Anwaltsrecht

Verschwiegenheitspflicht und Datenschutz: Was das Recht von Kanzlei fordert

Abschlussbericht des Ausschusses 6 der 6. Satzungsversammlung*

Prof. Dr. Thomas Gasteyer, Frankfurt am Main (als Vorsitzender des Ausschusses 6 der 6. Satzungsversammlung)

Wie Anwältinnen und Anwälte mit die Pflicht zur Verschwiegenheit umgehen sollen und wie sie die Vorgaben des Datenschutzes beachten können, ist in den vergangenen Jahren zu einer zentralen Frage geworden. Der Gesetzgeber hat im Berufsrecht, aber auch im Datenschutz versucht, das Recht der Wirklichkeit in einer digitalisierten Welt anzupassen. Die Satzungsversammlung hat durch beständige Fortschreibung des § 2 BORA mit der Entwicklung Schritt gehalten. Im Mai 2019 hat sie einen neuen Abs. geschaffen, der vor allem die E-Mail Kommunikation regelt, Erleichterungen für die Praxis bietet und frühestens zum 1. November 2019 in Kraft treten wird (Lührig, AnwBl 2019. 330). Das Anwaltsblatt dokumentiert den Abschlussbericht des Ausschusses 6, weil er nicht nur einen Überblick des Zusammenspiels von Zivil-, Straf-, Berufs- und Datenschutzrecht gibt, sondern auch den zukünftigen § 2 Abs. 2 BORA erläutert.

1. Einleitung

Der Ausschuss 6 der 6. Satzungsversammlung hat insgesamt vierzehnmal in Präsenzsitzungen oder Telefonkonferenzen getagt. Weitere Sitzungen fanden in Unterausschüssen statt. Mit seinem Abschlussbericht („Bericht“) fasst er die Erkenntnisse aus seiner Tätigkeit sowie verbliebene offene Fragen zur Unterrichtung eines Nachfolgeausschusses der 7. Satzungsversammlung und zur Erleichterung seiner künftigen Arbeit zusammen.

Zugleich kann der Bericht unseren Kolleginnen und Kollegen in Teilen als Grundlage für die praktische Umsetzung des § 2 Abs. 4 BORA dienen. Der Bericht ist keine Handlungsanweisung, sondern eine Hilfestellung.

Der Bericht konzentriert sich auf die im Ausschuss und im Plenum diskutierten Themen und ist nicht als allgemeiner oder gar abschließender Kommentar zu den unten aufgeführten Rechtsvorschriften zu verstehen. Wenn für den Ausschuss offensichtlich unter Beachtung der Satzungskompetenz der Satzungsversammlung kein Bedarf zur Ausfüllung einer gesetzlichen Regelung oder zur Klärung eines Themas bestand, geht dieser Bericht nicht hierauf ein. Außerdem hat sich der Ausschuss 6 nach einem Gespräch beim Bundesamt für Sicherheit in der Informationstechnik (BSI) bemüht, in Anlehnung an das BSI-Papier C 5 (Anforderungskatalog Cloud Computing)[1] die einzelnen Risikosituationen in der anwaltlichen Praxis zu erfassen und zu bewerten. Diese Arbeit wurde nicht vollendet, zahlreiche Detailerkenntnisse flossen jedoch in den Bericht und insbesondere die Anlagen ein.

2. Grenzen der Regulierung

2.1

Eine kasuistisch abschließende Regelung des von einem Rechtsanwalt zum Schutz der Vertraulichkeit und der Daten erwarteten Verhaltens durch Normsetzung ist nicht möglich, da sich Anforderungen der Mandanten, deren Gegner oder Verhandlungspartner sowie der Gerichte und Behörden, das technische Umfeld und Angebot und die Arbeitsorganisation laufend ändern. Die Verantwortung liegt daher bei dem einzelnen Rechtsanwalt, da nur er seine Kanzlei, ihre Organisation und vorhandene Risiken kennt und darauf eingehen kann.

2.2

Dieses Konzept ist mit dem Ansatz des BSI konform. In Bezug auf Dienstleister im Gebiet Cloud-Computing wurde vom BSI ein Anforderungskatalog Cloud Computing (C 5) entwickelt, der aber keine abschließende Vorgabe für Organisation und Verhalten, sondern Prüfungsschritte für die Evaluation durch zum Beispiel Wirtschaftsprüfer oder den Kunden darstellt. Die Verantwortung liegt damit beim Nutzer.

3. Übersicht der relevanten Normen

3.1 Das Berufsgeheimnisschutzgesetz mit § 203 StGB sowie §§ 43 a und 43 e BRAO

Das Berufsgeheimnisschutzgesetz[2] ermöglichte Ende 2017 im Wege einer grundlegenden Reform die rechtssichere Einbeziehung von Outsourcing- Dienstleistern in die Abläufe der Kanzlei, § 203 Abs. 3 StGB. Abgesichert wurde dies durch deren Einbeziehung in den Adressatenkreis der Strafnorm und die Gewährung von Beschlagnahmeschutz und Zeugnisverweigerungsrechten, vgl. 6.1. 43 a Abs. 2 BRAO wurde um entsprechende Sorgfaltsanforderungen bei der Einbeziehung von externen Dienstanbietern erweitert, der neue § 43 e BRAO setzt die Rahmenbedingungen für die Involvierung von Dienstleistern. Der Gesetzgeber hat dabei verschiedene Anforderungen aus dem damaligen § 2 BORA in ähnlicher, aber nicht identischer Form übernommen, was zu Reformbedarf bei § 2 BORA führte. Die Fortschreibung des § 2 BORA wird voraussichtlich fortzuführen sein, wenn und sobald Fälle der Praxis Regelungsbedarf indizieren.

3.2 § 280 BGB

Das Verhalten des Rechtsanwalts wird auch durch seine zivilrechtlichen Verpflichtungen bestimmt. Diese Pflichten können weiter gehen als die berufs- rechtliche Pflichtenlage und eingreifen, auch wenn ein Verhalten oder Unterlassen keinen Verstoß gegen Straf-, Berufs- oder Datenschutzrecht darstellt. Das diese Verhaltenssteuerung durch zivilrechtliche Normen vorhanden sein kann, war dem Ausschuss bewusst, wenn er den Bedarf zusätzlicher Regulierung bedachte.

* Der Abschlussbericht des Ausschusses 6 „Verschwiegenheitspflicht und Datenschutz“ der 6. Satzungsversammlung ist auf dem Stand vom 5. April 2019.

1 BSI Anforderungskatalog Cloud Computing: https://www.bsi.bund.de/.

2 Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017, BGBl 2017 I 3618

3.3 Datenschutzrecht

Die DSGVO ist im Mai 2018 in Kraft getreten, das gänzlich neue BDSG wenig später. Sie haben die Diskussion über das Verhältnis von Datenschutz und Berufsrecht auf eine neue Grundlage gestellt (dazu 4.).

3.4 Telemediengesetz

Zeitgleich mit Inkrafttreten der DSGVO war ursprünglich die Einführung der ePrivacy-VO geplant, welche die ePrivacy Richtlinie ablösen soll. Eine endgültige Fassung steht noch aus. Die Datenschutzkonferenz (DSK) hat sich in Bezug auf die weitere Anwendbarkeit des Telemediengesetzes geäußert, insbesondere in Bezug auf die datenschutzrechtlichen Regelungen der §§ 12, 13 und 15 TMG. Laut DSK kommt als rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch Telemedienanbieter nur Art. 6 Abs. 1 der DSGVO in Frage.[3]

3.5 § 2 Abs. 3 und 4 BORA

Aufgrund der Neuregelung des § 43e BRAO hat die Satzungsversammlung § 2 BORA angepasst.

Abs. 3 behandelt Fälle, in denen keine Verschwiegenheitsbruch vorliegt, weil a) der Mandant sein Einverständnis abgibt, b) wenn das Verhalten des Rechtsanwalts zur Wahrnehmung berechtigter Interessen notwendig ist oder c) wenn es sozialadäquat ist. Anwälte müssen nach Abs. 4 aktiv das Mandatsgeheimnis wahren. Die Norm legt dem Anwalt die Pflicht auf, solche organisatorischen und technischen Maßnahmen zu ergreifen, die für die Wahrung des Mandatsgeheimnis erforderlich sind, so lange sie risikoadäquat sind. Zur Konsistenz und um die Belastungen zu reduzieren, können technische Maßnahmen als ausreichend betrachtet werden, so lange sie den Sicherheitsanforderungen der DSGVO gerecht werden. Außerdem müssen die technischen Maßnahmen dem Stand der Technik entsprechen, jedoch sind Maßnahmen nur durchzuführen, wenn der Aufwand in einem angemessenen Verhältnis zu den notwendigen Sicherheitsanforderungen steht.

4. Das Verhältnis des Datenschutzrechts zum Berufsrecht

4.1 Vorrang des formellen Gesetzes gegenüber dem Satzungsrecht (als untergesetzlichem materiellen Recht)

Alle in 3. aufgeführten Rechtsquellen, also die durch das Berufsgeheimnisschutzgesetz abgeänderten oder neu geschaffenen § 203 StGB, §§ 43a und 43e BRAO, § 280 BGB, die DSGVO, das BDSG sowie das TMG haben Vorrang gegenüber der BORA, weil Satzungsrecht hinter formelle Gesetze zurücktritt.

Das gilt dogmatisch auch im Verhältnis zu § 280 BGB. Jedoch sind Situationen vorstellbar, in denen aus der BORA ein Handlungsgebot abgeleitet werden kann, dessen Missachtung (etwa des erforderlichen Schutzniveaus) auch als Verletzung einer Nebenpflicht aus dem Anwaltsvertrag gewertet werden könnte. Dagegen stellt sich bei anderen Konstellationen die Frage nicht, ob ein Schadensersatzanspruch des Mandanten schon deswegen ausgeschlossen ist, weil sich der Anwalt berufs- rechtskonform verhalten hat.

Anders ist die Situation jedoch, wenn eine gesetzlich angeordnete Handlungspflicht (etwa Benutzung bestimmter Kommunikationswege) zu einem Schaden des Mandanten führt. Hier verdrängt möglicherweise die Pflicht zur Befolgung der gesetzlichen Anordnung die potenzielle Haftung wegen Verletzung einer Schutzpflicht gegenüber dem Mandanten. Anders formuliert: Wenn der Rechtsanwalt das beA benutzt, kann er nicht deswegen gegenüber den Mandanten schadensersatzpflichtig sein. Die Frage ist von der weiteren zu trennen, ob der Rechtsanwalt stets verpflichtet ist, gesetzlich vorgegebene Kommunikationswege zu wählen. Das ist zweifelhaft, aber eine Frage des Einzelfalls. Selbst wenn das Berufsrecht im Übrigen ein Verweigerungsrecht des Rechtsanwalts anerkennen sollte, ließe sich daraus keine spiegelbildliche Verweigerungspflicht begründen; es würde zu weit führen, jedem Anwalt die Rolle des Michael Kohlhaas abzuverlangen.

4.2 Vorrang das Datenschutzrechts und/oder dessen Integration in das Berufsrecht?

Vor Inkrafttreten der DSGVO wurde immer wieder die Frage thematisiert, ob angesichts der umfassenden Verpflichtungen zur Verschwiegenheit der Berufsgeheimnisträger das Datenschutzrecht überhaupt auf Anwaltskanzleien anwendbar ist.[4] Außerdem war strittig, wer die für Rechtsanwälte zuständige Aufsichtsbehörde ist. Die wohl überwiegende Meinung stellte zurecht darauf ab, ob gesetzliches Berufsrecht im Gegensatz zu den Regelungen des europäischen und deutschen Datenschutzrechts stand; im Übrigen „sollte" das Datenschutzrecht beachtet werden, soweit es nicht ohnehin – zum Beispiel beim Beschäftigtendatenschutz – unzweifelhaft anwendbar war.

Mit dem Inkrafttreten der DSGVO ist dieser Diskussion der Boden entzogen. Die DSGVO stellt unmittelbar und ohne einen Umsetzungsakt geltendes Recht dar. Das novellierte BDSG nimmt für sich in Anspruch, mit der DSGVO konform zu sein und sich mit seinen Regelungen innerhalb der durch die DSGVO eröffneten Spielräume zu halten. Die DSGVO sieht keine Bereichsausnahme für Rechtsanwälte und ist grundsätzlich auf Rechtsanwälte anwendbar,[5] jedoch geht das Mandatsgeheimnis im Falle eines Konfliktes vor. Dies wird insbesondere durch § 1 Abs. 2 Satz 2 BDSG unterstrichen („Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.").[6] Instruktiv sind die Ausführungen auf der Website der BRAK,[7] auf die verwiesen wird. Offen ist noch die politische Frage, ob für die verkammerten Berufe, also insbesondere die Rechtsanwaltschaft, jeweils ein besonderer Datenschutzbeauftragter eingesetzt werden sollte. Die Zuständigkeit zur Ahndung berufsrechtlicher Verstöße haben die RAK ohnehin.

Bei einzelnen Regelungen können gleichwohl Konflikte mit nationalen Gesetzen bestehen, insbesondere im Berufsrecht, und sie bedürfen dann der Lösung. Das AnwG Berlin hat kürzlich in der Begründung einer Entscheidung das Da-

3 *Gierschmann:* Positionsbestimmung der DSK zur Anwendbarkeit des TMG (ZD 2018, 297).

4 *Kulow* (2018, März). Datenschutz in der Kanzlei nach der Datenschutzgrundverordnung. Abgerufen von https://rak-muenchen.de/.

5 Fragen und Antworten zur DS-GVO und zum BDSG-neu – Stand Mai 2018, Abs. 2. (2018, Mai). Abgerufen 14. März, 2019, von https://www.brak.de/.

6 *Kulow* (2018, März). Datenschutz in der Kanzlei nach der Datenschutzgrundverordnung. Abgerufen von https://rak-muenchen.de/.

7 Informationen finden sich auf der Website der BRAK unter folgendem Link: https://www.brak.de/fuer- anwaelte/datenschutz.

tenschutzrecht in das Berufsrecht integriert.[8] Ein Verstoß gegen Regelungen des BDSG – heute also der Datenschutzgrundverordnung und ihren „Umsetzungsgesetzen" – stelle zugleich einen Berufsrechtsverstoß gegen die Generalklausel des § 43 BRAO dar. Die strikte Beachtung der datenschutzrechtlichen Regelungen gehöre zum Kernbereich anwaltlicher Pflichten.

Diese Begründung wurde im Ausschuss sehr unterschiedlich bewertet. Selbstverständlich sind Rechtsanwälte dazu verpflichtet, das Datenschutzrecht zu beachten, soweit keine spezifischen berufsrechtlichen Pflichten entgegenstehen. Auch verfolgt die Rechtsanwaltschaft und in vorderster Linie die BRAK das Ziel, einen Datenschutzbeauftragten für die Rechtsanwaltschaft einzurichten, der die Beachtung des Datenschutzrechts prüfen und etwaige Verstöße verfolgen soll. Damit deckt sich die Feststellung des Anwaltsgerichts über die Pflichten des Rechtsanwalts.

Andererseits aber ist nicht jede Rechtsverletzung ein Verstoß gegen Berufsrecht. Die Ahndung eines sonstigen Gesetzesverstoßes zugleich als Verletzung der Generalklausel § 43 BRAO setzt stets voraus, dass die Verletzungshandlung einen berufsrechtlichen Überhang aufweist. Nur unter dieser Voraussetzung kann im Übrigen gerechtfertigt sein, dass – wie hier – eine Rechtsanwaltskammer den Sachverhalt nochmals aufgreift, nachdem der für Datenschutz zuständige Datenschutzbeauftragte den Fall abgeschlossen hat. Außerdem sind die datenschutzrechtlichen Regelungen auf vielen Gebieten unklar, die den Kernbereich anwaltlicher Tätigkeit nicht berühren. Es erscheint für die Konsistenz der Auslegung und Rechtsfortbildung nicht wünschenswert, diese offenen Fragen neben den Verwaltungsgerichten von einem weiteren Gerichtszweig, den Anwaltsgerichten, klären zu lassen.

Der Ausschuss kam im Ergebnis zu folgender Auffassung:
(1) Im Grundsatz stehen das Datenschutz- und das Berufsrecht nebeneinander.
(2) Das allgemeine Datenschutzrecht gilt auch für alle Rechtsanwältinnen und Rechtsanwälte.
(3) Nicht jeder datenschutzrechtliche Verstoß stellt automatisch einen berufsrechtlichen Verstoß dar; eine Ahndungsbefugnis der Rechtsanwaltskammer setzt vielmehr einen berufsrechtlichen Überhang voraus.

Diese Überlegungen sollen keine Urteilsschelte sein. Jedoch ist das Verhältnis von Berufsrecht zu Datenschutzrecht alles andere als klar. Jeder Fall ist anders zu behandeln und jeweils zu überdenken. Wie schwierig die Bewertung sein kann, zeigt die Diskussion über die Verschlüsselung bei elektronischer Kommunikation. Der Ausschuss hat sich auch hierzu viele Gedanken gemacht und der Bericht kommt auf dieses Thema wieder zurück.

4.3

Der Normadressat der BRAO (und der sie im Rahmen der Ermächtigung konkretisierenden BORA) einerseits und der DSGVO/BDSG andererseits ist der Rechtsanwalt, und er muss beide beachten. Harmonisierung konfligierender Normen kann durch ihre Interpretation vor dem Hintergrund der Einheit der Rechtsordnung erzielt werden. Das jeweils geschützte Rechtsgut kann ein anderes sein, was bei ihrer Anwendung (gegebenenfalls teleologische Reduktion) auf den Lebenssachverhalt zu berücksichtigen ist. Das führt zu der Frage, ob man sich bei allen Unterschieden in der Zielsetzung der Normen zur Auslegung und Anwendung des Berufsrechts dennoch auf Wertungen der DSGVO und des BDSG stützen kann und vice versa. Das ist im Grundsatz zu begrüßen, erspart aber nicht das Überdenken im Einzelfall.

4.3.1

Nach § 43e Abs. 4 BRAO setzt zum Beispiel der Bezug von Dienstleistungen aus dem Ausland ein funktional äquivalentes Schutzniveau voraus. Der Schutzmechanismus muss nicht dem nach deutschem Recht entsprechen, aber der auf andere Weise gewährte Schutzeffekt muss äquivalent sein. Der Gesetzgeber ist davon ausgegangen, dass dies in allen Staaten der EU der Fall ist[9] und hat damit eine Wertung aus dem Datenschutzrecht übernommen. Berufsrechtlich gibt es keine Veranlassung, einen strengeren Maßstab anzulegen, auch wenn er europarechtskonform wäre. Mangels einer Rechtsverordnung als Richtschnur für Rechtsanwälte[10] ist die Übernahme dieser Wertung eine sachlich und rechtlich zu begrüßende Lösung.

4.3.2

Der Begriff „organisatorische und technische Maßnahmen" wird in § 2 Abs. 4 BORA benutzt, während das Datenschutzrecht die „technischen und organisatorischen Maßnahmen" kennt, vgl. Art. 32 DSGVO. § 2 Abs. 4 S. 2 BORA lässt sich entnehmen, dass der dortige Begriff weiter interpretiert werden kann, als er im Datenschutz verstanden wird. Ein Wertungswiderspruch ist aber nicht ersichtlich.

4.3.3

Wegen der Nähe der Wertungen wollte und konnte der Ausschuss eine doppelte Belastung des Anwalts durch unterschiedliche Maßstäbe vermeiden und hat in § 2 Abs. 4 S. 2 BORA bei technischen Maßnahmen die Beachtung des Datenschutzrechts für genügend erklärt; alle technischen Maßnahmen müssen aber dem Stand der Technik genügen.

5. Das nach Berufsrecht gebotene Schutzniveau

5.1 Rechtsquellen

Die Verpflichtung zur Verschwiegenheit in § 43a Abs. 2 BRAO besteht unabhängig von dem Regelungsumfang des § 203 StGB. Deswegen kann ein berufsrechtlicher Verstoß gegen die Verschwiegenheit vorliegen, auch wenn der Tatbestand des § 203 StGB nicht verwirklicht ist. Daher wird § 203 StGB nachstehend nicht vertieft betrachtet.

§ 43e BRAO ist auf die Einschaltung anderer Personen bei der Erbringung der anwaltlichen Dienstleistung fokussiert und lässt weitere Gebiete der Selbstorganisation des Anwalts unberührt. § 2 Abs. 4 BORA spricht von organisatorischen und technischen Maßnahmen. Diese Regelung deckt die gesamte Bandbreite anwaltlicher Organisation ab, also auch die „Technik- oder IT-fernen" Bereiche. Die Überlegungen des Satzungsgebers zur Bedeutung organisatorischer und tech-

8 AnwG Berlin, Beschluss vom 5.3.2018 – 1 AnwG 34/16, BeckRS 2018, 11237; auszugsweises Zitat: „Mit der Verletzung von §§ 4, 28 Abs. 1 Satz 1 Nr. 3 BDSG liegt zugleich ein Verstoß gegen anwaltliches Berufsrecht vor. Ein Rückgriff auf § 43 BRAO ist möglich, weil berufsrechtliche Spezialregeln fehlen, aber gegen in anderen Normen auferlegte Pflichten verstoßen wurde und diese berufsrelevanten Regelungsinhalt aufweisen. Die strikte Beachtung der datenschutzrechtlichen Regelungen gehört zum Kernbereich anwaltlicher Pflichten."

9 BT-Drs. 18/11936, 35.

10 Gefordert wurde im Vorfeld eine Rechtsverordnung der BMJV mit einer Liste der „sicheren" Staaten; Ausschuss für Recht und Verbraucherschutz, Protokoll-Nr. 18/146, 15.5.2017 https://www.bundestag.de/

nischer Maßnahmen sind daher insgesamt als Leitlinie für die Rechtsanwälte relevant. Die Begründung des Ausschusses zu § 2 Abs. 4 BORA[11] behandelt dieses Thema und ist Grundlage der nachstehenden Zusammenfassung.

5.2 Begriff der organisatorischen und technischen Maßnahmen im Sinne des Berufsrechts

5.2.1

Organisatorische Maßnahmen erfassen alle Maßnahmen, die dem Schutz der Vertraulichkeit mandatsbezogener Informationen dienen. Der Begriff ist weit zu verstehen und geht über die Anforderungen des Datenschutzes hinaus, der auf den Schutz von Daten und deren Sammlung, Speicherung und Verarbeitung konzentriert ist, nicht auf den Schutz sonstiger Informationen.

5.2.2

Technische Maßnahmen sind auch im Hinblick auf analoge Daten erforderlich, also etwa die Verwahrung von physischen Akten in gesicherten Räumen.

5.3 Maximale Sicherheit als unbedingtes Ziel oder „nur" risikoadäquater Schutz?

Der Rechtsanwalt muss gemäß § 2 Abs. 4 BORA geeignete technische und organisatorische Maßnahmen treffen, um ein risikoadäquates Schutzniveau zu gewährleisten. Die Norm ist kein unverbindlicher Appell, sondern begründet eine rechtliche Verpflichtung.

5.3.1

Welche Maßnahmen erforderlich sind, richtet sich nach dem Risiko, das nach Einschätzung des Rechtsanwalts für die von ihm verwahrten und/oder verarbeiteten Informationen besteht. Diese Risikobewertung ist der Ausgangspunkt für den Rechtsanwalt. Der Rechtsanwalt muss die Maßnahmen am Risikoprofil seiner Kanzlei und ihrer Mandantschaft messen, es wird also nicht erwartet, dass alle verfügbaren Maßnahmen ergriffen werden. Bei der Entscheidung über die Schutzmaßnahmen kann er deren Wirtschaftlichkeit berücksichtigen. Zweckmäßigerweise sollte er seine Überlegungen dokumentieren. Ziel ist nicht das Maximum an Sicherheit zu jedem Preis, sondern der nach Abwägung des Gefährdungspotentials und der denkbaren Schutzmaßnahmen angemessene Schutz. Diese Abwägung ist der nach Art. 32 DSGVO erforderlichen ähnlich,[12] nach dem geeignete technische und organisatorische Maßnahmen in einem ausgewogenen Verhältnis von möglichen Risiken, erzieltem Schutzniveau, Implementierungskosten und Stand der Technik stehen müssen.[13]

5.3.2

Stand der Technik" ist gesetzlich nicht definiert. Dem Begriff liegt die Annahme zugrunde, dass die technische Entwicklung schneller voranschreitet als die Rechtsetzung, weswegen der Normsetzer es vorzieht den Begriff „Stand der Technik" zu verwenden anstatt konkrete technische Anforderungen zu benennen. Technologien entsprechen regelmäßig dem Stand der Technik, wenn sie auf gefestigten Erkenntnissen beruhen und einem in der Praxis existierendem Standard entsprechen. Auch hiernach ist also nicht das jeweils Neueste gefordert. Der Einsatz technisch überholter Produkte reicht nicht aus.

Einzelne Überlegungen des Ausschusses aus seiner Befassung mit dem Papier C 5 finden sich in Anlage 5.3.2.

5.3.3

Das Risiko kann jedoch denklogisch nicht unter dem liegen, das allgemein für jeden besteht. Auf dem Gebiet der IT können daher gängige und marktübliche Programme zum Schutz und deren regelmäßige Aktualisierung als Minimum erwartet werden. Organisatorisch muss der Rechtsanwalt überdenken, welche Mitarbeiter in welchem Ausmaß Zugang zu den entsprechenden Daten haben sollen. Je nach Sensibilität des Mandats oder des Mandanten können Zugriffsbeschränkungen geboten sein. Grundsätzlich sollten sowohl die technischen als auch die organisatorischen Maßnahmen fortlaufend an die äußeren Entwicklungen angepasst werden.

5.4 Zumutbarkeit für den Anwaltsberuf

Eine Maßnahme ist nur erforderlich, wenn sie, objektiv betrachtet, dem Rechtsanwalt auch zumutbar ist. Der Ausschuss hat bei dieser Formulierung eher außergewöhnliche Situationen vor Augen gehabt, bei denen der Sicherheitsaufwand die normalen Kanzleiabläufe beeinträchtigt oder mit dem Berufsbild schwer in Einklang zu bringen ist. Zum Beispiel kann man bezweifeln, dass sich ein Rechtsanwalt zur Wahrung der Vertraulichkeit auf konspirative Treffen einlassen muss. Eine Abneigung gegenüber technologischen oder organisatorischen Schutzmaßnahmen oder ein fehlender Wille selbst zu überschaubaren Investitionen ändern an der objektiven Zumutbarkeit nichts.

5.5 § 2 Abs. 3 c) BORA, insbesondere Sozialadäquanz

Nach Inkrafttreten des Berufsgeheimnisschutzgesetzes hat sich der Ausschuss gefragt, ob das berufsrechtlich relevante Konzept der Sozialadäquanz damit überflüssig geworden war. Die 6. Satzungsversammlung hat nach Erlass der Berufsgeheimnisschutzgesetze trotz einer umfassenden Anpassung des § 2 BORA den Verweis auf die Rechtsfigur der Sozialadäquanz nicht gestrichen, weil sie trotz der detaillierten Regelung in § 43 e BRAO nach wie vor Raum und Bedarf für das Konzept der Sozialadäquanz sah. Das Berufsgeheimnisschutzgesetz befasst sich mit der Einschaltung Dritter, während Sozialadäquanz für alle anderen Fragen relevant bleibt. Das erklärt die Formulierung in § 2 Abs. 4 letzter Satz BORA. Ein Beispiel ist die Nutzung des Mobiltelefons. Der „normal" telefonierende Rechtsanwalt zeigt objektiv eine übliche, von der Allgemeinheit gebilligte Verhaltensweise im sozialen Leben (Sozialadäquanz). Dazu mehr in Anlage 6.4 Ziffer 1.2.

6. Einzelne Pflichten und Risiken – allgemeine Büroorganisation ohne Heranziehung von Dienstleistern

6.1 Die Terminologie

Das von uns allen begrüßte Berufsgeheimnisschutzgesetz beruht in seiner Vorgeschichte auf zwei Handlungssträngen und zwei Entwürfen, die dann zusammengeführt wurden: einerseits der strafrechtlichen und strafprozessualen Regelung,

11 SV-Materialien 11/2017.

12 Eine einheitliche Meinung über das Verständnis von erforderlichen organisatorischen und technischen Maßnahmen gibt es im Datenschutzrecht wohl noch nicht. BeckOK BORA/Römermann/Praß BORA § 2 Rn. 36.

13 BeckOK DatenschutzR/Paulus DS-GVO Art. 32 Rn. 4–9.

wer alles und unter welchen Umständen strafrechtlichen Sanktionen unterliegt (§ 203 StGB) und wie er sich durch prozessuale Gegenrechte vor dem Vorwurf rechtswidriger Offenbarung schützen kann (§§ 53a, 97 StPO); andererseits den berufsrechtlichen Regelungen, in welchem Umfang und unter welchen Voraussetzungen ein Rechtsanwalt (und andere Vertrauensberufe) bei seiner Berufsausübung Dritte, insb. Dienstleister, einschalten darf (§§ 43a Abs. 2, 43e BRAO).

Das Berufsgeheimnisschutzgesetz fand unterschiedliche berufsrechtliche Regelungen vor, ein Zeichen der Zersplitterung des Berufsrechts der Vertrauensberufe aufgrund unterschiedlicher Organisation in den einzelnen Berufen und unterschiedlicher Arbeitsweisen. Es hat dann eine neue Terminologie geschaffen, es gibt Dienstleister, mitwirkende Personen und Gehilfen. Aber die Regelungen wurden nicht insgesamt für die Vertrauensberufe vereinheitlicht, nur harmonisiert. Unterschiedliche Formulierungen laden natürlich dazu ein, unterschiedliche Gestaltungen zu wählen und unterschiedliche Interpretationen für richtig zu halten.

Der Ausschuss hatte Anlass, über diese Problematik nachzudenken aufgrund eines Praxishinweises der Wirtschaftsprüferkammer (WPK) zur Mitwirkung Dritter in der Berufsausübung. Dieser Stellungnahme lag die Frage zu Grunde, ob jeder, der nicht in der Sphäre des Wirtschaftsprüfers arbeite, Dienstleister sein müsse mit der Folge, dass nach § 50a WPO der Mandant einwilligen müsse. Die WPK sieht als mitwirkende Personen gemäß § 50 WPO neben angestellten Mitarbeitern auch freie Mitarbeiter an, die sich in der Sphäre des Berufsträgers befinden und insbesondere auch der Verschwiegenheitspflicht unterliegen. Ein Mitarbeiter befindet sich nach diesem Modell in der Sphäre des Berufsträgers, wenn er im Hinblick auf die vom WP getroffenen Maßnahmen zum Schutz des Mandatsgeheimnisses organisatorisch, insbesondere in das Qualitätssicherungssystem der WP-Praxis, integriert ist, und zwar unabhängig von der Frage, wie das Rechtsverhältnis zum Mitarbeiter zu qualifizieren ist.

Dieser Grundgedanke ließe sich auf §§ 43a, 43e BRAO übertragen und berührt eine bereits vor dem Berufsgeheimnisschutzgesetz bestehende Unklarheit. Dem Gedanken des Geheimnisschutzes trägt der Praxishinweis Rechnung. Ob die Lösung sich durchsetzt, wird man noch sehen.

Der Ausschuss hält das Thema für wichtig, weil die Rechtsanwaltschaft als Berufsstand ein Interesse daran hat, gerade die Neuregelungen aufgrund des Berufsgeheimnisschutzgesetzes gleichlaufend mit den anderen Vertrauensberufen zu interpretieren. Wir wollen eine Zersplitterung vermeiden. Das sollte ein Grundprinzip auch künftiger Arbeit in der Satzungsversammlung sein.

6.2 Die Verpflichtung von Mitarbeiten zur Vertraulichkeit

Die Verpflichtung muss schriftlich erfolgen, während bei Dienstleistern die Textform genügt, § 43e BRAO. Allerdings lässt sich § 43a Abs. 2 S. 3 BRAO nicht entnehmen, dass die Textform ausgeschlossen sein soll (vgl. § 126 Abs. 3 BGB). Hier könnte Klärungsbedarf bestehen.

6.3 Risiken bei der Mandatsanbahnung

6.3.1

Im Rahmen der Mandatsanbahnung sind Fälle vorstellbar, in denen der angefragte Rechtsanwalt sich vor der Mandatsannahme bei anderen Rechtsanwälten und/oder deren beziehungsweise gemeinsamen Mitarbeitern vergewissern muss, dass er nicht verhindert ist. Das gilt insbesondere für Bürogemeinschaften, deren Existenz den potentiellen Mandanten nicht bekannt sein muss. Zwar kann man die Auffassung vertreten, dass die Nachfrage bei den anderen Bürogemeinschaftern kein Verstoß gegen die Vertraulichkeit ist, weil der Rechtsanwalt vorrangig rechtlich verpflichtet ist, rechtliche (nicht wirtschaftliche) Konflikte im Vorfeld auszuschließen. Das kann er nur durch Rückfrage bei den anderen Mitgliedern der Bürogemeinschaft. Jedoch wurde im Ausschuss die Meinung vertreten, dass der angefragte Rechtsanwalt den potenziellen Mandanten vor seiner internen Rückfrage informieren muss, dass diese erfolgen wird. Dem potenziellen Mandanten soll die Möglichkeit eingeräumt werden, seinen Beratungsbedarf insgesamt geheim zu halten, auch wenn dann der anfragende Rechtsanwalt das Mandat ohne die dann verweigerte Rückfrage nicht annehmen kann.

6.3.2

Der Ausschuss hat sich weiter mit dem Inhalt von Aussagen befasst, mit denen Rechtsanwälte nach außen auf ihre Sachkunde unter Verweis auf bereits durchgeführte Beratungen oder Verfahren verweisen. Derartige Aussagen können, abhängig von ihrem Wortlaut, gegen das Gebot der Verschwiegenheit verstoßen. Primär wurde der Komplex unter dem Gesichtspunkt der Werbung behandelt und war daher auch nach Kenntnis des Ausschusses 6 Gegenstand von Beratungen des Ausschusses 2, den der Ausschuss 6 insoweit für federführend hält.

6.4 Organisation von Besprechungen

Durch Fehler kann der Umstand für Dritte ersichtlich werden, dass eine bestimmte Person rechtlichen Beratungsbedarf hat und deswegen Kontakt zu einem Rechtsanwalt gesucht hat. Auch wenn diese Information in vielen Fällen keinen Neuigkeitswert hat und jedenfalls nicht überraschend ist, weil nach der Art ihrer beruflichen oder sonstigen Tätigkeit die Einschaltung von Rechtsanwälten allgemein erwartet wird, ist diese konkrete Information geschützt. Überlegungen zur Risikoadäquanz und Zumutbarkeit von Gegenmaßnahmen sind hier von besonderer Bedeutung. Zum Beispiel kann der Rechtsanwalt leicht zu vermeiden suchen, dass bei Besprechungen in Hotelräumen auf den Reservierungsschildern Mandantennamen genannt werden. Er kann sein Personal anweisen, in seiner eigenen Kanzlei die Mandanten möglichst rasch in Besprechungsräume zu bringen und bei der Terminierung dafür zu sorgen, dass sie sich nicht in einem Wartebereich treffen. Die Anforderungen an die Räumlichkeiten dürfen aber nicht überzogen werden und das gelegentliche Begegnen von Mandanten auf dem Flur wird sich nicht vermeiden lassen.

6.5 Telefonate

Der Rechtsanwalt muss dafür Sorge tragen, dass Telefongespräche mit Mandanten nicht von anderen innerhalb oder außerhalb der Kanzlei auch ohne technische Hilfsmittel mitgehört werden können. Das gilt für von ihm selbst geführte Telefongespräche, zum Beispiel während Besprechungen mit Dritten, in der Öffentlichkeit, bei Reisen, etc., aber auch für von seinem Personal geführte, zum Beispiel in der Telefonzentrale und bei der Telefonvermittlung.

6.6 Aktenbearbeitung, -verwahrung und -vernichtung

6.6.1

Bei der Bearbeitung der Akten besteht das Risiko der Einsicht durch unbefugte Dritte. Daher sind sie in Bearbeitungspausen und über Nacht sicher zu verschließen. Bei Tätigkeit auf Reisen ist eine Einsicht ebenfalls auszuschließen, etwa durch Nutzung einer Sichtschutzfolie auf dem Bildschirm des Laptops. Bei Tätigkeit von Handwerkern, externen Reinigungskräften etc. ist eine Überwachung sicherzustellen, insbesondere bei Nachtarbeit oder am Wochenende.

6.6.2

Die Verwahrung in Aktenschränken darf nicht zur Offenlegung der Parteien oder des Gegenstands durch die Beschriftung der Aktendeckel und deren Einsichtbarkeit durch Besucher führen.

6.6.3

Das Kopieren/Scannen von Akten sowie ihre Vernichtung muss durch eigenes Personal oder Dienstleister unter Beachtung des § 43e BRAO erfolgen.

6.7 Weitere Aspekte

Das IDW hat inzwischen eine Publikation „Hilfestellung zur Beauftragung von Dienstleistern" veröffentlicht, die auf den Seiten der BRAK abgerufen werden kann. Sie befasst sich mit einzelnen Risikosituationen und enthält auch für Rechtsanwälte interessante Hinweise.

7. Einzelne Pflichten und Risiken – allgemeine Büroorganisation unter Heranziehung von Dienstleistern

7.1 Ausgangspunkt Organisationsfreiheit

Der Rechtsanwalt ist in seiner Entscheidung frei, ob er alle betrieblichen Abläufe ausschließlich mit eigenem Personal durchführt oder inwieweit er Dritte einschaltet. Dies ergibt sich aus § 43e Abs. 1 BRAO, der inhaltlich voraussetzt, dass der Rechtsanwalt über die Inanspruchnahme der Dienstleistung eines Dienstleisters entschieden hat. Hat sich der Rechtsanwalt für die Zusammenarbeit mit einem Dienstleister entschieden, hat er allerdings die erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, § 2 Abs. 4 BORA, und deren Wahrung sicherzustellen.

7.2 Überprüfungshandlungen und Pflicht zur Vertragsbeendigung

§ 2 Abs. 6 BORA a.F. lautete: „Der Rechtsanwalt darf Personen und Unternehmen zur Mitarbeit im Mandat oder zu sonstigen Dienstleistungen nicht hinzuziehen, wenn ihm Umstände bekannt sind, aus denen sich konkrete Zweifel an dem mit Blick auf die Verschwiegenheitspflicht erforderlichen Zuverlässigkeit ergeben oder nach Überprüfung verbleiben."

Diese Formulierung hat die 6. Satzungsversammlung gestrichen, da § 43e Abs. 2 Satz 1 BRAO ausdrücklich die Verpflichtung zur sorgfältigen Auswahl vorgesehen hat. Die Norm könnte als weiter als § 2 Abs. 6 BORA a.F. verstanden werden, wenngleich die 5. Satzungsversammlung den Wortlaut sicher nicht eng interpretiert hat.

Wann eine Überprüfungspflicht eingreift und wie sie ausgestaltet sein muss, ist bisher nicht geregelt. Eine entsprechende Formulierung wurde aus dem Referentenentwurf nichts ins Gesetz übernommen. Hier könnte künftig Regulierungsbedarf entstehen.

§ 43e Abs. 2 Satz 2 statuiert keine aktive Überprüfungspflicht nach Erteilung des Auftrages. Es genügt, wenn der Rechtsanwalt der Auffassung ist, dass die Beachtung der Vorgaben im Sinne des § 43e gewährleistet ist. Daraus folgen wohl als Minimum die vertragliche Einräumung eines Prüfungsrechts und eine Prüfungspflicht, wenn dem Rechtsanwalt Indizien bekannt werden, aus denen sich eine Gefährdung der Vertraulichkeit ergeben könnte. Unter Beachtung des Risikoprofils der Mandanten oder der Mandate und des Zuschnitts der Praxis im Allgemeinen kann es aber auch bedeuten, dass der Rechtsanwalt regelmäßig und nicht nur akzidentiell darüber zu entscheiden hat, ob seine zu einem früheren Zeitpunkt getroffene Auswahl des Dienstleisters nach wie vor eine tragfähige Grundlage hat. In jedem Fall ist es empfehlenswert, diese Überlegung und die Begründung ihres Ergebnisses zu dokumentieren.

7.3 Domizildienstleister

Der Ausschuss hat sich mit Risiken befasst, die aus der Nutzung des Angebots von Domizildienstleistern folgen. Als Vorfrage hat er Bedenken geprüft, nach denen diese Organisationsform von vorneherein unzulässig wäre, weil es sich um Bürogemeinschaften der dort betreuten Rechtsanwälte handelte, bei denen die (wenigen) auf Bürogemeinschaften anwendbaren Regelungen nicht beachtet würden. Der Ausschuss hält diese Bedenken für unangebracht, weil es bei dieser Konstellation an einer gemeinschaftlichen Nutzung der Ressourcen des Domizilanbieters fehlt, vielmehr eine parallele Nutzung der Ressourcen auf der Grundlage separat bestehender schuldrechtlicher Verträge vorliegt.

Diese Organisationsentscheidung des Rechtsanwalts ist nach § 43e BRAO nicht angreifbar, wenn die sonstigen Vorgaben der Norm beachtet werden. Dazu gehört auch die Beachtung der organisatorischen und technischen Maßnahmen, die der Rechtsanwalt zu beachten hätte, wenn er die Kanzlei selbst unterhalten würde. Sie muss der Rechtsanwalt vereinbaren, auch ein Prüfungsrecht, vgl. 7.2.

8. Einzelne Pflichten und Risiken – elektronische Kommunikation

Der Ausschuss hat sich in fast jeder Sitzung mit dem Thema der elektronischen Kommunikation befasst. Dies zeigt die Bedeutung des Themas, das sicher künftige Satzungsversammlungen nicht weniger beschäftigen wird.

8.1 Ursache sind die verschiedenen Spannungsfelder, in denen es liegt:

(i) Soweit nicht der Schutz der Vertraulichkeit und des Mandats- geheimnisses Vorrang hat, stehen Berufsrecht und Datenschutzrecht im Prinzip nebeneinander und gelten voneinander unabhängig. Anwaltliches Verhalten kann aber zugleich gegen Datenschutzrecht und gegen Berufsrecht verstoßen, vgl. 4.

(ii) Die technischen Möglichkeiten der elektronischen Kommunikation, ihre spezifischen Risiken und Schutzmöglichkeiten sind in laufender Entwicklung und ändern sich rasch. Jede spezielle Regulierung birgt daher die Gefahr in sich, schnell veraltet und überholungsbedürftig zu sein. Das

spricht gegen sie, andererseits sollte eine weite Regulierung wohl nicht Kommunikationsmethoden „absegnen", über die kein übergreifender Konsens besteht.
(iii) Das Verständnis, wann eine Kommunikationsform zulässig sein sollte, ist bei den relevanten Gruppen (etwa Rechtsanwälten und Mandanten) nicht annähernd deckungsgleich. Mandanten können Risiken subjektiv anders bewerten und deshalb andere, geringere Anforderungen an das Schutzniveau haben. Hier stellt sich die Fragen, inwieweit die Regulierung dem Rechnung tragen kann oder muss, und darüber hinaus, wie alltagstauglich eine Regulierung sein muss, um nicht schlicht von den – ihr nicht unterworfenen – Mandanten unterlaufen zu werden.

All diese Fragen werden nicht einmal für immer entschieden werden können, sondern bedürfen des regelmäßigen Austarierens der Antworten mit der möglichen Folge der Überarbeitung des § 2 BORA. Der Ausschuss hat sich gegen Ende der Berichtsperiode die Frage gestellt, sie aber offengelassen, ob eine eigene Norm, etwa ein § 2 a BORA, geschaffen werden sollte, die sich ausschließlich mit der elektronischen Kommunikation befasst. Dies würde den (unzutreffenden) Eindruck vermeiden, die Grundprinzipien des § 2 BORA wären keine Konstante anwaltlicher Tätigkeit.

8.2 Elektronische Kommunikation, insbesondere Verschlüsselung bei E-Mailverkehr

In der Sitzungsperiode hat die Diskussion der erforderlichen Verschlüsselung eine besondere Intensität gewonnen. Mit diesem Thema hat sich der Ausschuss in mehreren Sitzungen und das Plenum in zwei Sitzungen befasst. Zunächst soll die technische Begrifflichkeit geklärt werden-

8.2.1 E-Mail: Transportverschlüsselung

Jede E-Mail wird, in Datenpaketen und meist über unterschiedliche Verbindungen, vom Ausgangspunkt zum Zielserver transportiert. Dabei passiert sie zahlreiche Server und kann dort mitgelesenen werden. Daher wurden diverse Methoden (Protokolle) zur Verschlüsselung auf diesem Weg entwickelt, von denen viele schon wieder überholt sind. Stark vereinfachend wird bei der Transportverschlüsselung die versendete Botschaft gleichsam durch einen Tunnel gesendet, der beim Versender anfängt und beim Empfänger endet. Wenn diese Art der Verschlüsselung richtig gemacht wird, kann die versendete Botschaft nicht bei den zahlreichen Stationen im Tunnel mitgelesen werden.

8.2.2 E-Mail: Ende-zu-Ende Verschlüsselung

Einen absoluten Schutz gibt es aber nicht, daher besteht das Bestreben, immer höhere Sicherheit zu bewirken. Die weitere Form der Verschlüsselung besteht darin, dass der Inhalt, also die Botschaft selbst, erst verschlüsselt wird, bevor sie auf den Weg geschickt wird (sogenannten Inhaltsverschlüsselung). Hier hat der Empfänger den Schlüssel, um den Inhalt dieser Botschaft dann bei sich selbst zu entschlüsseln. Bei dieser Art der Inhaltsverschlüsselung kommt es also gar nicht darauf an, ob jemand anderes die Botschaft unterwegs kopieren kann, weil er sie noch entschlüsseln müsste. Bei anspruchsvoller Verschlüsselung ist diese Aufgabe kaum zu erledigen. Das ist die Ende-zu-Ende-Verschlüsselung. In der Literatur[14] wird die Ende-zu-Ende-Verschlüsselung mehrheitlich nicht als datenschutzrechtliches Gebot angesehen. Landesdatenschutzbeauftragte[15] sehen das zum Teil anders. Bei der Transportverschlüsselung sieht die Lage schon anders aus. Hier gibt es sehr viele Stimmen, die in unterbliebener Transportverschlüsselung einen Verstoß gegen Datenschutzrecht sehen. Auch einige Landesdatenschutzbeauftragte haben sich in diesem Sinne geäußert, und die unterschiedlichen Auffassungen führten zu einem Austausch und der Antwort des Präsidenten der Hanseatischen Rechtsanwaltskammer Dr. Lemke auf die Auffassung des Hanseatischen Datenschutzbeauftragten. Herr Dr. Lemke zeigte auf, dass die datenschutzrechtliche Betrachtung keinesfalls zu so klaren Ergebnissen führt, wie behauptet. Eine Einzelfallbetrachtung sei erforderlich, datenschutzrechtlich und nach § 2 Abs. 4 BORA. Verschlüsselung könne nicht als Mindeststandard verlangt werden, unverschlüsselte Kommunikation sei sozialadäquat und mangels konkreter Gefährdung die Verschlüsselung eine unzulässige Belastung. Diese – stark verkürzte – Antwort muss ernst genommen werden und sie zeigt, dass man datenschutzrechtlich bisher nicht davon ausgehen kann, dass Transportverschlüsselung geboten ist.[16]

8.2.3 Anforderungen an den Rechtsanwalt und Verhalten des Mandanten

Der Rechtsanwalt hat die Risikolage seiner Kanzlei und der jeweiligen Mandanten im Sinne von § 2 Abs. 4 BORA zu überdenken und gegebenenfalls dem Mandanten die Ende-zu-Ende-Verschlüsselung vorzuschlagen. Wünscht der Mandant sie von sich aus, muss man dem nachkommen. Wenn sich der Rechtsanwalt dazu nicht in der Lage sieht, darf er das Mandat erst gar nicht annehmen oder muss es beenden.

Der Rechtsanwalt kann zwar die Transportverschlüsselung einschalten oder eine Ende-zu-Ende Verschlüsselung anbieten, beides funktioniert aber nur, wenn der Empfänger technisch darauf eingerichtet ist. Ist er das im Fall der Transportverschlüsselung nicht, wird unverschlüsselt gesendet. Viele Mandanten werden genau das wollen. Wie aber ist die Situation der Kollegen, die dann wie gehabt weiter über E-Mail kommunizieren? Der Ausschuss sieht es als wichtiges Ziel an, hier Rechtssicherheit zu schaffen. Bei E-Mail handelt es sich allerdings um eine Kommunikationsart, die technisch von vielen bereits als überholt angesehen wird. Der Ausschuss hält eine isolierte Regelung nicht für sinnvoll und sieht das Spektrum des Regelungsbedarfs weiter. Es erstreckt sich auf elektronische Kommunikation und sonstige Kommunikationsformen. Da diese Überlegungen mit der Fertigstellung des Berichts parallel liefen, wird insoweit auf das Protokoll und Material der Sitzung der Satzungsversammlung vom 6. Mai 2019 verwiesen.

8.3 Social Media

Der Ausschuss hatte wegen einer Anfrage Veranlassung, sich mit der Nutzung von Social Media, Messenger Services und Kommunikationsplattformen durch Rechtsanwälte zu befassen. Im Vordergrund standen dabei Verletzungen der Vertraulichkeit durch den Datenhunger mancher Apps, die vom Nutzer nicht kontrollierbar gespeicherte Kontaktdaten von Personen kopieren und verteilen, auch soweit diese nicht in

14 *Schöttle*, BRAK-Mitt. 2018, 124 https://www.brak.de/.

15 *Schöttle*, BRAK-Mitt. 2018, 124 https://www.brak.de/ aus S. Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27.3.2014, www.bfdi.bund.de/ und Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, 138, www.saechsdsb.de/.

16 Seither haben weitere Datenschutzbeauftragte der Länder Stellung genommen und sich für die Ende-zu- Ende Verschlüsselung ausgesprochen.

die Kommunikation eingebunden sind. Manche dieser Medien bieten sogar eine Ende-zu-Ende Verschlüsselung und sind aus dem Gesichtspunkt der Verschlüsselung nicht zu beanstanden. Der Ausschuss hat es wegen der Schnelllebigkeit der technischen Entwicklung nicht für zweckmäßig gehalten, derartige Programme zu identifizieren und individuell berufsrechtlich von der Nutzung auszuschließen oder zuzulassen.

Er verwies jedoch auf die Pflichten aus § 2 Abs. 4 BORA. Danach ist der Rechtsanwalt verpflichtet, diese Offenlegung seiner Daten zu verhindern und gefährdende Programme allenfalls auf einem zweiten, privaten Smartphone (oder in einem softwaremäßig verlässlich getrennten Bereich seines Endgeräts) zu nutzen, nicht aber beruflich.

Hinter dieser Überlegung steht die Wertung, dass der Mandant zwar Herr des Geheimnisse ist, soweit im weitesten Sinne sein Mandat betroffen ist. Jenseits dieses Bereiches bleibt aber die Pflichtigkeit aus § 2 Abs. 4 BORA zum aktiven Schutz der Vertraulichkeit unberührt.

8.4 Cloud-Computing

8.4.1 Begriff

Cloud-Computing bezeichnet aus Sicht des Nutzers die Inanspruchnahme von IT-Dienstleistungen, die ein Dienstleister auf Servern bereitstellt, über die der Nutzer nicht die Sachherrschaft hat. Die angebotenen Dienstleistungen umfassen hierbei die komplette Bandbreite der Informationstechnik wie unter anderem Infrastruktur, Plattformen und Software. Man kann hierbei grob zwischen einer Public Cloud (Services werden der Allgemeinheit oder einer größeren Gruppe zur Verfügung gestellt) und einer Private Cloud (die Cloud wird ausschließlich für eine Organisation betrieben) unterscheiden.[17]

8.4.2 Zulässigkeit und Selbstverantwortung des Auftraggebers

(a) Die Nutzung von Cloudlösungen ist aufgrund der Reform durch das Berufsgeheimnisschutzgesetz unter Beachtung der Maßgaben der §§ 203 StGB, 43a und 43e BRAO, des § 2 BORA und der einschlägigen Regelungen des Datenschutzrechts zulässig.
(b) Der Ausschuss hat mit dem BSI Gespräche über Cloud-Lösungen, ihre Risiken und Gegenmaßnahmen geführt. Die Satzungsversammlung hat sich durch einen Vertreter des BSI unmittelbar über diese Themen unterrichten lassen. Der Ausschuss hat sich ausführlich mit dem BSI-Papier C 5 und dessen Konzept der Eigenverantwortung befasst und hält es für sinnvoll.
(c) Der Ausschuss hat keinen Versuch einer eigenständigen Regulierung von Cloud-Nutzungen unternommen und hält ihn angesichts der raschen technischen Entwicklungen und der umfassenden gesetzlichen Regelungen nicht für geboten. Die Satzungsversammlung hat Kompetenz nur zur Konkretisierung. Einen entsprechenden Bedarf oder Spielraum hat der Ausschuss nicht gesehen.
(d) Weiterführende Hinweise finden sich auf diversen Webseiten der berufsständischen Organisationen, Kammern und insbesondere der BRAK.[18]

Anlage 5.3.2

Einzelne Anforderungen bei der Nutzung von Technik und Informations- und Kommunikationstechnologie (IKT)

Die nachstehenden Formulierungen geben Überlegungen und Erkenntnisse des Ausschusses 6 aus seiner Befassung mit dem Papier C 5 des BSI wieder. Sie diente dem Ausschuss dazu, ein besseres Verständnis für die eigenen Aufgaben und die praktische Umsetzung zu gewinnen. Die Feststellungen des Ausschusses sind nicht umfassend und waren nicht zur laufenden Aktualisierung gedacht. Inzwischen sind auf den Websites der BRAK, des DAV und einzelner RAK einschlägige Empfehlungen veröffentlicht worden.

1. Die Pflege der eingesetzten Programme

Der Datenschutz fordert im Rahmen der technischen und organisatorischen Maßnahmen, dass die Datenverarbeitung sicher erfolgt. Sicherheit bedeutet zunächst, dass vorhandene Programme gepflegt werden.

1.1 Updates

Es gibt praktisch keine Software, die von ihrem Hersteller nach Erwerb in dem Zustand belassen wird, zu dem sie lizensiert wurde. Dem Erwerb derartiger Software, soweit sie überhaupt noch vorhanden ist, muss der Rechtsanwalt kritisch gegenüberstehen. Üblich ist es stattdessen, dass im laufenden Betrieb zu Tage tretende Fehler und Sicherheitslücken behoben werden, die für Angriffe durch Dritte ausgenutzt werden oder sie ermöglichen. Hierbei handelt es sich um Updates, die vom Hersteller in regelmäßigen oder unregelmäßigen Zeitpunkten zur Verfügung gestellt werden. Wenn ein Computer vom Netz genommen ist und *stand-alone* eingesetzt wird, was nur in seltenen Fällen eine realistische Annahme sein dürfte, ist es erforderlich, diese Updates aus Sicherheitsgründen unverzüglich herunterzuladen und zu installieren, am besten automatisch. Updates werden für einen erheblichen Zeitraum nach erstmaliger Lizensierung zur Verfügung gestellt, und solange nichts Gegenteiliges bekannt wird, kann der Rechtsanwalt davon ausgehen, dass das so gepflegte Programm „sicher“ ist.

1.2 Versionswechsel

Die Hersteller der Standardprogramme liefern aber nicht nur Updates, sondern sie sehen in unregelmäßigen Zeitabständen auch neue Versionen des Standardprogramms vor. Diese Versionen sind erhältlich, während die früheren Versionen noch durch Updates gepflegt werden. Z.B. sind derzeit noch Updates für Windows 7 erhältlich, obwohl Windows 10 seit einiger Zeit auf dem Markt ist. Ob ein Versionswechsel aus operativen Gründen sinnvoll ist, soll hier nicht weiter erörtert werden. Generell gilt aber nach Überzeugung des Ausschusses 6, dass ein Versionswechsel nicht berufs- oder datenschutzrechtlich erforderlich, solange die frühere Version noch über Updates gepflegt wird und der Einschätzung der Sicherheit keine konkreten Informationen entgegenstehen.

17 https://bsi.bund.de/.
18 https://www.brak.de/; https://www.brak.de/

2. Die Absicherung des eigenen Rechners

Sicherheit der Datenverarbeitung bedeutet, dass der Datenbestand und die Prozesse vor Angriffen Dritter zu schützen sind. Dazu gehören nicht nur die Pflege der eingesetzten Programme (vgl. 9.1), sondern auch der Einsatz von speziellen Programmen.

2.1 Virenschutz

Üblich und geboten sind zunächst Programme, die die Infiltration des Computers oder des Computersystems durch Viren und Trojaner verhindern sollen. Zu ihrer Pflege gelten wiederum die Ausführungen zu 8.1.

2.2 Firewall

Angriffe durch Dritte erfolgen nicht nur durch die Platzierung von Viren, sondern sie können auch durch die nichtbestimmungsgemäße Nutzung der Software („Hacken“) erfolgen, mit der Folge, dass auf dem Computer gespeicherte Daten manipuliert oder auf andere Systeme kopiert werden können. Virenschutzprogramme bieten hiergegen keinen Schutz. Deswegen ist es üblich und geboten, auch spezielle Programme zu nutzen, die eine „Firewall“ gegen derartige Eindringversuche Dritter schaffen sollen.

2.3 Import von Daten über Schnittstellen

Externe Speicher werden meist über USB Anschlüsse mit dem Rechner verbunden. Hier besteht das Risiko, dass die Daten an der Firewall vorbei importiert werden und bei falscher Konfiguration auch die Virenprüfung zu spät erfolgt, nämlich nachdem der Rechner bereits infiziert wurde.

2.4 Verhinderung des ungewollten Exports von Daten

Je neuer das Betriebssystem, desto umfangreichere Daten werden nach der vorgegebenen Standardeinstellung oft ohne weitere Rückfrage an den Hersteller des Programms (oder der dort gebündelten Programmkomponenten) übermittelt. Des Risikos für die Vertraulichkeit sollte sich der Rechtsanwalt bewusst sein und die Einstellungen der Software entsprechend ändern (lassen).

2.5 Verschlüsselung von Daten auf der Festplatte

Bei mobilen Endgeräten einschließlich Laptops, USB-Sticks und anderen Speichermedien besteht das Risiko des Abhandenkommens. Für diesen Fall müssen die darauf befindlichen Daten geschützt sein. Der normale Passwortschutz zum Anmelden bei einem Laptop genügt nicht, da die Festplatte ausgebaut und dann von einem anderen Gerät ausgelesen werden kann. Das lässt sich mit der Verschlüsselung des Speichermediums insgesamt, also nicht nur einzelner Dateien, verhindern.

2.6 Nutzung von WLAN

WLAN-Netze sind allgemein üblich und ihre Nutzung (durch Mitarbeiter und Mandanten) wird von vielen Mandanten als selbstverständlich angesehen. Sie sind aber auch ein Einfallstor für Hacker. Professionelle Unterstützung bei der Auswahl der Hardware und Konfiguration der Software einschließlich Verschlüsselung ist geboten.

2.7 Voice-over-IP

Die festnetzbasierte Telefonie wird systematisch abgeschafft und die Teilnehmer werden zur Nutzung von Voice-over-IP gezwungen. Dadurch entstehen weitere Gefährdungen der Vertraulichkeit. Praktische Wege, sich der Änderung der technischen Rahmenbedingungen zu entziehen, gibt es für den Rechtsanwalt nicht. Ihm ist anzuraten, sich bei der Anschaffung und Konfiguration der Anlage von Fachleuten beraten zu lassen.

2.8 Weitere Aspekte

Die vorgenannten Programme und Maßnahmen sind das Minimum, das erwartet werden kann. Wiederum gilt, dass der Anwalt das Risikoprofil seiner Mandanten und der von ihm bearbeiteten Mandate zu bewerten hat. Stellt er eine besondere Gefährdungslage fest, können über den Standard hinausgehende Sicherungs- maßnahmen geboten und zumutbar sein. Das ist dann bei der Architektur seines IT-Systems zu bedenken. Dabei kann sich der Anwalt sachkundiger Beratung bei der Gestaltung und Implementierung der Systeme bedienen. Externer Rat ist im Regelfall empfehlenswert, um sich im Falle eines erfolgreichen Einbruchs in den Datenbestand gegen den Vorwurf leichtfertigen Verhaltens abzusichern.

3. Die Sicherung der Daten

Datensicherung umfasst „alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.“[19] Aufgrund von technischem Versagen oder fehlerhafter Handhabung können gespeicherte Daten verloren gehen oder unbrauchbar werden. Durch eine angemessene Datensicherung soll sichergestellt werden, dass der Verlust von Datenbeständen verhindert wird. Das BSI hat im Rahmen der Publikation zum IT-Grundschutz[20] Umsetzungshinweise zur Datensicherung veröffentlicht. Dazu zählt zunächst die sorgfältige Auswahl einer geeigneten Sicherungssoftware sowie die Unterrichtung der Mitarbeiter zur Datensicherung. Die regelmäßige Erstellung von Sicherungskopien und die geeignete Dokumentation der Datensicherungen sind ebenso wichtig wie die geeignete Lagerung der Backup-Datenträger und die regelmäßige Prüfung der Wiederherstellbarkeit der Daten.[21] Auch die Sicherstellung der Betriebskontinuität zur konsistenten Einhaltung des Betriebsplans wird zur Beurteilung der Informationssicherheit miteinbezogen.[22]

Prof. Dr. Thomas Gasteyer, Frankfurt am Main

Der Autor war Vorsitzender des Ausschusses 6 der 6. Satzungsversammlung. Die 6. Satzungsversammlung war bis Ende Juni 2019 im Amt.

Leserreaktionen an anwaltsblatt@anwaltverein.de.

19 https://www.bsi.bund.de/.

20 Vgl. Fußnote 19:

21 BSI. (o.D.). Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept. Abgerufen von https://www.bsi.bund.de/.

22 BSI. (2017, September).Anforderungskatalog Cloud Computing (C5). Abgerufen von https://www.bsi.bund.de/.