Anwaltsrecht

§ 2 BORA – Schutz des Mandatsgeheimnisses als Handlungspflicht

Konkretisierung der Berufspflicht tritt am 1. Januar 2018 in Kraft – Tipps

Rechtsanwalt Prof. Dr. Thomas Gasteyer, Frankfurt am Main

„Der Anwalt ist zur Verschwiegenheit verpflichtet." Der Berufspflicht des § 43 Abs. 2 Satz 1 BRAO wird durch bloßes Schweigen schon lange nicht mehr genügt. Das Mandatsgeheimnisses müssen Anwälte und Anwälte heute auch aktiv schützen. Die Satzungsversammlung hat daher den § 2 BORA (seit 1. Juli 2015 in Kraft) neu geregelt, um das Outsourcing in Kanzleien zu erfassen (siehe dazu AnwBl 2015, 70 und AnwBl 2015, M 132, seit 19. November 2017 auch in der BRAO geregelt: Grupp, AnwBl 2017, 816). Jetzt zum 1. Januar 2018 tritt mit dem neuen § 2 Abs. 7 BORA eine Handlungspflicht in Kraft. Was Anwältinnen und Anwälte zum Schutz des Mandatsgeheimnisses aktiv leisten müssen, erläutert der Autor.

I. Der neue § 2 Abs. 7 BORA

Am 19. Mai 2017 hat die Satzungsversammlung § 2 BORA um einen neuen Absatz 7 ergänzt (so dass der bisherige § 2 Abs. 7 BORA[1] nun Abs. 8 wird):

> „Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Rechtsanwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit des Datenschutzrechts dessen Anforderungen entsprechen; sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen. Abs. 3 lit. c) bleibt hiervon unberührt."

Verschwiegenheit wird bei uns oft mit der wohl selbstverständlichen Verpflichtung des Rechtsanwalts gleichgesetzt, selbst keine vertraulichen Daten preiszugeben. Allenfalls sieht man in ihr noch ein Abwehrrecht gegenüber staatlichen Eingriffen, die der Vertraulichkeit durch Abhören und Datensammeln die Basis entziehen. Dieses Verständnis ist zu eng. Der Rat der Europäischen Anwaltschaften (CCBE) hat bereits unmissverständlich die Verpflichtung des Rechtsanwalts postuliert, Datenschutz und Datensicherheit aktiv herzustellen, vgl. CCBE Recommendation on the protection of client confidentiality within the context of surveillance activities und CCBE Guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance[2].

Dem hat sich jetzt die Satzungsversammlung angeschlossen. Beides, Datenschutz und Datensicherheit sind Grundlagen des Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant. Die Absicherung dieses Vertrauensverhältnisses ist Sache des Rechtsanwalts. Parallel zu der Pflichtenlage im Datenschutz (vgl. § 9 BDSG), gebietet es die berufsrechtliche Verschwiegenheitspflicht dem Rechtsanwalt, die dazu erforderlichen und angemessenen organisatorischen und technischen Schutzvorkehrungen zu treffen.

II. Das Gebot zum Schutz des Mandatsgeheimnisses

1. Reichweite

Dieses Gebot bezieht sich nicht nur auf Daten in elektronischer Form, sondern auch auf Daten auf konventionellen Datenträgern, zum Beispiel Papierakten und Diktierbändern. Dass man Schriftstücke nicht beliebig herumliegen lässt, wenn fremde Personen sie sehen, ist uns vertraut. Ebenso vertraut, aber oft nicht beachtet, ist der Schutz dieser Informationen, wenn wir im Zug mit Mandanten oder Kollegen telefonieren oder Korrekturen zu Schriftsätzen durchgeben. Dort sieht man häufig geöffnete Bildschirme, die keinen Leseschutz bieten, obwohl die Nutzung einer Privacy-Folie einfach und effizient wäre.

Dass elektronische Daten ebenfalls zu schützen sind, ist für die Rechtsanwaltschaft ebenfalls nichts Neues. Nur geht uns die Umsetzung dieses Postulats noch nicht wie selbst von der Hand. Das Spektrum möglicher organisatorischer Maßnahmen ist weit. Es reicht von der bereits erwähnten Nutzung von Privacy-Folien über Sicherungsmaßnahmen gegen Hackerangriffe und Einschleusung von Viren und Trojanern, die Verschlüsselung von E-Mail-Verkehr und Datenübermittlung bis hin zu intern und extern gestaffelten Zugangsberechtigungen zu digitalen Datenbeständen.

Manch ein Rechtsanwalt mag sich bei der Beurteilung erforderlicher Maßnahmen schwertun und auf Leitlinien seitens der Berufs-/Standesorganisationen oder der Rechtsanwaltskammern hoffen. Wegen der raschen Entwicklung der im Markt verfügbaren Produkte und Techniken und dem daraus folgenden permanenten Änderungsbedarf jeder bewertenden Marktübersicht (falls sie wettbewerbsrechtlich überhaupt zulässig wäre), ist das aber keine realistische Erwartung. Wir bewegen uns hier auf einem Gebiet, auf dem wir alle – mit wohl nur wenigen Ausnahmen – schnell dazulernen müssen; das aber nicht wegen geänderten Berufsrechts, sondern aufgrund der Anforderungen der Mandanten und des Marktes. Sie erwarten zu Recht, dass der Rechtsanwalt moderne Bürotechnik beherrscht, effizient arbeitet und seine Standards nicht hinter denen des Datenschutzes hinterherhinken.

2. Umsetzung

Grundsätzlich gilt: Der Rechtsanwalt hat die umzusetzenden Maßnahmen konkret für seine Kanzlei festzulegen. Deren Auswahl muss sich an der Risikoadäquanz und am Datenschutzrecht orientieren. Soweit die Anforderungen des Datenschutzrechts zu beachten sind, gelten berufsrechtlich keine schärferen. Risikoadäquanz verlangt die Bewertung des Risikos, des bei Verletzung zu erwartenden Schadens für den Mandanten sowie die Auswahl von Schutzmaßnahmen einschließlich der Analyse ihrer Verfügbarkeit und des dafür erforderlichen Aufwands. Auch die konkrete Bedeutung der Ge-

1 Sein Wortlaut: „Die Bestimmungen des Datenschutzrechts zum Schutz personenbezogener Daten bleiben unberührt." (ab 1. Januar 2018 nun § 2 Abs. 8 BORA).

2 Vgl. CCBE Recommendation on the protection of client confidentiality within the context of surveillance activities und CCBE Guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance, http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf

heimhaltung der anvertrauten Informationen ist zu bedenken sowie die Wahrscheinlichkeit, dass es zufällig oder durch gezieltes Ausspionieren zur unbefugten Kenntnisnahme durch Dritte kommt.

Wer laufend börsennotierte Gesellschaften im Hinblick auf ad-hoc pflichtige Sachverhalte berät oder als Strafverteidiger in Fällen von hohem Interesse für die Öffentlichkeit auftritt, mag eher ein Ziel von Wirtschaftsspionage werden als

> „Die Frage der Systemabsicherung ist also nicht abstrakt, sondern konkret für die jeweilige Kanzlei und ihren Zuschnitt zu beantworten."

ein Spezialist für die Abwicklung von Verkehrsunfällen. Beide müssen ihre Systeme absichern, aber nicht auf identische Weise. Die Frage ist also nicht abstrakt, sondern konkret für die jeweilige Kanzlei und ihren Zuschnitt (Mandate und Mandantschaft) zu beantworten. Kein Rechtsanwalt muss also alles Verfügbare implementieren, sehr wohl aber Risiken und Möglichkeiten bedenken und seine Entscheidung für bestimmte Schutzmaßnahmen dann umsetzen.

In diesem Artikel soll nicht der Versuch unternommen werden, ein Schutzkonzept zu erarbeiten. Ein marktübliches Programm zum Schutz gegen Viren und Trojaner sowie eine Firewall darf jedoch jeder Mandant erwarten. Was man hat, muss man auf Stand halten und regelmäßig empfohlene Updates einspielen. Problematisch ist die Nutzung von Programmen, für die wegen ihres Alters keine Sicherheitsupdates mehr zur Verfügung stehen. Organisatorisch muss sich der Rechtsanwalt überlegen, welcher Personenkreis die Daten ansehen darf. Nicht jeder Vorgang muss von jedem Mitarbeiter einsehbar sein. Bei hochsensiblen Vorgängen ist über gestaffelte Zugangsberechtigungen nachzudenken.

Die eigenen Festlegungen sollten regelmäßig und anlassbedingt überdacht werden. Kommt es etwa durch die Fortentwicklung digitaler Kommunikationsformen oder andere Innovationen zu zusätzlichen neuen Risiken, muss man diese bestmöglich verhindern. Der Stand der Technik ist zu wahren. Auch hier gilt wieder, dass nicht alles ungeprüft angeschafft und implementiert werden muss, was neu auf den Markt kommt, es sei denn ein festgestelltes Risiko wurde bisher nicht adäquat berücksichtigt.

3. Verhältnismäßigkeit/Sozialadäquanz

Eine Maßnahme ist jedoch nur erforderlich, wenn sie dem Rechtsanwalt auch zumutbar ist. Der verfassungsrechtlich vorgegebene Verhältnismäßigkeitsgrundsatz schließt die wirtschaftliche Vertretbarkeit ein. Bei der Bestimmung der Zumutbarkeitsschwelle ist allerdings nicht darauf abzustellen, was dem einzelnen Rechtsanwalt zumutbar erscheint. Technophobie oder mangelnder Investitionswille dürfen nicht zur Schädigung des Mandanten führen. Anzulegen ist ein objektiver Maßstab, der berufstypische Spezifika berücksichtigt. Die dafür beispielhafte Frage lautet: „Ist es einem Rechtsanwalt (statt: dem Rechtsanwalt N.N.) zumutbar, für sein Computersystem eine Firewall einzuführen?"

Aus Satz 3 des neuen Abs. 7 folgt, dass ein in Abs. 3 lit. c) beschriebener Arbeitsablauf, der somit „objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)" nach wie vor keinen berufsrechtlichen Verstoß gegen das Verschwiegenheitsgebot begründet. Auch insoweit sollen künftig also keine unverhältnismäßigen Maßnahmen verlangt werden. Die systematische Unterlassung der Pflege der eigenen Systeme wird man jedoch nicht als „von der Allgemeinheit gebilligte Verhaltensweise" ansehen können.

III. Fazit: Konkretisierung bestehender Anforderungen

Der neue § 2 Abs. 7 BORA wurde in Kenntnis der Reformvorschläge des Geheimschutzgesetzes beschlossen. Dessen Inkrafttreten lässt ihn unberührt, während § 2 BORA im Übrigen von der Satzungsversammlung überprüft wird.[3] § 2 Abs. 7 BORA konkretisiert als Berufspflicht Anforderungen, die inhaltlich bereits in ähnlicher Form oder Formulierung aufgrund anderer Normen bestehen. Das Mandatsgeheimnis ist für Mandanten die Grundlage, sich ihrem Rechtsanwalt anzuvertrauen und deswegen von höchster Bedeutung. Es entspricht nicht dem Selbstverständnis der Anwaltschaft – die Position der CCBE ist eindeutig –, dass ihre Standards sich auf den für alle geltenden Datenschutz beschränken. Aus diesen Gründen ist die aktives Handeln erfordernde Regelung im neuen Abs. 7 zur Stärkung des Schutzes der Vertraulichkeit geboten.

Prof. Dr. Thomas Gasteyer, Frankfurt am Main

Der Autor ist Rechtsanwalt. Er ist Mitglied der Satzungsversammlung und dort Vorsitzender des Ausschusses 6 „Verschwiegenheitspflicht und Datenschutz".

Leserreaktionen an anwaltsblatt@anwaltverein.de.

3 Z. B. verlangt § 2 Abs. 4 und 5 die Schriftform während der höherrangige § 43e Abs. 3 BRAO bei Dienstleistern die Textform genügen lässt..