.

Zum Ganzen Böck, Anwaltspostfach beA. Rechtsanwaltsregister musste abgeschaltet werden, Spiegel Online, Beitrag vom 13. April 2018 (**Anlage K 9**).

BB) IM BESONDEREN: GRUNDKONZEPTION OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Neben den vorstehend beschriebenen Sicherheitsmängeln ist das **wesentliche Sicherheitsrisiko bereits in der Grundkonzeption des beAs verankert**. Denn die Systemarchitektur des beAs gewährleistet **keine Ende-zu-Ende-Verschlüsselung**.

(1) WESENSELEMENT EINER ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Eine **Ende-zu-Ende-Verschlüsselung** liegt nur dann vor, wenn **ausschließlich die Kommunikationspartner die zwischen ihnen ausgetauschten Nachrichten ver- und entschlüsseln können**. Wesensmerkmal ist mithin, dass es **während des Kommunikationsvorganges keine weiteren zwischengeschalteten Akteure oder Instanzen** gibt, die **in die Verschlüsselung eingreifen** und mitlesen können.

Um dies zu gewährleisten ist **conditio sine qua non**, dass sich die sog. **privaten bzw. geheimen Schlüssel**, die zur Verschlüsselung der Nachrichten verwendet werden, **in der alleinigen Verfügungsgewalt der sie verwendenden Kommunikationspartner** befinden.

Ende-zu-Ende-Verschlüsselung

„Unter Ende-zu-Ende-Verschlüsselung (englisch ‚end-to-end encryption‘, ‚E2EE‘) versteht man die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg. **Nur die Kommunikationspartner (die jeweiligen Endpunkte der Kommunikation) können die Nachricht entschlüsseln.** (...) Theoretisch verhindert sie das Abhören der Nachricht durch alle anderen, inklusive der Telekommunikationsanbieter, Internet-Provider und sogar der Anbieter der genutzten Kommunikationsdienste. Bei Verwendung einer synchronen Verschlüsselung darf der Schlüssel zur Sicherstellung der Ende-zu-Ende-Verschlüsselung nur den End-Kommunikationspartnern bekannt sein. Bei Verwendung einer asymmetrischen Verschlüsselung muss sichergestellt sein, dass der geheime Schlüssel ausschließlich im Besitz des Empfängers ist“.

Wikipedia, Ende-zu-Ende-Verschlüsselung (Anlage K 10).

Asymmetrisches Kryptosystem

„Asymmetrisches Kryptosystem ist ein Oberbegriff für **Public-Key-Verschlüsselungsverfahren**, Public-Key-Authentifizierung und digitale Signaturen. Das „asymmetrische Kryptosystem“ oder „Public-Key-Kryptosystem“ ist ein kryptographisches Verfahren, bei dem im Gegensatz zu einem symmetrischen Kryptosystem die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel zu kennen brauchen. **Jeder Benutzer erzeugt sein eigenes**

Schlüsselpaar, das aus einem **geheimen Teil (privater Schlüssel)** und einem **nicht geheimen Teil (öffentlicher Schlüssel)** besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Besitzer des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Besitzer, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. (...) Die zu **übertragenden Daten werden auf Senderseite ver- und erst beim Empfänger wieder entschlüsselt**.

Wikipedia, Asymmetrisches Kryptosystem (Anlage K 11).

Pretty Good Privacy

„Pretty Good Privacy (PGP; engl. ‚ziemlich gute Privatsphäre‘) ist ein (...) Programm zur Verschlüsselung und zum Unterschreiben von Daten. (...) PGP benutzt ein sogenanntes **Public-Key-Verfahren**, in dem es ein eindeutig zugeordnetes Schlüsselpaar gibt: Genutzt werden ein **öffentlicher Schlüssel**, mit dem jeder Daten für den Empfänger verschlüsseln und dessen Signaturen prüfen kann, und ein **privater geheimer Schlüssel, den nur der Empfänger besitzt** und der normalerweise durch ein Passwort geschützt ist. Nachrichten an einen Empfänger werden mit dessen öffentlichem Schlüssel verschlüsselt und können dann ausschließlich mittels seines privaten Schlüssels entschlüsselt werden. Diese Verfahren werden auch **asymmetrische Verfahren** genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden“.

Wikipedia, Pretty Good Privacy (Anlage K 12).

Das Verfahren der Ende-zu-Ende-Verschlüsselung ist zudem wie folgt **patentiert**:

„Ende-zu-Ende-Verschlüsselung

Die Erfindung betrifft ein Verfahren zur Generierung und Verteilung von Geheimschlüsseln zur **Ende-zu-Ende-Verschlüsselung** von Informationen einer Kommunikationsverbindung zwischen zwei Teilnehmern eines digitalen Kommunikationssystems“.

„Unter der Bezeichnung **Ende-zu-Ende Verschlüsselung** (End-To-End-Encryption - ETEE) versteht man die Möglichkeit zum uni- oder bidirektionalen Austausch von Informationen (insbesondere Sprache aber auch Fax oder Daten) zwischen zwei Teilnehmern innerhalb eines digitalen Kommunikationssystems in verschlüsselter Form. **Charakteristisch ist hierbei die Verschlüsselung am Ort des Senders und die Entschlüsselung erst beim Empfänger einer Nachricht wobei der dazwischenliegende Kommunikationskanal**

keinen Einfluß auf die Chiffrierung besitzt. Innerhalb der digitalen Übertragungskette existiert keine Möglichkeit zur Umwandlung der Nachricht in den ursprünglichen Klartext“.

Europäisches Patentamt, Europäische Patentanmeldung EP 0 877 507 A2, Veröffentlichungstag 11. November 1998, Patentblatt 1998/64, S. 2 (Anlage K 13).

(2) VERSTOß DER BEA-SYSTEM-ARCHITEKTUR GEGEN DAS PRINZIP DER ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Das beA wurde von der Beklagten dergestalt eingerichtet, dass **sämtliche über das beA versandte Nachrichten durch ein sog. Hardware Security Modules (kurz: HSM) geschleust werden, in dem sowohl der öffentliche als auch der private Schlüssel (!) erstellt und gespeichert werden.**

Die Beklagte selbst beschreibt dies wie folgt:

„Die zentrale beA-Anwendung **speichert den privaten Schlüssel des Postfachs als verschlüsseltes Objekt in der Datenbank.** Dieser private Schlüssel des Postfaches und der zugehörige öffentliche Schlüssel werden beim Anlegen des Postfaches **in einem Hardware Security Modul (HSM) erstellt.** Auf Grund der Anforderung der Verwaltung von mehr als 360.000 Postfächern und den technischen Gegebenheiten zur internen Speicherung von Schlüsselmaterial in einem HSM, werden die im HSM erstellten privaten Schlüssel im HSM selbst mit einem weiteren Schlüssel verschlüsselt und in dieser Form **aus dem HSM exportiert.** Da kryptografische Operationen unter Verwendung des privaten Postfachschlüssels nur innerhalb des HSM möglich sind, müssen hierzu die **in der Datenbank abgelegten verschlüsselten privaten Schlüssel in das HSM geladen werden“.**

BRAK, D. Fragen zur technischen Funktionsweise und Entwicklung, Werden private Schlüssel von Atos oder einem Dienstleister auf anderen als den Kanzleirechnern der betroffenen Rechtsanwälte gespeichert? (Anlage K 14).

Demnach werden **sämtliche privaten Schlüssel der beA-Postfach-Inhaberinnen und -Inhaber im HSM erstellt** und liegen damit **notwendigerweise zunächst im HSM unverschlüsselt** vor. Sodann werden die privaten Schlüssel den Angaben der

Beklagten zufolge im HSM verschlüsselt, in eine „Datenbank“ exportiert und so dann in das HSM reimportiert.

Des Weiteren kann beim Nachrichtenversand innerhalb des HSMs (!) eine Umschlüsselung stattfinden. Die Beklagte stellt dies selbst wie folgt dar:

„Im Unterschied zum EGVP ermöglicht das beA jedoch einen Zugriff auf das Postfach für mehrere Nutzer mit unterschiedlichen Berechtigungen, um die Aufgabenverteilung innerhalb einer Kanzlei abzubilden. Hierfür kommt ein **Hardware Security Module (HSM)** zum Einsatz. Dabei handelt es sich um spezielle Hardwarekomponenten, die unter Einsatz kryptographischer Schlüssel bestimmte vordefinierte Funktionen ausführen. Sie sind dabei gegen jede Art von Manipulation geschützt.

Wenn eine Nachricht von einem berechtigten Nutzer gelesen werden soll, muss dieser sich zunächst mit dem öffentlichen Schlüssel seines Sicherheits-Tokens – z.B. seiner beA-Karte – authentifizieren. **Das HSM schlüsselt nach Prüfung der Berechtigung des anfragenden öffentlichen Schlüssels – im geschützten Bereich des HSM – den Nachrichtenschlüssel für den jeweiligen berechtigten Leser um.**

Vor dem Umschlüsseln prüft das HSM, ob eine vom Postfachbesitzer kryptographisch signierte Berechtigung (MAC) vorliegt. Allein der Postfachinhaber oder eine von ihm mit dem Recht „Berechtigungen verwalten“ versehene Person kann dem HSM das Umschlüsseln für einen konkreten Leser gestatten. **Nur das HSM ist in der Lage, Nachrichten umzuschlüsseln, da die Postfachschlüssel im HSM verschlüsselt abgelegt sind und auch nur dort entschlüsselt werden können“.**

BRAK, Technische Informationen zum Verschlüsselungsverfahren beim beA (Anlage K 15).

Die von der Beklagten gewählte technische Umsetzung des beAs verstößt demnach gegen das Grundprinzip und Wesensmerkmal der Ende-zu-Ende-Verschlüsselung in gleich mehrfacher Weise.

Siehe auch:

Böck, So geht es mit dem Anwaltspostfach weiter, Beitrag vom 29.01.2018, golem.de,

ders., Die unnötige Ende-zu-Mitte-Verschlüsselung von BeA, golem.de (Anlage K 16),

Drenger, Vortrag beim Deutschen Anwaltverein am 22. Januar 2018, ab 1:00:50,
<https://www.youtube.com/watch?v=IZkPvqBgQ4w>

sowie ausf.:

Löschhorn, Pflicht zur Nutzung des besonderen elektronischen Anwaltspostfachs (beA) und zur anwaltlichen Verschwiegenheit, MMR 2018, 204 (Anlage K 17).

(A) ERSTELLUNG UND SPEICHERUNG DER PRIVATEN SCHLÜSSEL IM HSM SOWIE SPEICHERUNG DER PRIVATEN SCHLÜSSEL IN EINER DATENBANK

Die privaten Schlüssel sämtlicher zur Nutzung des beAs verpflichteter Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälten werden **vom HSM generiert**, liegen in diesem damit **notwendigerweise auch zunächst unverschlüsselt** vor und werden sodann **verschlüsselt in einer Datenbank** sowie **im HSM gespeichert**.

Dabei ist **unklar, in welcher Art und Weise die Verschlüsselung der privaten Schlüssel erfolgt**, wo die hierfür benötigten **Schlüssel hinterlegt** sind und wer hierauf **Zugriff** hat.

Weiter ist **nicht nachvollziehbar**, warum sämtliche privaten Schlüssel aus dem HSM **extrahiert und in einer Datenbank gespeichert** werden, um sodann wieder in das **HSM reimportiert** zu werden. Es ist auch **nicht bekannt**, um **welche Art von Datenbank** es sich handelt, **wo sich diese befindet** und wer auf diese **Zugriff** hat.

Des ungeachtet **widerspricht** dieses Verfahren evident den **essentiellen Mindestanforderungen einer Ende-zu-Ende-Verschlüsselung**. Denn es ist, wie dargelegt,

„**conditio sine qua non**“ der Ende-zu-Ende-Verschlüsselung, dass **ausschließlich die miteinander kommunizierenden Personen die Verfügungsgewalt über ihre privaten Schlüssel** haben und sich diese **allein im Besitz der Kommunikationspartner** befinden.

Die **Erstellung und Speicherung der privaten Schlüssel im HSM sowie einer externen Datenbank** ist damit schlechterdings **unvereinbar**.

Darüber hinaus birgt die **zentrale Speicherung sämtlicher privater Schlüssel** aller Rechtsanwältinnen und Rechtsanwälte sowie Syndikusrechtsanwältinnen und Syndikusrechtsanwälte, die zur Nutzung des beAs verpflichtet sind, ein **besonders hohes Angriffsrisiko**. Denn das **HSM stellt als zentraler Knotenpunkt für die Kommunikation der gesamten Anwaltschaft** ein **äußerst attraktives Angriffsziel** dar.

(B) UMSCHLÜSSELUNG IM HSM

Des Weiteren verstößt die in der Systemarchitektur des beAs vorgesehene Möglichkeit der **Umschlüsselung von Nachrichten im HSM** gegen das Kernelement der Ende-zu-Ende-Verschlüsselung, einen **unmittelbaren geheimen Nachrichtenaustausch zwischen Kommunikationspartnern** zu gewährleisten.

Anstatt allein aufeinander vertrauen zu können, werden **Absender und Empfänger gezwungen, darauf zu vertrauen, dass die Nachricht im HSM nicht ohne ihren Willen umgeschlüsselt wird**.

Die Möglichkeit der Umschlüsselung zur Weiterleitung einer Nachricht an einen anderen Empfänger bietet einen **besonders risikobehafteten Angriffspunkt, um Nachrichten unbemerkt abfangen** zu können. Eben dies soll eine Ende-zu-Ende-Verschlüsselung gerade vermeiden.

Eine Ende-zu-Ende-Verschlüsselung soll gewährleisten, dass die **Kommunikationspartner nur gegenseitig aufeinander vertrauen** müssen und **nicht auf eine zwischengeschaltete Instanz**. Eine solche aber hat die Beklagte durch das **HSM** geschaffen.

Aufgrund der Zwischenschaltung des HSMs liegt mithin **keine Ende-zu-Ende-Verschlüsselung** vor, deren unabdingbare Voraussetzung ein **unmittelbarer vertraulicher Nachrichtenaustausch** zwischen den Kommunikationspartnern ist.

4. WEIGERUNG DER BEKLAGTEN ZUR EINRICHTUNG DES BEAS MIT ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Der Beklagten ist die dargestellte **Diskrepanz** zwischen der von ihr gewählten technischen Gestaltung des beAs und den Erfordernissen einer Ende-zu-Ende-Verschlüsselung **bekannt**, und dies auch bereits **seit längerer Zeit**.

So berichtet die Beklagte selbst, dass sie jedenfalls (spätestens) bei dem von ihr veranstalteten sog. „**beAthon**“ auf die Problematik der nicht gegebenen Ende-zu-Ende-Verschlüsselung hingewiesen wurde:

„Das **beA-HSM** ist eine spezielle Hardware-Komponente des beA-Systems. Hier findet die kryptografische Umschlüsselung des Schlüsselmaterials statt, mit dem die im beA versendeten Nachrichten verschlüsselt sind. Diese Umschlüsselung gewährleistet, dass es verschiedene Zugangsberechtigungen für den Nachrichtenabruf gibt, so wie es der Gesetzgeber vorgeschrieben hat. **Dazu erörterten die Teilnehmer auch die Frage, inwieweit das derzeitige System aufgrund der Umschlüsselung terminologisch als ein Ende-zu-Ende verschlüsseltes System bezeichnet werden könne**“.

Schreiben der BRAK an die Präsidentinnen und Präsidenten der Rechtsanwaltskammern vom 30. Januar 2018 (**Anlage K 18**).

Der für das **beA** zuständige **Vize-Präsident der Beklagten**, Rechtsanwalt Dr. Martin Abend, wird zudem mit der Aussage auf der Mitgliederversammlung der Rechtsanwaltskammer Sachsen zitiert:

„Im HSM werde dem Nachrichtenschlüssel eine neue Codierung beigelegt. Das sei **keine eigentliche Ende-zu-Ende-Verschlüsselung**‘, aber ein hoher Industriestandard“.

Papenmeier, beA-Skandal bei der RAK Sachsen, Beitrag vom 23. März 2018, blog.erbrecht-papenmeier.de (**Anlage K 19**).

Dabei ist darauf hinzuweisen, dass es sich **freilich nicht nur um eine „terminologische“ Frage** handelt, ob die beA-Konstruktion unter Einsatz des HSMs eine Ende-zu-Ende-Verschlüsselung gewährleistet. Abgesehen davon, dass es sich bei der Ende-zu-Ende-Verschlüsselung wie dargelegt um ein **eindeutig definiertes Verfahren** handelt, geht es nicht etwa lediglich um eine richtige „Etikettierung“ des beAs, wie es die Beklagte in ihrem vorstehend zitierten Schreiben an die Kammern vom 30. Januar 2018 darzustellen sucht. Vielmehr handelt es sich hierbei um eine **Rechtsfrage**: Denn die **Gewährleistung einer Ende-zu-Ende-Verschlüsselung ist eine rechtlich notwendige Mindestanforderung an das beA**, wie sogleich gezeigt wird.

Die Beklagte hat bis zur Klageerhebung **nicht zu erkennen gegeben**, dass sie die Grundarchitektur des beAs unter Verwendung des einer Ende-zu-Ende-Verschlüsselung entgegenstehenden HSMs **zu ändern beabsichtigt**.

Vielmehr erklärt die Beklagte:

„Aus den vorläufigen Einschätzungen des bisherigen Befundes geht aber auch hervor, dass **keine der bislang identifizierten Schwachstellen eine grundsätzliche Überarbeitung der beA-Systemarchitektur erfordert**“.

Schreiben der BRAK an die Präsidentinnen und Präsidenten der Rechtsanwaltskammern vom 28. März 2017, zitiert nach beA-ABC-Blog, Erste Ergebnisse der Sicherheitsanalyse: Anwaltspostfach beA bleibt vorerst weiterhin offline, Beitrag vom 28. März 2018 (**Anlage K 20**).

II. RECHTLICHE WÜRDIGUNG

1. ZULÄSSIGKEIT

Die Klage ist **zulässig**.

A) ERÖFFNUNG DES RECHTSWEGES ZUM ANWALTSGERICHTSHOF BERLIN

In vorliegender Sache ist der **Rechtsweg zum Anwaltsgerichtshof Berlin eröffnet**. Gemäß § 112a Absatz 1 BRAO entscheidet der Anwaltsgerichtshof im ersten Rechtzug über **alle öffentlich-rechtlichen Streitigkeiten nach der Bundesrechtsanwaltsordnung, nach einer auf Grund der Bundesrechtsanwaltsordnung erlassenen Rechtsverordnung** oder nach einer Satzung einer Rechtsanwaltskammer oder der Bundesrechtsanwaltskammer, soweit nicht die Streitigkeiten anwaltsgerichtlicher Art oder einem anderen Gericht ausdrücklich zugewiesen sind.

Die Pflicht der Beklagten zur Einrichtung des beAs folgt aus **§ 31a Absatz 1 BRAO**, die Pflicht der Klägerin und der Kläger, das beA zu nutzen, aus **§ 31a Absatz 6 BRAO**; die konkrete Ausgestaltung des beAs richtet sich nach **§ 31c Nr. 3 Buchstabe b BRAO i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV**.

Nach der **Rechtsprechung des Anwaltsgerichtshofes Berlin** ist die Regelung des beAs in der Bundesrechtsanwaltsordnung dem öffentlichen Recht zuzuordnen, weshalb es sich um eine **öffentlich-rechtliche Streitigkeit** handle (Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15, juris-Rn. 14).

Dies folgt im Übrigen auch aus dem Umstand, dass die Klägerin und die Kläger in einem **Subordinationsverhältnis** zur Beklagten als Körperschaft des öffentlichen

Rechts (§ 176 Absatz 1 BRAO) stehen (grdl. BGH, Urteil vom 10. Juli 1954 – VI ZR 120/53, juris-Rn. 17).

Eine **Sonderzuweisung** an ein anderes Gericht ist **nicht ersichtlich**.

B) SACHLICHE ZUSTÄNDIGKEIT

Zur **sachlichen Zuständigkeit** hat der Anwaltsgerichtshof Berlin in Bezug auf die Einrichtung des beAs bereits klargestellt:

„(...) (A)ngesichts der umfassenden Formulierung des § 112a Abs. 1 BRAO wird **hoheitliches Verwaltungshandeln** auch dann erfasst, wenn es **keinen Verwaltungsakt** darstellt, aber **geeignet ist, in die berufsrechtlich begründeten Rechte der Beteiligten einzugreifen oder sie einzuschränken** (vgl. Deckenbrock, in: Henssler/Prütting, BRAO, 4. Aufl., § 112a Rn. g)“.

Ebd., juris-Rn. 14.

So liegt es auch hier. Bei der **Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung** handelt es sich um einen **Realakt**, der **in die anwaltliche Berufsausübungsfreiheit der Klägerin und der Kläger eingreift**.

Die sachliche Zuständigkeit des Anwaltsgerichtshofes Berlin als **Eingangsstanz** folgt im Übrigen aus § 112a Absatz 1 BRAO („entscheidet im **ersten Rechtszug**“).

C) ÖRTLICHE ZUSTÄNDIGKEIT

Die **örtliche Zuständigkeit** folgt vorliegend aus § 112b Satz 1 Halbsatz 2 BRAO. Danach ist der Anwaltsgerichtshof zuständig, der für den **Oberlandesgerichtsbezirk** errichtet ist, in dem eine **hoheitliche Maßnahme, die berufsrechtliche Rechte und Pflichten der Beteiligten beeinträchtigt oder verwirklicht**, erlassen wurde oder zu erlassen wäre. Nach § 112b Satz 2 BRAO ist „in allen anderen Angelegenheiten (...)“

der Anwaltsgerichtshof zuständig, der für den Oberlandesgerichtsbezirk errichtet ist, in dem der **Beklagte seinen Sitz**, seine Kanzlei oder ansonsten seinen Wohnsitz hat“.

Die **Beklagte**, von der vorliegend die beeinträchtigende Maßnahme in Gestalt der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung ausgeht, hat ihren **Sitz in Berlin**, sodass der Anwaltsgerichtshof Berlin örtlich zuständig ist (siehe bereits Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15, juris-Rn. 15).

D) STREITGENOSSENSCHAFT

Im Verfahren vor dem Anwaltsgerichtshof gelten die zivilprozessrechtlichen Vorschriften zur **Streitgenossenschaft** entsprechend nach § 112c BRAO i. V. m. § 64 VwGO (Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 <BGBl. I S. 686>, zuletzt geändert durch Artikel 5 Absatz 2 des Gesetzes vom 8. Oktober 2017 <BGBl. I S. 3546>) i. V. m. §§ 59 ff ZPO (Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 <BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781>, zuletzt geändert durch Artikel 11 Absatz 15 des Gesetzes vom 18. Juli 2017 <BGBl. I S. 2745>).

Die Klägerin und die Kläger klagen in hiesiger Sache als **Streitgenossen**. Denn sie sind aufgrund ihrer Zulassung zur Rechtsanwaltschaft **in gleicher Weise gemäß § 31a Absatz 6 BRAO verpflichtet, das von der Beklagten eingerichtete beA zu nutzen**. Insofern beruht das **gemeinsame rechtliche Begehren** gegenüber der Beklagten, die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung zu unterlassen und dieses mit Ende-zu-Ende-Verschlüsselung zur Verfügung zu stellen, **auf denselben tatsächlichen und rechtlichen Gründen**, vgl. §§ 59 f. ZPO.

E) STATTHAFTE KLAGART

Die Klägerin und die Kläger verfolgen ihr Begehrt mit einer **allgemeinen Leistungsklage**.

Diese ist in der Verwaltungsgerichtsordnung, auf die § 112c BRAO verweist, zwar nicht ausdrücklich geregelt, jedoch in den §§ 43 Absatz 2, 11 und 113 Absatz 4 VwGO erwähnt und jedenfalls **in gefestigter höchstrichterlicher Rechtsprechung anerkannt**.

Grdl. BVerwGE 31, 301.

Sie ist nach der Rechtsprechung des Bundesverwaltungsgerichts **statthaft**, wenn die **Verurteilung zu einer anderen Leistung als dem Erlass eines Verwaltungsaktes begehrt** wird (ebd., juris-Rn. 35).

So liegt es hier: Die Klägerin und die Kläger begehren das **Unterlassen der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung und die Bereitstellung des beAs mit Ende-zu-Ende-Verschlüsselung**. Das Begehrt ist demnach **nicht auf den Erlass eines Verwaltungsaktes gerichtet**, sondern vielmehr auf ein **tatsächliches Handeln der Beklagten**, mithin einen **Realakt**.

F) KLAGEBEFUGNIS

Die Rechtsprechung fordert auch für die allgemeine Leistungsklage die Darlegung der **Klagebefugnis** analog § 42 Absatz 2 VwGO.

Grdl. BVerwGE 36, 192.

Die Klägerin und die Kläger machen geltend, durch die von der Beklagten vorgenommene Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung in ihren Rechten, insbesondere in ihrer **Berufsausübungsfreiheit aus Artikel 12 Absatz 1 GG** (Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 13. Juli 2017 <BGBl. I S. 2347>), jedenfalls aber in ihrem **grundrechtlichen Anspruch auf Rechtmäßigkeit staatlichen Handelns (Artikel 2 Absatz 1 GG)** verletzt zu sein.

Das Bundesverwaltungsgericht formuliert die **Anforderungen an die Klagebefugnis** wie folgt:

„Eine Klage ist **nur dann nach § 42 VwGO Abs. 2 unzulässig**, wenn **offensichtlich und eindeutig nach keiner Betrachtungsweise** die vom Kläger behaupteten **Rechte bestehen oder ihm zustehen können**“.

BVerwG, Urteil vom 30. Oktober 1963 – V C 219.62, Leitsatz.

Der **Anwaltsgerichtshof Berlin** hat bereits konstatiert, dass Rechtsanwältinnen und Rechtsanwälten ein **subjektives Recht in Gestalt des öffentlich-rechtlichen Unterlassungsanspruchs gegen die rechtswidrige Einrichtung des beAs** zusteht:

„Dem Antragsteller steht gegenüber der Antragsgegnerin (Anm.: der hiesigen Beklagten) ein **öffentlich-rechtlicher Unterlassungsanspruch** zu, dessen Herleitung zwar umstritten, aber gewohnheitsrechtlich anerkannt ist (BVerwG, Urteil vom 7. Oktober 1983 – 7 C 44/81, NJW 1984, 989). Denn das **Handeln der Antragsgegnerin im Zusammenhang mit der Einrichtung eines beA** für die Antragsteller stellt einen **Eingriff in die Berufsausübungsfreiheit** des Antragstellers dar, der **mangels gesetzlicher Regelung nicht gerechtfertigt** ist“.

Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15, juris-Rn. 18.

Die Klägerin und die Kläger machen geltend, dass die von der Beklagten vorgenommene **Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung** einen **ungerechtfertigten Eingriff in ihre Berufsausübungsfreiheit** darstellt, da sie **gegen die bestehenden gesetzlichen Vorgaben zur technischen Ausgestaltung des beAs verstößt**.

In Bezug auf den **grundrechtlichen Anspruch auf Rechtsmäßigkeit staatlichen Handelns**, den das Bundesverfassungsgericht grundlegend in seinem Elfes-Urteil (BVerfGE 6, 32) aus Artikel 2 Absatz 1 GG ableitete, hat das **Bundesverwaltungsgericht** ausgeführt:

„Weil der **Adressat eines belastenden Verwaltungsakts stets einem staatlichen Freiheitseingriff unterliegt**, folgt nach der sog. **Adressatentheorie allein hieraus ein Klagerecht nach § 42 Abs. 2 VwGO**. Konsequenterweise und korrespondierend hiermit muss eine **als Eingriff in die Freiheit ihres Adressaten zu bewertende behördliche Verfügung** regelmäßig nach § 113 Abs. 1 Satz 1 VwGO **aufgehoben werden**, wenn die Sach- und Rechtsprüfung ergibt, dass der **grundrechtliche Anspruch auf Gesetzmäßigkeit** durch die Eingriffsverwaltung verletzt wurde, denn der **Eingriff ist dann nicht durch die Ermächtigungsgrundlage gedeckt**“.

BVerwG, Beschluss vom 19. Juli 2010 – 6 B 20/10, juris-Rn. 16.

Dies gilt entsprechend für die **Klagebefugnis bei der allgemeinen Leistungsklage analog § 42 Absatz 2 VwGO** für **Adressaten** einer Maßnahme der Verwaltung, die – wie vorliegend – kein Verwaltungsakt, sondern ein **Realakt** ist.

BVerwG, Urteil vom 23. Mai 1989 – 7 C 2/87, juris-Rn. 48.

Die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung stellt ein **schlicht hoheitliches Handeln der Beklagten** durch **Realakt** dar, das die Klägerin und die Kläger **unmittelbar betrifft**, weil sie gemäß § 31a Absatz 6 BRAO **zur Nutzung des beAs verpflichtet** sind.

Im Übrigen wird auf die **Ausführungen zur Begründetheit der Klage** verwiesen, mit denen die Verletzung der subjektiven Rechte der Klägerin und der Kläger durch die rechtswidrige Einrichtung des beAs im Einzelnen dargestellt und weiter substantiiert wird (siehe unten bei II.2, S. 35).

G) RECHTSSCHUTZBEDÜRFNIS

Die Klägerin und die Kläger haben ein **besonderes Rechtsschutzinteresse**, dass die Beklagte das beA nur mit einer Ende-zu-Ende-Verschlüsselung in Betrieb nimmt.

AA) BEGRÜNDETE BESORGNIS DER BALDIGEN INBETRIEBNAHME DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Die Geltendmachung eines (vorbeugenden) Unterlassungsanspruches im Wege der allgemeinen Leistungsklage – hier: gegen die Wiederinbetriebnahme des beAs ohne Ende-zu-Ende-Verschlüsselung – setzt voraus, dass das **streitgegenständliche Handeln der Beklagten**, gegen das sich das Begehrt richtet, „**alsbald zu besorgen**“ steht.

Vgl. BVerwG, Urteil vom 18. April 1985 – 3 C 34/84, juris-Rn. 34; BVerfG, Stattgebender Kammerbeschluss vom 23. Februar 2007 – 1 BvR 2368/06, juris-Rn. 28-35.

Vorliegend steht es **zu besorgen**, dass die Beklagte das beA in **unveränderter Form ohne Ende-zu-Ende-Verschlüsselung alsbald reaktivieren** wird. So erklärt die Beklagte u. a. selbst:

„Secunet bestätigt, dass sie nach aktuellem Untersuchungsstand **keine Fehler gefunden haben, die den grundlegenden Aufbau des beA-Systems in Frage stellen**“.

BRAK, Secunet berichtet über laufende Prüfung des beA, Presseerklärung Nr. 7 vom 15.04.2018 (**Anlage K 21**).

Und auch in ihrer übrigen öffentlichen Kommunikation hat die **Beklagte in keiner Weise in Aussicht gestellt, an der Konzeption des beAs ohne Ende-zu-Ende-Verschlüsselung nicht weiter festhalten zu wollen**. Das Rechtsschutzinteresse ist somit **nicht durch eine entsprechende Zusicherung der Beklagten entfallen**.

Vgl. hierzu Obergerverwaltungsgericht Rheinland-Pfalz, Beschluss vom 21. Januar 2004 – 6 A 11743/03, Leitsatz.

Vielmehr weist die **Gesamtheit der Äußerungen der Beklagten** zum beA und der hierdurch geschaffene gegenwärtige Zustand unzweifelhaft darauf hin, dass die Beklagte eine **Neukonzeption des beAs mit Ende-zu-Ende-Verschlüsselung nicht beabsichtigt**.

Vgl. hierzu BVerwG, Urteil vom 23. Mai 1989 – 7 C 2/87, juris-Rn. 81.

Insoweit wird auf die Ausführungen zur **nachweislichen Kenntnis der Beklagten von der nicht gegebenen Ende-zu-Ende-Verschlüsselung** sowie der **Weigerung**, das beA mit einer solchen auszustatten, verwiesen (siehe oben bei I.4., S. 23).

BB) DROHENDE VERLETZUNG DES MANDATSGEHEIMNISSES

Ein bereits einmaliges **Ausspionieren anwaltlicher Daten** kann **nicht rückgängig gemacht werden** und führt zu einer **irreversiblen Verletzung des Mandatsgeheimnisses**.

Dies hat das **Bundesverfassungsgericht** bereits in Bezug auf den **Grundrechtsschutz geschäftlicher E-Mail-Daten** festgestellt, sodass dies entsprechend erst recht für über das beA elektronisch ausgetauschte Anwaltsdaten gelten muss:

„Erginge die einstweilige Anordnung nicht, hätte die Verfassungsbeschwerde hinsichtlich der Beschlagnahme des Datenbestandes jedoch später Erfolg, so könnten dem Beschwerdeführer – möglicherweise irreparable – Beeinträchtigungen der rechtlich geschützten Geheimheit der Umstände und des Inhalts seiner E-Mail-Kommunikation erwachsen. Das grundrechtlich geschützte Vertrauen in die Abschottung der Telekommunikation vor fremdem, insbesondere vor staatlichem Zugriff bewahrt nicht erst vor der Verwertung unberechtigt erlangter Kenntnisse, sondern schon allein vor der fremden Kenntnisnahme“.

BVerfG, Einstweilige Anordnung vom 29. Juni 2006 – 2 BvR 902/06, juris-Rn. 20.

CC) DROHENDER VERLUST DES MANDANTENSTAMMS

Würden sich die Klägerin und die Kläger zur Vermeidung berufsrechtlicher Sanktionen der bestehenden gesetzlichen Pflicht zur Nutzung des beAs beugen und dieses nutzen, obgleich es keine Ende-zu-Ende-Verschlüsselung gewährleistet, so liefen sie **Gefahr, ihres Mandantenstamms verlustig zu werden**. Die Klägerin und die Kläger vertreten eine **Vielzahl von Mandanten, die ein besonders gesteigertes Interesse an der Wahrung des Mandatsgeheimnisses haben**.

DD) VERMEIDUNG VON SANKTIONEN BEI WEIGERUNG DER NUTZUNG DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Weiter drohen der Klägerin und den Klägern bei Verweigerung der Nutzung des beAs ohne Ende-zu-Ende-Verschlüsselung **berufsrechtliche Sanktionen** bis hin zum **Verlust der beruflichen Existenz** durch Ausschließung von der Rechtsanwaltschaft, §§ 31a Absatz 6, 113 Absatz 1, 114 Absatz 1 Nr. 5 BRAO.

Es ist in der höchstrichterlichen Rechtsprechung als besonderes Rechtsschutzbedürfnis anerkannt, dass sich niemand zunächst – sehenden Auges – **vorhersehbaren staatlichen Sanktionen aussetzen muss** und darauf verwiesen ist, deren etwaige

Rechtswidrigkeit erst „mit dem Rücken zur Wand“ einer gerichtlichen Klärung zu führen zu können.

Vgl. nur BVerwG, Urteil vom 30. Mai 1985 – 3 C 53/84, juris-Rn. 16.

Das **Bundesverfassungsgericht** hat bereits in Bezug auf den vergleichbaren Verlust des Patientenstamms eines Arztes anerkannt, dass dies zu „**irreparable(n) berufliche(n) und wirtschaftliche(n) Nachteile(n)**“ führe und diese „**schwerwiegenden Konsequenzen (...) praktisch kaum noch rückgängig zu machen**“ seien.

BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 15. März 2010 - 1 BvR 722/10, juris-Rn. 10; BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 23. November 2009 - 1 BvR 2709/09, Rn. 10.

2. BEGRÜNDETHEIT

Die Klage ist auch **begründet**.

Die Einrichtung eines empfangsbereiten beAs ohne Ende-zu-Ende-Verschlüsselung ist **rechtswidrig und verletzt die Klägerin und die Kläger in ihren Rechten**, § 112c BRAO i. V. m. § 113 Absatz 5 i. V. m. Absatz 1 VwGO analog.

A) RECHTSWIDRIGKEIT DER EINRICHTUNG DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Die von der Beklagten gewählte technische Ausgestaltung des beAs ohne Ende-zu-Ende-Verschlüsselung und **verstößt gegen § 174 Absatz 3 Sätze 3 und 4 ZPO sowie § 31c Nr. 3 Buchstabe b BRAO i. V. m. §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV**.

AA) VERSTOß GEGEN § 31A ABSATZ 1 BRAO I. V. M. § 174 ABSATZ 3 SÄTZE 3 UND 4 I. V. M. § 130A ABSATZ 4 NR. 2 ZPO

Das beA verstößt in seiner derzeitigen von der Beklagten verantworteten **HSM-Architektur ohne Ende-zu-Ende-Verschlüsselung** gegen die Vorgaben des Bundesgesetzgebers zur Einrichtung des beAs als sicherer Übermittlungsweg zur elektronischen Kommunikation mit den Gerichten.

Wie bereits beschrieben, hat der Bundesgesetzgeber durch das **Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten** vom 10. Oktober 2013 (BGBl. I S. 3786) **zum 01. Januar 2018** für Rechtsanwältinnen und Rechtsanwälte sowie für Syndikusrechtsanwältinnen und Syndikusrechtsanwälte die Pflicht eingeführt, gegenüber den Gerichten einen sicheren Übermittlungsweg zu eröffnen und vorgesehen, dass das beA einen solchen darstellen soll:

§ 174 Absätze 1 und 3 ZPO

(1) Ein Schriftstück kann an einen **Anwalt**, einen Notar, einen Gerichtsvollzieher, einen Steuerberater oder an eine sonstige Person, bei der auf Grund ihres Berufes von einer erhöhten Zuverlässigkeit ausgegangen werden kann, eine Behörde, eine Körperschaft oder eine Anstalt des öffentlichen Rechts gegen Empfangsbekenntnis zugestellt werden.

(...)

(3) An die **in Absatz 1 Genannten** kann auch ein **elektronisches Dokument** zugestellt werden. Gleiches gilt für andere Verfahrensbeteiligte, wenn sie der Übermittlung elektronischer Dokumente ausdrücklich zugestimmt haben. Das Dokument ist auf einem **sicheren Übermittlungsweg** im Sinne des § 130a Absatz 4 zu übermitteln und **gegen unbefugte Kenntnisnahme Dritter zu schützen**. Die in Absatz 1 Genannten haben einen **sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen**.

§ 130a Absatz 4 Nr. 2 ZPO

Sichere Übermittlungswege sind

(...)

2. der Übermittlungsweg zwischen dem **besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung** oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts,

(...).

Entscheidend ist hierbei, dass der Bundesgesetzgeber in § 174 Absatz 3 Satz 3 ZPO konkretisiert hat, dass der „**sichere Übermittlungsweg**“ zu gewährleisten hat, dass die übermittelten Nachrichten „**gegen unbefugte Kenntnisnahme Dritter zu schützen**“ sind.

Diese gesetzliche Vorgabe kann **nur durch eine Ende-zu-Ende-Verschlüsselung umgesetzt** werden, bei der **allein die miteinander Kommunizierenden** in der Lage sind, die zwischen ihnen ausgetauschten Nachrichten zu ver- und entschlüsseln, **ohne dass Dritte am Verschlüsselungsprozess beteiligt** sind, was insbesondere zwingend erfordert, dass **nur die Kommunikationspartner über ihre eigenen privaten Schlüssel verfügen**.

So führte auch der **Bundesrat** im Verlaufe des Gesetzgebungsverfahrens in seiner Stellungnahme zum Entwurf des § 174 Absatz 3 ZPO aus:

„Die vorgeschlagene Streichung der Bezugnahme auf ‚sichere Übermittlungswege‘ im Sinne des § 130a Absatz 4 ZPO-E führt auch nicht etwa zur Zulassung ‚unsicherer‘ Übertragungswege, da die **Anforderung, die Übermittlung „gegen unbefugte Kenntnisnahme Dritter zu schützen“**, bestehen bliebe und diese beim Einsatz der EGVP-Infrastruktur durch die automatisierte **(Ende-zu-Ende-)Verschlüsselung** der Daten über das sogenannte OSCI-Transportprotokoll gewährleistet wird“.

Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 06. März 2013, BT-Drs. 17/12634, S. 46 f.

Indem die Beklagte das beA technisch dergestalt realisiert hat, dass es **keine Ende-zu-Ende-Verschlüsselung** gewährleistet, weil es insbesondere die **privaten (!) Schlüssel der beA-Postfach-Inhaber zentral in einem HSM speichert**, hat sie ge-

gen die gesetzliche Auflage verstoßen, in Gestalt des beAs einen **sicheren Übermittlungsweg einzurichten**, der die übermittelten Nachrichten gegen unbefugte Kenntnisnahme Dritter durch eine Ende-zu-Ende-Verschlüsselung schützt.

Das beA ist mithin **in der von der Beklagten gewählten aktuellen Grundkonzeption gesetzeswidrig**.

BB) VERSTOß GEGEN § 31A ABSATZ 1 I. V. M. § 31C NR. 3 BUCHSTABE B BRAO I. V. M. DEN §§ 19 ABSATZ 1 SATZ 1, 20 ABSATZ 1 SATZ 2 RAVPV

Des Weiteren verstößt das beA in seiner derzeitigen von der Beklagten nach § 31a Absatz 1 BRAO zu verantwortenden HSM-Architektur gegen die **rechtlichen Vorgaben der auf Grundlage der Bundesrechtsanwaltsordnung erlassenen Rechtsanwaltsverzeichnis- und -postfachverordnung zur Einrichtung des beAs**.

Der Bundesgesetzgeber hat die Regelung der **Einzelheiten zur technischen Ausgestaltung des beAs** in § 31c Nr. 3 Buchstabe b BRAO **an den Verordnungsgeber delegiert**. Auf dieser Grundlage hat das Bundesministerium der Justiz und für Verbraucherschutz mit Zustimmung des Bundesrates in der **Rechtsanwaltsverzeichnis- und -postfachverordnung** Folgendes bestimmt:

§ 19 Absatz 1 Satz 1 RAVPV

Das besondere elektronische Anwaltspostfach dient der elektronischen Kommunikation der in das Gesamtverzeichnis eingetragenen Mitglieder der Rechtsanwaltskammern, der Rechtsanwaltskammern und der Bundesrechtsanwaltskammer mit den Gerichten auf einem **sicheren Übermittlungsweg**.

§ 20 Absatz 1 Satz 2 RAVPV

Die **Bundesrechtsanwaltskammer hat fortlaufend zu gewährleisten**, dass die in § 19 Absatz 1 genannten **Personen und Stellen miteinander sicher elektronisch kommunizieren können**.

Die hier verwendeten **unbestimmten Rechtsbegriffe** „sicherer Übermittlungsweg“ und „sichere elektronische Kommunikation“ sind dahingehend **auszulegen**, dass sie eine **Ende-zu-Ende-Verschlüsselung verlangen**.

(1) GRAMMATIK

Im Wortlaut verwendet der Verordnungsgeber lediglich das **allgemein-umschreibende Attribut** „sicher“. Insofern lässt sich allein aus der vom Normgeber gewählten Formulierung **nicht abschließend bestimmen**, unter welchen Bedingungen eine „sichere“ elektronischen Kommunikation über das beA gegeben ist.

(2) SYSTEMATIK

Normsystemtisch gibt § 20 Absatz 1 Satz 2 RAVPV zu erkennen, dass das Attribut „sicher“ in Bezug zu der Kommunikation zwischen den Personen zu verstehen ist, die das beA nutzen. Die gesetzlich verlangte **Sicherheit ist mithin nicht Selbstzweck**. Es genügt insofern nicht bereits, wenn das beA für sich, als Konstrukt, „sicher“ ist. Vielmehr bezieht der Verordnungsgeber den Sicherheitsaspekt ausdrücklich auf die **Kommunikation der beA-Nutzer miteinander**. Diese muss „sicher“ sein. Dies muss das beA gewährleisten, um seinerseits „sicher“ zu sein.

Diesen Befund stützt die **systematische Verknüpfung des § 20 Absatz 1 Satz 2 RAVPV mit § 174 Absatz 3 Satz 3 ZPO** über die Verweiskette der §§ 174 Absatz 3 Satz 3, 130a Absatz 4 Nr. 2 ZPO i. V. m. den §§ 31a Absatz 1, 31c Nr. 3 Buchstabe b BRAO. Wie vorstehend dargelegt, konkretisiert § 174 Absatz 3 Satz 3 ZPO den Rechtsbegriff des „sicheren Übermittlungsweges“ dahingehend, dass die **übermittelten Nachrichten gegen unbefugte Kenntnisnahme Dritter zu schützen** sind.

Vor diesem Hintergrund ist ein „sicherer Übermittlungsweg“ i. S. d. Rechtsanwaltsverzeichnis- und -postfachverordnung nur dann gegeben, wenn sichergestellt ist, dass **nur die jeweiligen Kommunikationspartner Zugriff auf die zwischen ihnen ausgetauschten Nachrichten** haben. Und dies kann **technisch nur durch eine Ende-zu-Ende-Verschlüsselung** gewährleistet werden, bei der **allein die miteinander Kommunizierenden ihre Nachrichten ver- und entschlüsseln** können, was wiederum voraussetzt, dass **ausschließlich sie über ihre eigenen privaten Schlüssel verfügen**.

(3) HISTORIE

Eine **eindeutige Aussage** dazu, dass die „Sicherheit“ des beAs im Sinne der RAVPV eine **Ende-zu-Ende-Verschlüsselung notwendig** voraussetzt, findet sich darüber hinaus in der Begründung des Ordnungsgebers, und dies an gleich **zwei Stellen**. Zum einen in den Ausführungen zu § 19 RAVPV:

„Soweit auch dabei stets die Beachtung der **elementaren Grundelemente des besonderen elektronischen Anwaltspostfachs (wie beispielsweise die Ende-zu-Ende-Verschlüsselung von Nachrichten)** sichergestellt sein muss, wird dies dadurch gewährleistet, dass auch für die Kommunikation mit anderen Stellen und Personen die Vorgaben des § 20 Absatz 1 RAVPV gelten“.

Verordnung des Bundesministeriums der Justiz und für Verbraucherschutz über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (Rechtsanwaltsverzeichnis- und -postfachverordnung - RAVPV), BR-Drs. 417/16 vom 10. August 2016, S. 35 zu § 19 Absatz 1 (**Anlage K 22**).

Und zum anderen zu § 20 RAVPV:

„Zur **Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung** hat der Betrieb der besonderen elektronischen Anwaltspostfächer nach Absatz 1 Satz 1 auf der Grundlage des Protokollstandards „Online Services Computer Interface“ (OSCI) oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu erfolgen“.

Ebd., S. 35 zu § 20 Absatz 1.

Damit ist unmissverständlich klargestellt, dass **nach dem Willen des Normgebers eine Ende-zu-Ende-Verschlüsselung zwingende Grundvoraussetzung für das beA** ist, um eine sichere Kommunikation der Nutzer zu gewährleisten.

In Anbetracht der **allgemein bekannten, eindeutigen Definition des Verfahrens der Ende-zu-Ende-Verschlüsselung** kann auch kein vernünftiger Zweifel bestehen, dass der Normgeber in Bezug auf das beA mit der Verwendung der **feststehenden, technischen Fachterminologie „Ende-zu-Ende-Verschlüsselung“** nicht etwa lediglich eine irgendwie geartete Verschlüsselung der elektronischen Kommunikation über das beA ausreichen lassen will, sondern vielmehr explizit die Sicherheit des beAs dergestalt fordert, dass **allein den beA-Nutzern die Ver- und Entschlüsselung ihrer über das beA versandten Nachrichten möglich sein darf**. Denn diese Anforderung ist, wie dargelegt, ihrerseits **„elementares Grundelement“ der Ende-zu-Ende-Verschlüsselung**.

(4) TELOS

Allein diese, vom Normgeber in der Begründung zu den §§ 19 und 20 RAVPV ausdrücklich formulierte Auslegung des „sicheren Übermittlungsweges“ als Ende-zu-Ende-Verschlüsselung wird auch dem **Sinn und Zweck** des rechtlichen Erfordernisses einer sicheren elektronischen Kommunikation zwischen den beA-Nutzern gerecht.

Wie dargestellt, soll das beA zuvörderst der **sicheren elektronischen Kommunikation zwischen Anwaltschaft und Gerichtsbarkeit** dienen. Darüber hinaus soll das beA ermöglichen, dass **jedermann** auf sicherem elektronischen Wege Nachrichten an die beA-Postfächer sämtlicher zugelassener Rechtsanwältinnen und Rechtsanwälte

sowie Syndikusrechtsnawältinnen und Syndikusrechtsanwälte senden kann. Dies können neben den in der RAVPV genannten Kammern auch Behörden sowie schließlich insbesondere auch **Mandanten** sein. So nimmt auch der Verordnungsgeber ausdrücklich Bezug auf den „**EGVP-Bürger-Client**“, über den nach eigenen Angaben der Beklagten (siehe oben bei I.3.a) S. 12) das beA erreichbar sein soll.

Demnach soll das beA das **elektronische Referenzkommunikationsmittel der Anwaltschaft** sein. Und schließlich ist diese auch schlechterdings **verpflichtet, das beA zu nutzen**, § 31a Absatz 6 BRAO.

Der Gesetzgeber hat folglich ein „**beA-Monopol**“ mit **Nutzungspflicht** geschaffen.

Vor diesem Hintergrund liegt es auf der Hand, dass das **beA in besonderer Weise eine sichere elektronische Kommunikation gewährleisten** muss. Dies betonte auch der **Bundesgesetzgeber**, als er die Nutzungspflicht in § 31a Absatz 6 BRAO festlegte:

„Mit der in ihm (Anm.: § 31a Absatz 1 BRAO) vorgesehenen Pflicht der Bundesrechtsanwaltskammer, für jeden Rechtsanwalt zum 1. Januar 2016 ein besonderes elektronisches Anwaltspostfach einzurichten, sollen die rechtlichen Grundlagen für den **mit besonderem Vertrauensschutz ausgestatteten elektronischen Rechtsverkehr des Anwalts mit den Gerichten sowie die Kommunikation von Anwalt zu Anwalt** geschaffen werden (Bundestagsdrucksache 17/12634, S. 38)“.

Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Beruf vom 05. September 2016, BT-Drs. 18/9521, S. 107 zu Nummer 8 (§ 31a BRAO-E) Buchstabe c Absatz 6 (**Anlage K 23**).

Dieser „**besondere Vertrauensschutz**“, den der elektronische Rechtsverkehr dem Willen des Gesetzgebers zufolge zu bieten hat, lässt sich technisch nur durch eine

Ende-zu-Ende-Verschlüsselung gewährleisten. Denn nur diese stellt sicher, dass **ausschließlich die Kommunikationspartner über die Ver- und Entschlüsselung der zwischen ihnen ausgetauschten Nachrichten verfügen**, sodass diese **vor einem Zugriff unberechtigter Dritter geschützt** sind.

(5) VERFASSUNGSKONFORME AUSLEGUNG

Das Ergebnis der klassischen Auslegung nach Grammatik, Systematik, Historie und Telos wird gestützt durch die **verfassungskonforme Auslegung** der §§ 19, 20 RAVPV.

In seinem Beschluss vom 20. Dezember 2017 – **mithin kurz vor dem Bekanntwerden der gravierenden Sicherheitsmängel des beAs** – hat das **Bundesverfassungsgericht** konstatiert:

„Das beA verwendet zur sicheren Übermittlung eine so genannte **Ende-zu-Ende-Verschlüsselung** (vgl. § 20 Abs. 1 RAVPV)“.

BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 20. Dezember 2017 – 1 BvR 2233/17, Rn. 5.

Demzufolge legt auch das Bundesverfassungsgericht den § 20 Absatz 1 RAVPV dahingehend aus, dass das **beA eine Ende-zu-Ende-Verschlüsselung gewährleisten muss**.

Es darf dabei davon ausgegangen werden, dass sich das Bundesverfassungsgericht – bedauerlicherweise – in dem Verfassungsbeschwerdeverfahren **nicht damit auseinandersetzte, ob das beA auch tatsächlich die rechtlich verlangte Ende-zu-Ende-Verschlüsselung sicherstellt**. Dies ergibt sich aus der Feststellung der Kammer:

„jedenfalls aber **fehlt es an einer Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen** wie etwa der **Ende-zu-Ende-Verschlüsselung**“.

Ebd., Rn. 14.

Da es sich bei der Entscheidung um einen **Nichtannahmebeschluss** handelt, wurde zudem **weder eine mündliche Verhandlung noch eine Sachverständigenanhörung** durchgeführt, § 93d i. V. m. § 93b BVerfGG (Bundesverfassungsgerichtsgesetz in der Fassung der Bekanntmachung vom 11. August 1993 <BGBl. I S. 1473>, zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Oktober 2017 <BGBl. I S. 3546>). Insofern war es dem Bundesverfassungsgericht schlechterdings **nicht möglich, die tatsächliche technische Umsetzung des beAs durch die Beklagte zu beurteilen**.

Und schließlich verdeutlicht die **ausdrückliche Bezugnahme auf § 20 Absatz 1 RAVPV**, dass die Kammer offenkundig allein von den **rechtlichen Vorgaben** ausging und **keine Feststellung zur tatsächlichen Funktionsweise des beAs** getroffen hat.

Weiter ist auf die **Rechtsprechung des Bundesverfassungsgerichts zur freien Advokatur** zu verweisen, die **besonders hohe Anforderungen** an die Rechtfertigung von Maßnahmen stellt, die in die **anwaltliche Berufsfreiheit** eingreifen:

„Die Herauslösung des **Anwaltsberufs** aus beamtenähnlichen Bindungen und seine Anerkennung als ein **vom Staat unabhängiger freier Beruf** kann als ein wesentliches Element des Bemühens um rechtsstaatliche Begrenzung der staatlichen Macht angesehen werden, das der Verfassungsgeber vorgefunden und in seinen Willen aufgenommen hat. Es entspricht dem **Rechtsstaatsgedanken** und dient der Rechtspflege, dass dem **Bürger** schon aus Gründen der Chancen- und Waffengleichheit **Rechtskundige zur Verfügung stehen, zu denen er Vertrauen hat** und die seine Interessen möglichst frei und unabhängig von staatlicher Einflussnahme wahrnehmen können“.

BVerfGE 63, 266 (283 f.).

Insofern ist zu konstatieren:

„Die **sachliche und organisatorische Ausgestaltung der Kanzlei** als Raum zur Entfaltung der verfassungsrechtlich verbürgten unabhängigen und freien

anwaltlichen Tätigkeit **muss ganz grundsätzlich dem Rechtsanwalt selbst überlassen bleiben.**

Ein Eingriff hierin kann allenfalls insoweit gerechtfertigt sein, als dies **für die anwaltliche Tätigkeit zwingend erforderlich** und dem **Rechtsanwalt zumutbar** ist. Denn es ist die ureigene, höchstpersönliche Entscheidung des Rechtsanwalts, selbst und frei darüber zu entscheiden, **„welche sachlichen, personellen und organisatorischen Mittel für seine individuelle Art der Berufsausübung erforderlich sind“** (Weyland in Feuerich/Weyland, § 5 Rn. 6; Hartung in ders., Berufs- und Fachanwaltsordnung, 5. Aufl. 2012, § 5 Rn. 61)“.

Delhey, Verfassungsrechtliche Grenzen einer Pflicht für Rechtsanwälte zur Nutzung elektronischer Kommunikationsmittel, NJW 2016, 1274 (1278) (**Anlage K 24**).

Auch der **EGMR** anerkennt die gebotene **Vertraulichkeit anwaltlicher Kommunikation** in seiner ständigen Rechtsprechung und gewährt ihr **Schutz nach Artikel 8 EMRK**.

Siehe etwa jüngst EGMR, Urteil vom 27. April 2017 – 73607/13 Sommer vs. Deutschland m. w. N. sowie speziell zum **Schutz elektronischer anwaltlicher Kommunikation** EGMR, Urteil vom 16. Oktober 2007 – 74336/01 Wieser u. a. vs. Österreich; Urteil vom 03. April 2007 – 62617/00 Copland vs. Vereinigtes Königreich.

Und schließlich ist auf die besondere **Bedeutung der Vertraulichkeit anwaltlicher Kommunikation für die Mandantinnen und Mandanten** und damit **potentiell für jede Bürgerin und jeden Bürger** hinzuweisen. Das **Bundesverfassungsgericht** hat dies bereits klargestellt:

„Der Schutz der **Vertrauensbeziehung zwischen Anwalt und Mandant** liegt darüber hinaus auch **im Interesse der Allgemeinheit** an einer **wirksamen und geordneten Rechtspflege**. Diese Belange verlangen eine **besondere Beachtung** bei der Prüfung der **Angemessenheit** der Zwangsmaßnahme (vgl. BVerfGE 113, 29 <47 ff.>)“.

BVerfG, Beschluss vom 29. Januar 2015 – 2 BvR 497/12, juris-Rn. 18.

Es ist daher

„(...) zu vergegenwärtigen, dass Rechtsanwälte ihre **„eigenständige und unabhängige Funktion in der Durchsetzung des Rechts“** (...) gerade in Bezug auf ihre jeweiligen **Mandanten**‘ wahrnehmen (BVerfGE 108, 150 <158>). Plakativ formuliert: **Hinter jedem Rechtsanwalt steht ein Mandant**. Eine Pflicht für Rechtsanwälte zur Nutzung elektronischer Kommunikationsmittel wirkt sich damit mittelbar auch auf den Bürger aus, der anwaltliche Vertretung in Anspruch nimmt. Verpflichtet der Staat die Rechtsanwaltschaft zur elektronischen Kommunikation, so greift er damit zugleich in das **Recht auf mediale Selbstbestimmung des Bürgers als Mandanten des Rechtsanwalts** ein. – Im Rechtsstaat ist die Freiheit des Rechtsanwalts bei der Ausübung seines Berufs zugleich ein **Gradmesser für die Freiheit des Bürgers** (BVerfGE 63, 266 <312>).

Delhey, Verfassungsrechtliche Grenzen einer Pflicht für Rechtsanwälte zur Nutzung elektronischer Kommunikationsmittel, NJW 2016, 1274 (1278).

Vor diesem Hintergrund ist evident, dass die **elektronische anwaltliche Kommunikation**, zu der die **gesamte Anwaltschaft ausnahmslos verpflichtet** ist, besonderen Sicherheitsmaßstäben genügen muss – und eben dies kann nur durch eine **Ende-zu-Ende-Verschlüsselung** gewährleistet werden.

CC) ZWISCHENERGEBNIS: RECHTSWIDRIGKEIT DER EINRICHTUNG DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Das beA verstößt in seiner derzeitigen von der Beklagten verantworteten **HSM-Architektur, die keine Ende-zu-Ende-Verschlüsselung gewährleistet**, zum einen gegen die Vorgaben des Bundesgesetzgebers zur Einrichtung des beAs als sicherer Übermittlungsweg zur elektronischen Kommunikation mit den Gerichten nach **§ 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO** sowie zum anderen gegen die rechtlichen Vorgaben der auf Grundlage der Bundesrechtsanwaltsordnung erlassenen Rechtsanwaltsverzeichnis- und -postfachverordnung zur Einrichtung des beAs gemäß **§ 31a Absatz 1 i. V. m. § 31c Buchstabe b BRAO i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV**.

B) VERLETZUNG DER BERUFS AUSÜBUNGSFREIHEIT DER KLÄGERIN UND DER KLÄGER DURCH RECHTSWIDRIGE EINRICHTUNG DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Die von der Beklagten vorgenommene unrechtmäßige Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung **verletzt die Klägerin und die Kläger in ihren Rechten.**

AA) EINGRIFF IN DEN SCHUTZBEREICH

Die von der Beklagten zu verantwortende Ausgestaltung des beAs ohne Ende-zu-Ende-Verschlüsselung stellt einen ungerechtfertigten Eingriff in die Berufsausübungsfreiheit der Klägerin und der Kläger dar.

Nach der Rechtsprechung des Bundesverfassungsgerichts handelt es sich bei den Rechtsvorschriften zum beA um **Berufsausübungsregelungen** (BVerfG, Beschluss vom 20. Dezember 2017 – 1 BvR 2233/17, Rn. 10). Die auf eben diesen Normen beruhende tatsächliche **Einrichtung des beAs durch die Beklagte** stellt dementsprechend einen **Eingriff** in die von **Artikel 12 Absatz 1 GG** gewährleistete **Berufsfreiheit der Klägerin und der Kläger** dar. Schließlich sind diese **verpflichtet, das beA bei der Ausübung ihrer anwaltlichen Berufstätigkeit zu nutzen**, § 31a Absatz 6 BRAO. Insofern liegt in der technischen Ausgestaltung und Zurverfügungstellung des beAs ohne Ende-zu-Ende-Verschlüsselung ein **finaler, unmittelbarer und auch erheblicher Eingriff in Gestalt eines Realaktes** der Beklagten vor; das Grundrecht auf freie anwaltliche Berufsausübung schützt anerkanntermaßen auch vor **faktischen Beeinträchtigungen**:

„Die anwaltliche Berufsausübung wird seit einem Jahrhundert durch den **Grundsatz der freien Advokatur** gekennzeichnet, der **einer staatlichen Kontrolle und Bevormundung grundsätzlich entgegensteht** (vgl. BVerfGE

15, 226 (234); 34, 293 (302); 37, 67 (78)). Auch der **Vorstand der Rechtsanwaltskammer** darf gemäß Art. 12 Abs. 1 GG in die freie anwaltliche Berufsausübung nur aufgrund eines Gesetzes und **nur durch solche Maßnahmen eingreifen, die materiellrechtlich den Anforderungen an Berufsausübungsregelungen genügen** (vgl. BVerfGE 36, 212 (219)). Im übrigen unterliegt die anwaltliche Berufsausübung unter der Herrschaft des Grundgesetzes der **freien und unreglementierten Selbstbestimmung des Einzelnen**“.

BVerfG, Beschluss vom 08. November 1978 – 1 BvR 589/72, juris-Rn. 37.

BB) RECHTSWIDRIGKEIT DES EINGRIFFS

Der **Anwaltsgerichtshof Berlin** hat bereits **klargestellt**, dass in Bezug auf das **beA** der **Gesetzesvorbehalt** gilt:

„Ein solcher **Eingriff in die anwaltliche Berufsfreiheit durch Öffnung eines Anwaltspostfachs (...)** bedarf einer **hinreichend bestimmten gesetzlichen Grundlage** (Art. 12 Abs. 1 Satz 1 GG)“.

Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15, juris-Rn. 24.

Wie dargelegt, **verstößt die von der Beklagten realisierte Ausgestaltung des beAs ohne Ende-zu-Ende-Verschlüsselung gegen die einschlägigen gesetzlichen Vorgaben des Gesetzgebers** aus § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO sowie § 31a Absatz 1 i. V. m. § 31c Buchstabe b BRAO i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV. Sie **genügt folglich nicht den materiellrechtlichen Anforderungen der zitierten einschlägigen gesetzlichen Berufsausübungsregelungen** und ist somit **rechtswidrig**.

C) ANSPRUCH AUF UNTERLASSUNG DER EINRICHTUNG DES BEAS OHNE ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Der **Anwaltsgerichtshof Berlin** hat bereits klargestellt, dass gegenüber der Beklagten ein **Unterlassungsanspruch in Bezug auf eine rechtswidrige Inbetriebnahme des beAs** besteht.

Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 16/15, juris-Rn. 18.

Damals **mangelte es an einer gesetzlichen Grundlage** für die beA-Nutzungspflicht. Inzwischen besteht zwar mit § 31a Absatz 6 BRAO eine solche. Allerdings liegt der Fall vorliegend nunmehr so, dass **das beA gegen die einschlägigen gesetzlichen Vorgaben zu seiner Einrichtung verstößt**. Im Ergebnis läuft dies auf dasselbe hinaus:

Ein gesetzwidriges beA ist nicht weniger rechtswidrig und grundrechtsverletzend als ein gesetzloses beA.

D) ANSPRUCH AUF EINRICHTUNG DES BEAS MIT ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Des Weiteren leitet sich ein **subjektives Recht** der Klägerin und der Kläger auf ein **beA mit Ende-zu-Ende-Verschlüsselung** ab aus § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO i. V. m. § 31a Absätze 1 und 6 i. V. m. § 31c Nr. 3 i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV i. V. m. 43a Absatz 2 Satz 1 BRAO.

Nach der in ständiger höchstrichterlicher Rechtsprechung anerkannten „**Schutznormtheorie**“ gilt,

„dass ein **subjektives öffentliches Recht** dann vorliegt, wenn ein Rechtssatz des öffentlichen Rechts **nicht nur öffentlichen Interessen**, sondern – **zumindest auch** – **Individualinteressen derart zu dienen bestimmt** ist, dass die Träger der Individualinteressen die **Einhaltung des Rechtssatzes sollen verlangen können** (sogen. Schutznormtheorie)“.

BVerwG, Urteil vom 15. November 1985 – 8 C 43/83, juris-Rn. 15 m. w. N.

Ob diese Voraussetzungen vorliegen, ist durch **Auslegung** zu ermitteln, wobei dem Willen des Gesetzgebers, wie er sich aus den **Gesetzgebungsmaterialien** ergibt, regelmäßig **besondere Bedeutung** beigemessen wird.

Siehe nur Wahl/Schütz, in: Schoch/Schneider/Boer, Verwaltungsgerichtsordnung, 33. EL Juni 2017, § 42 Absatz 2 Rn. 45 m. w. N.

AA) SCHUTZZWECK: GEWÄHRLEISTUNG EINER SICHEREN ELEKTRONISCHEN ANWALTlichen KOMMUNIKATION MIT DEN GERICHTEN UNTER WAHRUNG ANWALTlicher VERSCHWIEGENHEIT

Das Normenkonvolut bezweckt den **Schutz der vertraulichen anwaltlichen Kommunikation über das beA**. Dieser normative Schutzzweck ergibt sich unzweifelhaft nicht nur bereits aus dem Wortlaut der Normen und ihrem systematischen Zusammenhang (vgl. oben bei II.2.a)bb), S. 39), sondern geht zudem eindeutig aus den begründenden Ausführungen des **Gesetzgebers** hervor, die hier im Kern nochmals zitiert werden sollen:

„Mit der in ihm (Anm.: § 31a Absatz 1 BRAO) vorgesehenen Pflicht der Bundesrechtsanwaltskammer, für jeden Rechtsanwalt zum 1. Januar 2016 ein besonderes elektronisches Anwaltspostfach einzurichten, sollen die rechtlichen Grundlagen für den **mit besonderem Vertrauensschutz ausgestatteten elektronischen Rechtsverkehr des Anwalts mit den Gerichten sowie die Kommunikation von Anwalt zu Anwalt** geschaffen werden (Bundestagsdrucksache 17/12634, S. 38)“.

Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im

Bereich der rechtsberatenden Berufe vom 05. September 2016, BT-Drs. 18/9521, S. 107 zu Nummer 8 (§ 31a BRAO-E) Buchstabe c Absatz 6.

Wie bereits dargelegt, ist die **Sicherheit des beAs kein reiner Selbstzweck**, sondern vielmehr **bezogen auf die Gewährleistung vertraulicher anwaltlicher Kommunikation**, wie sich insbesondere aus der Anforderung an das beA, **übermittelte Nachrichten vor unbefugtem Zugriff Dritter zu schützen**, ergibt, § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO i. V. m. §§ 31a Absätze 1 und 6, 31c Nr. 3 BRAO i. V. m. §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV.

Im Übrigen würden andernfalls die **gesetzlich vorgegebenen Pflichten der Klägerin und der Kläger** zur Nutzung des beAs (§ 31a Absatz 6 BRAO) einerseits sowie zur anwaltlichen Verschwiegenheit (§ 43a Absatz 2 Satz 1 BRAO) andererseits schlechterdings miteinander **kollidieren**, sollte die gesetzlich geforderte Sicherheit des beAs nicht zugleich die Vertraulichkeit der anwaltlichen Kommunikation gewährleisten müssen.

Vgl. Löschhorn a. a. O., 209.

BB) SCHUTZ DES ANWALTlichen INDIVIDUALINTERESSES AN EINER SICHEREN, VERTRAULICHEN ELEKTRONISCHEN KOMMUNIKATION ÜBER DAS BEA

Der dargestellte normative Schutzzweck dient auch ersichtlich in sachlicher wie personeller Hinsicht konkret dem **individuellen Interesse der Klägerin und der Kläger** an einer sicheren, vertraulichen elektronischen (syndikus-)anwaltlichen Kommunikation über das beA, wie ebenfalls bereits der vorstehend zitierten Passage der Gesetzesbegründung unmissverständlich zu entnehmen ist.

CC) RECHT AUF EINHALTUNG DER SCHUTZNORMEN

Die Klägerin und die Kläger haben gegenüber der Beklagten auch ein **Recht auf Einhaltung der mit Schutzwirkung zugunsten ihrer vertraulichen anwaltlichen Kommunikation ausgestatteten Vorschriften über die Einrichtung eines beAs.**

In den Worten *Georg Jellineks* (System der subjektiven öffentlichen Rechte, 2. Auflage 1905, S. 51) haben sie die „**Fähigkeit, Rechtsnormen im individuellen Interesse in Bewegung zu setzen**“.

(1) RECHT AUF RECHTMÄßIGES HANDELN DER KAMMER ALS DER PFLICHTMITGLIEDSCHAFT INHÄRENTER ANTAGONISMUS

„Es entspricht gefestigter Rechtsprechung des Bundesverwaltungsgerichts, daß die **Mitglieder öffentlich-rechtlicher Verbände mit Pflichtmitgliedschaft**, worunter auch die **berufsständischen Kammern** fallen, von dem Verband die **Einhaltung der Grenzen verlangen können, die seinem Tätigwerden durch die gesetzlich normierte Aufgabenstellung gezogen sind** (vgl. insbesondere BVerwGE 34, 69; 59, 231 (238); 59, 242 (245); a.A. Fröhler/Oberndorfer, Körperschaften des öffentlichen Rechts und Interessenvertretung, 1974, S. 77). Das folgt insbesondere aus **Art. 2 Abs. 1 GG**, der nicht nur das Recht gewährt, von der Mitgliedschaft in einem "unnötigen" Verband verschont zu bleiben, sondern **dem einzelnen Mitglied auch ein Abwehrrecht gegen solche Eingriffe des Verbandes in seine Handlungsfreiheit einräumt, die sich nicht im Wirkungskreis legitimer öffentlicher Aufgaben halten oder bei deren Wahrnehmung nicht dem Gebot der Verhältnismäßigkeit entsprechen wird** (Urteil vom 24. September 1981 - BVerwG 5 C 53.79 -)“.

BVerwG, Urteil vom 17. Dezember 1981 – 5 C 56/79, juris-Rn. 16.

Nach dieser ständigen höchstrichterlichen Rechtsprechung des Bundesverwaltungsgerichts folgt aus der **Pflichtmitgliedschaft in einer berufsständischen Kammer** mithin – als **inhärenter Antagonismus** – das **Recht des Pflichtmitgliedes gegenüber der Kammer auf Einhaltung der rechtlichen Grenzen ihres Tuns.**

Daher folgt das subjektive Recht der Klägerin und der Kläger, von der Beklagten zu verlangen, dass diese die rechtlichen Anforderungen an die Einrichtung des beAs erfüllt, bereits aus der **Kammerpflichtmitgliedschaft der Klägerin und der Kläger**.

(2) GRUNDRECHTLICHER ANSPRUCH AUF RECHTMÄßIGKEIT STAATLICHEN HANDELNS

Bei der vorstehenden Rechtsfigur, die das **subjektive Recht aus einer individuellen Pflicht ableitet**, handelt es sich letztlich um eine Ausprägung des allgemein anerkannten rechtsstaatlichen Grundsatzes, dass **Artikel 2 Absatz 1 GG** jedermann ein „**Grundrecht auf Gesetzmäßigkeit**“ (Herzog, AöR 86 <1961>, 194, 202 Fn. 37) gewährt:

„Die **Freiheit der Entfaltung der Persönlichkeit** erschöpft sich nicht in der **allgemeinen Handlungsfreiheit**, sondern umfaßt in unserer grundgesetzlichen Ordnung auch den **grundrechtlichen Anspruch, durch die Staatsgewalt nicht mit einem Nachteil belastet zu werden, der nicht in der verfassungsmäßigen Ordnung begründet ist**“.

BVerfG, Beschluss vom 08. Januar 1959 – 1 BvR 425/52, juris-Rn. 25.

Das **Bundesverwaltungsgericht** hat dies bezüglich eines grundrechtlichen Anspruches auf rechtmäßiges **schlicht hoheitliches Verwaltungshandeln durch Realakt** – wie es vorliegend in der tatsächlichen Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung gegeben ist – wie folgt **konkretisiert**:

„Die **Grundrechte schützen den Bürger vor rechtswidrigen Beeinträchtigungen jeder Art**, auch solchen durch **schlichtes Verwaltungshandeln (Verwaltungsrealakt)**. Infolgedessen kann der Bürger, wenn ihm - wie dies hier von den Klägern geltend gemacht wird - eine derartige Rechtsverletzung droht, **gestützt auf das jeweils berührte Grundrecht Unterlassung verlangen** (BVerwGE 44, 235 <243>; Urteil vom 21. September 1984 - BVerwG 4 C 51.80 -, NJW 1985, 1481; BVerwGE 71, 183 <189, 199>)“.

BVerwG, Urteil vom 23. Mai 1989 – 7 C 2/87, juris-Rn. 48.

Damit kann das subjektive Recht der Klägerin und der Kläger auf die rechtmäßige Ausgestaltung des beAs durch die Beklagte subsidiär jedenfalls auch **auf Artikel 2 Absatz 1 GG gestützt** werden.

E) SPRUCHREIFE

Der Anwaltsgerichtshof kann die Beklagte auch konkret zu der von der Klägerin und den Klägern begehrten **Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung** verurteilen.

Nach zutreffender Ansicht kommt es bei einer **allgemeinen Leistungsklage**, deren Gegenstand ein schlicht hoheitliches Verwaltungshandeln ist, **nicht auf die Spruchreife** i. S. v. § 113 Absatz 5 VwGO an, weil die Vorschrift ausweislich ihres Wortlautes **nur für Verpflichtungsklagen auf Erlass eines Verwaltungsaktes** gilt.


Stuhlfauth, in: Bader/Funke-Kaiser/Stuhlfauth/von Albedyll, Verwaltungsgerichtsordnung, 6. Auflage 2015, § 113 Rn. 97.

Aber auch dann, wenn man **§ 113 Absatz 5 VwGO analog** anwenden wollte, **läge Spruchreife vor**. Denn der Beklagten ist **kein Ermessen** eingeräumt, das beA mit oder ohne Ende-zu-Ende-Verschlüsselung einzurichten. Gemäß § 20 Absatz 1 Satz 2 RAVPV „**hat**“ die Beklagte die sichere elektronische Kommunikation über das beA „**zu gewährleisten**“.

Da dies, wie dargelegt, die technische Ausgestaltung mit einer **Ende-zu-Ende-Verschlüsselung notwendig indiziert**, verbleibt der Beklagten insoweit kein Ermessensspielraum.

Vollmachten der Kläger zu 2), 3), 4), 6) und 7) im Original anbei. Die Vollmachten der Kläger zu 1) und 5) werden alsbald nachgereicht.

Zwei Abschriften anbei.


Baum
Rechtsanwalt