THE LEGAL®EVOLUTIONARY

Elektronische Kommunikation im Dschungel von Berufsrecht und Datenschutz

Moderne Kommunikationsformen und die Sicherstellung der Vertraulichkeit

Prof. Dr. Thomas Gasteyer | Knowledge Partner Germany | Clifford Chance
Eva Säljemar | Continuous Improvement Project Manager | Clifford Chance

27. November 2019

LR 2019, Seiten 211 bis 218 (insgesamt 8 Seiten)

Moderne Kommunikationsformen verbreiten und entwickeln sich rasch. E-Mail-Kommunikation beispielsweise wird von einigen bereits als überholt angesehen. Unsicherheit besteht insbesondere bezüglich der Frage, mit welchen technischen und organisatorischen Maßnahmen die Vertraulichkeit sichergestellt werden kann, stellt sie doch die Basis anwaltlicher Tätigkeit dar. An Regulierung mangelt es nicht. Die nachfolgenden Ausführungen geben einen Überblick über das Normengefüge und die Handlungsspielräume der Berufsgeheimnisträger. 1

I. Normengeflecht

Das Verhalten im anwaltlichen Berufsalltag unterliegt einer Vielzahl von Regelungen aus unterschiedlichen Rechtsgebieten. Allen ist gemeinsam, dass sie unmittelbar oder mittelbar die Vertraulichkeit absichern wollen. Allerdings stehen hinter den Normen jeweils unterschiedliche Schutzzwecke. 2

Zu beachten sind

- §§ 203, 204 Strafgesetzbuch (StGB),
- §§ 43a und 43e Bundesrechtsanwaltsordnung (BRAO),
- § 2 Berufsordnung für Rechtsanwälte (BORA)[1],
- die Datenschutzgrundverordnung (DSGVO),
- das Bundesdatenschutzgesetz (BDSG),
- das Geschäftsgeheimnisschutzgesetz (GeschGehG)

[1] Die Erläuterungen beziehen sich auf die ab dem 1.1.2020 gültige Fassung.

- und, oft vergessen, §§ 280 und 826 Abs. 2 Bürgerliches Gesetzbuch (BGB).

Das Berufsgeheimnisschutzgesetz machte Ende 2017 im Wege einer grundlegenden Reform die Einbeziehung von Outsourcing-Dienstleistern, z.B. Cloud-Services, in die Kanzleiabläufe rechtssicher und änderte sowohl die strafrechtlichen als auch die berufsrechtlichen Regelungen. Das gilt insbesondere für das Non-Legal Outsourcing, geht aber weit darüber hinaus. Die Aufnahme "sonstiger mitwirkender Personen" ist die wichtigste Anpassung am Kreis der Personen, mit denen Rechtsanwälte "das Geheimnis" teilen dürfen. Denn dies erlaubt es Anwälten, Dienstleistern die Kenntnisnahme geschützter Informationen zu ermöglichen und nicht nur "Gehilfen" und anderen sie unmittelbar unterstützenden Personen. § 43e Abs. 2 BRAO wurde um entsprechende Sorgfaltsanforderungen für die Einbeziehung von externen Dienstanbietern erweitert. Die in Textform erforderliche Zustimmung des Dienstleisters zur Geheimhaltungspflicht nach strafrechtlicher Belehrung stellt eine zusätzliche Erleichterung dar, um den Bedürfnissen der Berufspraxis Rechnung zu tragen. 3

Nicht offensichtlich sind allerdings die Wechselbeziehungen der Normen. Alle aufgeführten formellen Gesetze, also die durch das Berufsgeheimnisschutzgesetz abgeänderten und die neu geschaffenen § 203 StGB, §§ 43a und 43e BRAO, § 280 BGB, die DSGVO sowie das BDSG, haben Vorrang gegenüber der BORA (und damit gegenüber dem neugefassten § 2 Abs. 2 Satz 5 und Satz 6 BORA – dazu im Folgenden mehr). Denn als Satzungsrecht tritt die BORA hinter formellen Gesetzen zurück. 4

Sind die Voraussetzungen für die Einschaltung Dritter nach der BRAO gewahrt, ist eine Verletzung des § 203 StGB ausgeschlossen, da der Rechtsanwalt nicht mehr "unbefugt" handelt. Nicht jeder Verstoß gegen diese Anforderungen der BRAO beseitigt diese strafrechtliche Berechtigung. Andererseits bewahrt die Beachtung des Strafrechts nicht vor einer Verletzung des Berufsrechts. Mit die größten Unsicherheiten bestehen bei der Anwendung des Datenschutzrechts. Das Geschäftsgeheimnisschutzgesetz ist noch zu neu, als dass es schon durch Entscheidungen spezifiziert wäre. Die Definition der Schutzwürdigkeit des Geschäftsgeheimnisses deckt sich hier nicht mit dem Schutzzweck des § 203 StGB. Daher dürften beide getrennt zu beurteilen sein. Kumulativ kommen außerdem noch die Pflichten aus dem Anwaltsvertrag hinzu, also nach BGB. 5

II. § 2 Abs. 2 BORA

Das Mandatsgeheimnis bildet für Mandanten die Grundlage, sich ihrem Rechtsanwalt anzuvertrauen. Es wird nicht nur durch die Beschlagnahmeverbote und Zeugnisverweigerungsrechte sowie die Schweigepflicht abgesichert. § 2 Abs. 2 BORA sieht vielmehr eine aktive Handlungspflicht des Rechtsanwalts vor. Eine Schutzpflicht besteht auch als Nebenpflicht aus dem Anwaltsvertrag und dürfte inhaltlich bei den zu ergreifenden Maßnahmen zu denselben Ergebnissen führen. 6

So lange sie risikoadäquat zum Anwaltsberuf sind, verpflichten die Normen den Anwalt dazu, organisatorische und technische Maßnahmen zu ergreifen, die für die Wahrung des Mandatsgeheimnisses erforderlich sind. Das bedeutet, dass Maßnahmen als ausreichend angesehen werden, sofern sie dem nach der DSGVO erforderlichen Schutzniveau entsprechen. Relevant ist insbesondere Art. 32 DSGVO. Damit soll eine Doppelbelastung des Rechtsanwalts verhindert werden. Technische Maßnahmen müssen darüber hinaus dem Stand der Technik nach § 2 Abs. 2 BORA entsprechen. Ihre Implementierung setzt voraus, dass der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. 7

III. Anforderungen nach der DSGVO

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 lit. f) DSGVO in einer Weise verarbeitet werden, "die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‘Integrität und Vertraulichkeit')". Bei der Entscheidung können und sollen gemäß Art. 32 DSGVO unter anderem der Stand der Technik, die Implementierungskosten und der laufende Aufwand sowie Art, Umfang, Umstände und Eintrittswahrscheinlichkeit sowie die Schwere der Folgen berücksichtigt werden (vgl. auch § 2 Abs. 2 BORA). Diese Vorgaben wirken auf den ersten Blick klar und eindeutig, sind es in der Umsetzung aber nicht wirklich, weil bei den Begriffen ein Beurteilungsspielraum besteht. 8

Als mögliche technische und organisatorische Maßnahmen werden die Pseudonymisierung in Art. 32 DSGVO, Erwägungsgrund 78 und die Verschlüsselung in Erwägungsgrund 83 zur DSGVO genannt. Weitere Maßnahmen ergeben sich aus der Anlage zum früheren § 9 BDSG und beinhalten beispielsweise die Zutritts-, Zugang- und Zugriffskontrolle. 9

IV. Verhältnis von Berufsrecht und Datenschutzrecht

Die Vorschriften der DSGVO und des BDSG sind auch auf Rechtsanwälte anwendbar, soweit sie nicht vom strafrechtlichen Schutz der Verschwiegenheit und entsprechendem Berufsrecht verdrängt werden, vgl. § 29 BDSG. Die DSGVO und das Berufsrecht stehen nebeneinander, decken sich aber nicht in allen Punkten. Das führt zu Schwierigkeiten – nicht nur im materiellen Recht, sondern auch hinsichtlich Zuständigkeitsfragen. 10

Das Anwaltsgericht Berlin vertrat im Frühjahr 2018 die Auffassung, dass ein Verstoß gegen die Regelungen der DSGVO zugleich einen zu ahndenden Verstoß gegen die Generalklausel des § 43 BRAO darstelle. Die strikte Beachtung der datenschutzrechtlichen 11

Regelungen gehöre zum Kernbereich anwaltlicher Pflichten.[2] Dagegen hat die 6. Satzungsversammlung die Meinung vertreten, dass ein Verstoß gegen die Generalklausel des § 43 BRAO als Auffangtatbestand voraussetzt, dass die Verletzung einer nicht spezifisch berufsrechtlichen Norm einen berufsrechtlichen Überhang aufweist. Dieser etablierte Grundsatz gilt auch bei möglichen Verstößen gegen den Datenschutz. Die Besonderheiten unverschlüsselter Kommunikation sind nunmehr in § 2 Abs. 2 BORA idF ab 01.01.2020 geregelt, sodass keine Regelungslücke mehr besteht und die Anwendbarkeit des § 43 BRAO entfällt.

V. Arten und Wirkung der Verschlüsselung bei elektronischer Kommunikation

Hinsichtlich der Verschlüsselung elektronischer Kommunikation ist zwischen *Data in Motion* und *Data at Rest* zu differenzieren: Bei *Data in Motion* werden Daten über E-Mails oder Webverbindungen von einem Speicher zum nächsten bewegt, während sie bei *Data at Rest* auf einem geeigneten Medium gespeichert sind und als solche nicht bewegt werden. 12

Bezüglich der Verschlüsselung selbst ist zwischen Transportverschlüsselung (Ende zu Ende Verschlüsselung) und Inhaltsverschlüsselung zu unterscheiden. Transportverschlüsselung betrifft nur *Data in Motion*. Die Daten werden wie durch einen Tunnel gesendet und damit durch die Transportverschlüsselung nach derzeitigem Stand der Technik vor einem Zugriff geschützt. Allerdings besteht hier das theoretische Risiko gezielter Angriffe, die mit einigem technischem Aufwand verbunden sind. Das gilt insbesondere am Ende des Transportweges, wenn die Daten in ein anderes geschütztes Medium übertragen werden oder auf dem Weg, bei der Durchleitung durch Server. Die technische Absicherung wurde aber immer besser, sodass eine Bewertung der Vergangenheit nicht in jedem Fall gültig ist. Bei *Data in Motion* ist die Verschlüsselung über Transport Layer Security (kurz TLS) der gängige Standard. Hier wird durch die Prüfung von Zertifikaten zunächst die Echtheit und Aktualität der Schlüssel sichergestellt und im Anschluss die Verbindung mit der Ziel-Webseite verschlüsselt. Viele Nutzer sind sich nicht bewusst und auch die Diskussion in der Öffentlichkeit verdrängt den Umstand, dass die meisten Provider bereits standardmäßig eine Transportverschlüsselung vorsehen. 13

Die Inhaltsverschlüsselung betrifft die Daten selbst, nicht das Medium auf oder in dem sie sich befinden. Sie ist sowohl bei *Data at Rest* als auch bei *Data in Motion* anwendbar – bei Letzterem werden die Daten vor der Übertragung verschlüsselt. Bei der Inhaltsverschlüsselung wird allgemein ein lesbarer Text in einen nicht lesbaren, geheimen Text überführt, sodass die Informationen nur verfügbar sind, wenn der Leser den passenden Schlüssel hat. Die Meta-Informationen wie Absender, Empfänger und Betreff sind nicht verschlüsselt, aber durch die Transportverschlüsselung geschützt. Als rechtlich relevanter Unterschied sind bei der Inhaltsverschlüsselung die entstandenen Daten 14

[2] Vgl. *AnwG Berlin*, Beschluss vom 5.3.2018 - 1 AnwG 34/16, BeckRS 2018, 11237;

andere als die geheimnisgeschützten Daten, sodass jedenfalls § 43e BRAO und § 203 StGB nicht auf sie anwendbar sind.

VI. Schlüsselverwaltung

Der Unterschied zwischen *Data in Motion* und *Data at Rest* wurde kurz angerissen, ebenso die entsprechenden Sicherheitsmaßnahmen für *Data in Motion*. Aber wie sieht es mit *Data at Rest* aus? Wie können Daten sicher verschlüsselt werden und wo werden die Schlüssel aufbewahrt? Insgesamt gibt es drei verschiedene Verschlüsselungsmethoden, wenn es um *Data at Rest* geht: 15

- Server-Side Encryption (server held keys): Verschlüsselung, bei der die Schlüssel auf dem Server gespeichert sind und der Serviceanbieter die Schlüssel verwaltet. 16
- Server-Side Encryption (client held keys): Die Schlüssel werden auf dem Client gehalten, aber auf dem Server verschlüsselt.
- Client-Side Encryption: Bei der clientseitigen Verschlüsselung werden eigene Verschlüsselungscodes erstellt und verwaltet. Es müssen eigene Tools zum Verschlüsseln von Daten verwendet werden, bevor die Daten an Clouddienstanbieter gesendet werden. Der Clouddienstanbieter hat keine Kenntnis von den Schlüsseln, die zur Verschlüsselung verwendet wurden.

Bei der Entscheidung für eine dieser Methoden ist das Sicherheitsniveau zu berücksichtigen, welches für die gegebenen Daten erforderlich ist sowie der entstehende Aufwand. Wenn es darum geht, Daten in der Cloud zu speichern, schafft die clientseitige Verschlüsselung eine für Dritte unzugängliche Umgebung und erhöht damit die Sicherheit erheblich. Wie kommt es also, dass die clientseitige Verschlüsselung nicht die Standardmethode ist? Unter Berücksichtigung des Kosten-Nutzen-Verhältnisses erscheint ihr Einsatz nicht immer effizient, da ein hohes Maß an Computerleistung erforderlich ist. Außerdem muss evaluiert werden, ob die eigenen Systeme ein Sicherheitslevel sicherstellen können, das vergleichbar mit dem eines global agierenden Dienstanbieters ist. Die Folgen eines Schlüsselverlusts wären immens, wenn nicht existenzbedrohend. War die Implementierung und Pflege dieser Verschlüsselungsmethode bisher eher aufwändig, gibt es mittlerweile mehrere Anbieter solcher Technologien. 17

VII. Umsetzungsthemen / Praktisches Dilemma

Die Einigung zwischen Rechtanwalt und Mandant über die Art der Kommunikation wird sich nicht immer an den Erfordernissen des Rechtsanwalts ausrichten können. In so einem Fall kann sich der Rechtsanwalt dem Vorwurf ausgesetzt sehen, unzulässige Kommunikationswege zu nutzen. Dieser Unsicherheit soll die Neuregelung in § 2 Abs. 2 Satz 5 und Satz 6 BORA idF ab 01.01.2020 entgegenwirken und berufsrechtliche Sicherheit 18

schaffen. Nach § 2 Abs. 2 Satz 5 BORA ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges zwischen Rechtsanwalt und Mandant, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, dann erlaubt, wenn der Mandant zustimmt. Von einer Zustimmung ist nach Maßgabe von § 2 Abs. 2 Satz 6 BORA auszugehen, wenn der Mandant den Kommunikationsweg vorschlägt oder beginnt und fortsetzt, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat. Die datenschutzrechtliche Beurteilung ist offen, weil das Konzept des Mandanten als Herr des Geheimnisses im Datenschutz nicht durchgängig anerkannt ist. Insoweit verbleiben Unklarheit und Risiken.

VIII. Datenverarbeitung im Ausland – Vergleichbares Schutzniveau?

Nach § 43e Abs. 4 BRAO ist die Inanspruchnahme von Dienstleistungen aus einem anderen Land durch einen Rechtsanwalt zulässig, wenn für die Geheimnisse ein vergleichbares Schutzniveau besteht. 19

1. Die Prüfung der Lage im Ausland

Erfolgt die Leistung aus einem Mitgliedstaat der EU, wird nach der Gesetzesbegründung der Berufsgeheimnisschutzgesetze unterstellt, dass dieses Schutzniveau gleichwertig ist. 20

Bei Leistungen außerhalb der EU ist es notwendig zu prüfen, ob das Geheimhaltungsniveau mit dem nationalen Niveau vergleichbar ist. Da die rechtlichen Regelungen in Deutschland singulär sind, kommt es nicht auf identische Gesetze an, sondern auf die Existenz von Schutzmechanismen (funktionales Schutzniveau). Im Einzelnen sind die Anforderungen interpretationsfähig und unklar. Erfasst der Begriff "vergleichbar" die gegebenenfalls vertraglich vereinbarte Geheimhaltungspflicht des Dienstleisters oder den Ausschluss der potentiellen Kenntnisnahme durch strafrechtliche oder andere Behörden? Jedenfalls ist eine komplexe Bewertung der Rechtslage im jeweiligen Land erforderlich, mit hohem Aufwand für den Bezieher der Dienstleistung. Die vorsorgliche Zustimmung des Mandanten kann einfacher einzuholen sein, hilft aber nicht, wenn die Dienstleistung Teil der Infrastruktur ist. Dann müssten alle Mandanten zustimmen, was sich als wenig praktikabel darstellt. 21

Der Rechtsanwalt darf ohne Zustimmung des Mandanten ausländische Dienstleistungen in Anspruch nehmen, wenn ein vergleichbares Schutzniveau nicht festgestellt ist, die Beurteilung des Falles aber ergibt, dass ein solches Schutzniveau nicht erforderlich ist. Ein Beispiel ist die Auslagerung von Daten für Wartungszwecke, da während dieser kurzen Zeitspanne und der Verwendung von Inhaltsverschlüsselung keine Probleme entstehen sollten, beispielsweise die Beschlagnahme der Daten von ausländischen Behörden. 22

2. Maßstab: Das deutsche Schutzniveau

Die Übermittlung von Daten an ausländische Behörden findet auch nach dem in Deutschland anwendbaren Recht statt. Die öffentliche Diskussion fokussiert sich in diesem Zusammenhang auf die Lage im Ausland. Allerdings sind die Feststellung und die Bewertung des inländischen Rechts als Vergleichsmaßstab ebenso wichtig. Dazu sollen zwei Beispiele für künftige Entwicklungen genannt werden: 23

Die EU hat im Herbst 2018 die E-Evidence Verordnung initiiert, die die Übermittlung von Daten ohne Einschaltung eines inländischen Gerichts als Freigabeinstanz vorsieht. Die E-Evidence Richtlinie soll die Zusammenarbeit beschleunigen, die aufgrund von zeitintensiven Mutual Legal Assistance Treaties (kurz MLATs) oftmals nicht zielführend sind. Die E-Evidence Richtlinie weckt dennoch viel Widerspruch. So hat sich der Deutsche Anwaltsverein kritisch gegenüber dem Gesetzesentwurf geäußert und die Klarstellung der Regelungen verlangt. In welcher Form sie auch immer in Kraft treten wird, man muss sie in Zukunft als Teil des Vergleichsmaßstabs für ausländische Rechtssysteme berücksichtigen. 24

Darüber hinaus ist die EU mit einem Verwaltungsabkommen auf Grundlage des US Cloud Acts befasst. Gegenstand ist auch hier die Übermittlung von Daten ins Ausland, ohne dass ein Gericht im Ursprungsland der Daten zustimmen muss. Aufgrund dieses Abkommens darf allerdings der ersuchende ausländische Richter die Geheimhaltungsinteressen im Ursprungsland berücksichtigen. Insoweit ist die richterliche Prüfung eröffnet, allerdings die im anderen Land. Großbritannien beabsichtigt anscheinend einen bilateralen Abschluss einer derartigen Vereinbarung, die dem Parlament in London und dem Kongress in Washington D.C. inzwischen zur Erwägung vorliegen soll. 25

Eine vergleichbare Anforderung ergibt sich daneben aus dem Datenschutzrecht. Auch hier muss der Rechtsanwalt prüfen, ob ein vergleichbares Schutzniveau herrscht und falls nicht, angemessene Maßnahmen ergreifen (z.B. Standarddatenschutzklauseln mit einem Dienstleister abschließen). 26

IX. Fazit

Die Absicherung der elektronischen Kommunikation unterliegt Regelungen aus verschiedenen Rechtsgebieten, insbesondere dem Berufsrecht und dem Datenschutzrecht. Für eine Absicherung ist das Zusammenwirken beider Seiten erforderlich. Das ist bislang aber nicht in jedem Fall sichergestellt. § 2 BORA idF ab 01.01.2020 gewährt in berufsrechtlicher Hinsicht einen "sicheren Hafen". 27

Der Bezug von Dienstleistungen aus dem Ausland ist möglich, allerdings sind die Anforderungen an den Rechtsanwalt und insbesondere die Prüfungs- und implizierten Dokumentationslasten für den Rechtsanwalt immens. 28

Die Würdigung berufsrechtlich unbedenklicher Vorgänge unter datenschutzrechtlichen Aspekten kann abweichen. Rechtsanwälte und andere Berufsgeheimnisträger sollten sich über die Auffassungen der für sie zuständigen Datenschutzaufsichtsbehörden informieren und sie nicht ignorieren. 29