ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

11/2017

Die Zulässigkeit der Anwalts-Cloud nach der Neuordnung des Berufsrechts

Lesedauer: 8 Minuten

In der ZD 2017, 201 hat der renommierte Datenschutzrechtler *Eugen Ehmann* einen nachdenklich stimmenden, innovativen Gastkommentar zu der Neuordnung des Paragrafen 203 StGB, insbesondere im Gesundheitsbereich, abgegeben. Seine These ist einfach: Erstaunlicherweise schaffe dieses neue Gesetz keine ausdrückliche gesetzliche Rechtsgrundlage für die Übermittlung von Patientendaten an externe Dienstleister. Zumindest sei das Strafbarkeitsrisiko nach Art. 83 DS-GVO in Form von Geldbußen brisant.

Es möge offenbleiben, ob Ärzte wie Anwälte durch § 203 Abs. 1 und 3 StGB bei der Nutzung externer Dienstleister privilegiert sind. Auch ist auf Art. 90 DS-GVO verwiesen, der den Mitgliedstaaten die Verabschiedung spezifischer Regeln für Geheimnisträger erlaubt und diese von der Reichweite der Verordnung ausnimmt. Auf jeden Fall lohnt sich der Blick auf die Anwälte im neuen Gesetz, insbesondere was die Änderung der BRAO angeht. Denn hier hat sich nahezu unbemerkt Wichtiges getan.

Professor Dr. Thomas Hoeren ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster und Mitherausgeber der ZD.

Das Gesetzespaket zur Neugestaltung des § 203 StGB hat nämlich auch noch Änderungen im anwaltlichen Berufsrecht mit sich gebracht. § 43e BRAO n.F. legt die Grenzen und Möglichkeiten für die Einbindung externer Dienstleister ohne Einwilligung der berechtigten Person für Anwälte fest. Sind die Voraussetzungen dieser Vorschrift eingehalten, stellt die Einbindung externer Dienstleister keinen Verstoß gegen die anwaltliche Verschwiegenheitspflicht dar. Doch betrachtet man die Regelungen unter der Anwendung moderner IT-Lösungen im Anwaltsbetrieb, lassen sich hier einige Überlegungen anstellen, die die Regelung nicht mehr ganz so klar erscheinen lassen:

- Als besonderes Problem erweist sich § 43 Abs. 5 BRAO. Hiernach kann der Anwalt bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, dem Dienstleister Zugang zu Geheimnissen nur dann ermöglichen, wenn der Mandant darin spezifisch eingewilligt hat. Ausdrücklich spricht die Begründung des Gesetzes von Dienstleistungen, wie etwa der Beauftragung eines Sachverständigen, eines Detektivs oder eines Übersetzers (BT-Drs. 18/11936, S. 36). Die Reichweite der Vorschrift geht allerdings sehr viel weiter: Unter Daten, die „unmittelbar einem einzelnen Mandat zugeordnet sind", sind ebenfalls alle Abrechnungsdaten zu zählen, d.h. auch bereits die einzelne Honorarleistung. Allein im Rahmen einer Fernwartung fallen schon eine Fülle von Daten an, die aus einem konkreten Beratungsverhältnis stammen (können). Bereits die Angabe einer Scheidung als Abrechnungsart für ein Honorar kann dabei den Einwilligungszwang auslösen. Lediglich Pauschalhonorare ohne konkreten Verwendungszweck bedürfen keiner Einwilligung bei der externen Abrechnung. Damit unterliegt der Bereich der Honorarabrechnung nahezu vollständig der Einwilligung bei der Einbindung externer Dienstleister.

- Merkwürdig ist eine weitere Formulierung in der Begründung, wonach es für die Prüfung des unmittelbaren Mandatsbezugs nicht auf die konkrete Vertragsgestaltung ankomme. Entscheidend sei vielmehr die Frage, „ob für die jeweilige Dienstleistung, die in Anspruch genommen werden soll, ein besonderer Bedarf im einzelnen Mandat besteht" (BT-Drs. 18/11936, S. 36). Damit ergibt sich aus der Gesetzesbegründung selbst eine Art nicht kontrollierte Öffnungsklausel, die die Sache dabei gleichsam noch schwieriger gestaltet. Darüber hinaus muss jetzt auch noch geklärt werden, ob die externe Einbindung von Dienstleistern von einem besonderen Bedarf im Einzelfall gedeckt ist.

- Das Einwilligungserfordernis wird vor allem wegen der hohen Anforderungen an die Einwilligung ebenfalls als problematisch angesehen. Nach § 43e Abs. 6 BRAO gelten im Falle der Einwilligung besondere Bestimmtheitserfordernisse: Der Mandant muss ausdrücklich auch auf die Anforderungen des § 43e Abs. 2-4 BRAO verzichten. Aus der Sicht des externen Dienstleisters ergibt sich daraus eine schwierige Vertragskonstellation: Allgemein braucht er zunächst mit dem Anwalt eine Vereinbarung in Textform, auf Grund derer er zur spezifischen Geheimhaltung verpflichtet ist (§ 43e Abs. 3 BRAO). Für die Daten, die unmittelbar einem Mandat dienen, braucht er ferner eine ausdrückliche, individuelle Einwilligung des Mandanten.

- Als wäre dies nicht genug, findet sich in § 43e Abs. 8 BRAO noch der lapidare Zusatz „die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt". Damit ist das von *Ehmann* beschriebene Dilemma von Strafrecht und dem widersprechenden Datenschutzrecht nicht bei Ärzten akut, sondern durch die Öffnung in § 43e BRAO nur und ausschließlich für Anwälte. Denn diese sind trotz der Freistellung ihrer exter-

nen Cloud im Datenschutzrecht an die Datenschutzgrundverordnung gebunden. Vor allem trifft sie das Risiko einer Geldbuße gem. Art. 83 Abs. 4 und 5 DS-GVO hart. Wegen der Einbindung externer Dienstleister müsste der Anwalt vor allem Art. 28 DS-GVO und die dortigen Anforderungen an eine Auftragsdatenverarbeitung beachten. Losgelöst davon stellt bereits die BRAO Minimalanforderungen für die Auftragsdatenverarbeitung auf (Gesetzesbegründung in BT-Drs. 18/11936, S. 37). Man könnte zwar die These vertreten, dass damit der Verweis in § 43e Abs. 8 BRAO leerläuft und dass Art. 90 DS-GVO die Datenschutzgrundverordnung für Geheimnisträger nicht für anwendbar erklärt. Dann würde die BRAO auf ein Datenschutzrecht verweisen, das seinerseits auf Geheimnisträger nicht anwendbar ist. Dies kann von der Vorschrift aber nicht gemeint sein. Man wird daher zumindest vertreten können, dass das Datenschutzrecht und das Strafrecht parallel nebeneinander existieren, zumindest wenn es um Anwälte geht.

- Und schließlich bleibt noch das ewige Problem des internationalen Datenschutzrechts. § 43e BRAO verlangt von den Anwälten eine Prüfung, ob die Datenspeicherung in Drittstaaten den europäischen Standards gleichsteht. Sie belastet damit aber die anwaltliche Zunft mit einem enormen Prüfungsrisiko, da jetzt der einzelne Anwalt bei jedem Vorgang mit Datenschutzbezug vorab zu prüfen hat, ob sein Dienstleister die europäischen Datenschutzanforderungen entsprechend in seinem Heimatland beachtet. Wer sich mit den Finessen des US-Rechts an dieser Stelle beschäftigt, kommt dann gleich in die Schwierigkeit, ob und inwieweit man wirklich sagen kann, dass das Datenschutzrecht im Zeitalter von *Trump* den EU-Standards Rechnung trägt. Jedenfalls trägt der Anwalt die volle Sanktionslast, falls die Prüfung von ihm versehentlich falsch läuft.

- Zudem impliziert § 43e BRAO „eine tiefe Verneigung vor der heimischen IT- und TK-Wirtschaft" (so *Härting,* in: LTO, abrufbar unter: https://www.lto.de/recht/job-karriere/j/stgb-203-anwalt-mandant-verschwiegenheit-berufsrecht/2/). Denn vor der Beauftragung auch eines auswärtigen europäischen Dienstleisters muss der Anwalt im Einzelfall prüfen, ob der im Ausland bestehende Datenschutz „dem Schutz im Inland vergleichbar ist". Dies ist europarechtlich problematisch, da es IT-Dienstleister aus anderen EU-Mitgliedstaaten ohne sachlichen Grund diskriminiert. Es entspricht auch nicht dem Geist der DS-GVO, die den europäischen Datenraum einheitlich mit einem Rechtsrahmen für den Datenschutz ausstatten will.

- Angedacht wurde ferner, dass die Prüfung des auswärtigen Rechts für den Anwalt entbehrlich ist, wenn eine solche Prüfung mit dem Wesen des Geheimnisses unverträglich ist. Auf das einzelne Datenschutzniveau soll es nicht mehr ankommen, wenn dies für die Durchsetzung des Geheimnisschutzes unbedeutend ist. Auch der Hinweis auf eine solche de minimis-Regel ist aber wenig hilfreich, da dadurch der Geheimnisschutz verwässert und auf die Schultern des einzelnen Anwalts verlagert wird.

Der Gesetzesentwurf, der schon den *Bundesrat* passiert hat und der noch im Bundesgesetzblatt zu veröffentlichen ist, ist unausgegoren und gerade für Anwälte problematisch (dazu auch allg. demnächst ausführlich *Hoeren*, MMR 1/2018). Die Anwälte treffen künftig enorme Prüfungsrisiken, wenn sie externe Dienstleister – insbesondere mit der Speicherung von Honorardaten – beauftragen wollen.

Sie müssen schlimmstenfalls zwei verschiedene Abrechnungssysteme fahren und zwei getrennte externe Datenverarbeitungen vorhalten: Zum einen ist da der große Bestand an Anwaltsdaten ohne Mandatsbezug, der nach § 203 StGB bei bestehender Geheimhaltungsverpflichtung auf externe Dienstleister abgewälzt werden kann. Zum anderen wären die wenigen Kerndaten mit unmittelbarem Mandatsbezug, für deren externe Verwaltung die Einwilligung des Mandanten nachzuholen und ggf. zu beweisen wäre. Dies erscheint aber wenig praktikabel.

Fraglich ist, was es dazu an Alternativen gibt: Lässt man einmal das Datenschutzrecht außen vor und betrachtet sich nur die BRAO, drohen dem Anwalt bei Verstoß gegen § 43e BRAO lediglich anwaltsgerichtliche Verfahren, nicht aber strafrechtliche Konsequenzen. Die BRAO ist allerdings nur auf in Deutschland zugelassene Anwälte anwendbar. Ausländische Anwälte brauchen daher die Vorgaben der BRAO gar nicht zu beachten und können z. B. Daten mit Mandatsbezug ohne Einwilligung extern vergeben. Doch dann käme nur eine Flucht ins Ausland in den Blick, was dem in Deutschland niedergelassenen Anwalt wenig hilft.

Letztendlich verbleibt dem Anwalt nur die Verschlüsselung der Daten; denn dann fehlt es am Personenbezug. Dabei reicht eine einfache Verschlüsselung nicht aus, wenn diese allgemein rekonstruierbar ist. In dieser Situation kann ihm kaum ein richtiger Rat bedenkenlos gegeben werden. Es bedarf also einer restriktiven Auslegung des § 43e BRAO oder zumindest einer Feststellung der Anwaltskammern, wonach diese Vorschrift, was den Mandatsbezug angeht, eng auszulegen ist. Nur so wird die Schutznorm zu Gunsten des Mandanten ihrem eigentlichen Sinn zugeführt, nämlich den Schutz des Mandanten bei der Verarbeitung sensibelster Daten durch externe Dienstleister.