Daten-Outsourcing und IT-Compliance bei Berufsgeheimnisträgern
Die Neuregelungen im Umfeld des § 203 StGB

von Prof. Dr. Carsten Momsen und
Wiss. Mit. Laura Iva Savić[*]

Abstract
Mit dem "Gesetz zur Neuregelung des Schutzes von Geheimnissen bei Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen" ist es dem Gesetzgeber gelungen, die berufs- und strafrechtliche Grauzone beim Daten-Outsourcing zu beseitigen. Die Weitergabe von Daten an externe Dienstleister ist nun grundsätzlich von § 203 StGB-E gestattet. Gleichzeitig erweitert sich der Täterkreis um die externen Dienstleister. Zusätzlich hat der Gesetzgeber berufsrechtliche Compliance-Vorschriften festgelegt, die den Ruf nach Entwicklung verbindlicher IT-Sicherheitsstandards lauter werden lassen. Dieser Standards bedarf es in besonderer Weise im Datenverkehr mit ausländischen Anbietern, um unkalkulierbare Strafbarkeitsrisiken auszuschließen. Ferner bleibt abzuwarten, welche weiteren gesetzgeberischen Maßnahmen zur Harmonisierung des § 203 StGB mit §§ 53, 53a StPO folgen.

I. Einführung

§ 203 StGB stellt den Schutz von Geheimnissen, die Angehörigen bestimmter Berufsgruppen (im Folgenden: Berufsgeheimnisträger) im Rahmen ihrer Tätigkeit anvertraut wurden, vor unbefugter Offenbarung sicher. Das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“[1] soll die Norm sowie das mit ihr verbundene Verfahrens- und Berufsordnungsrecht so umgestalten, dass ein Geheimnisschutz auch im Zeitalter des – nicht nur digitalen – Outsourcings verschiedener Hilfstätigkeiten sichergestellt werden kann.

Viele Berufsgeheimnisträger sind bei ihrer beruflichen oder dienstlichen Tätigkeit auf die Einschaltung externer Dienstleister angewiesen, insbesondere in den Bereichen „Einrichtung, Betrieb, Wartung und Anpassung der informationstechnischen Anlagen, Anwendungen und Systeme“[2]. Die Heranziehung Dritter, außerhalb der eigenen Sphäre stehender Personen zu diesen Hilfstätigkeiten, birgt aber auch ein rechtliches Risiko, sofern diese Personen damit von geschützten Geheimnissen Kenntnis erlangen können und keine einschlägige Befugnisnorm oder ausdrückliche Einwilligung des Berechtigten vorhanden ist.[3] Die Berufsgeheimnisträger bewegten sich bisher bei der Beauftragung Dritter in einer berufs- und strafrechtlichen Grauzone.[4] Die Gesetzesänderung schafft diesbezüglich Rechtssicherheit.

Das Gesetz zielt darauf ab, umfänglich praktizierte Formen des Datenoutsourcings mit den Bedürfnissen eines strafrechtlich wirksamen Geheimnisschutzes in Einklang zu bringen. Diese Handhabung erscheint in dem Kontext der fortschreitenden Digitalisierung als sinnvoll. Die Idee, Dienstleistungen auszulagern, steht dabei im Vordergrund. Dabei geht es in dem Gesetz insbesondere um Formen des „Non Legal Outsourcing“, also nicht um die Übertragung von konkreten juristischen Aufgaben auf Dritte („Legal Outsourcing“[5]), sondern um Tätigkeiten wie Aktenvernichtung, Wartungsarbeiten an EDV-Anlagen, Schreib- oder Rechnungsarbeiten. In der Praxis lassen sich Berufsgeheimnisträger bei solchen Arbeiten in der Regel durch externe Dienstleister unterstützen, sei es aus reiner Kostenersparnis und/oder auch aus Qualitäts- und Verfügbarkeitsgesichtspunkten. Alle diese externen Dienstleister kommen gezwungenermaßen mit sensiblen Daten in Berührung,[6] die der – berufsrechtlichen – Verschwiegenheitspflicht unterliegen, und Mandanten ist es häufig nicht bewusst, wer da neben dem Anwalt Kenntnis von all den vertraulichen Informationen erhält.[7]

Entscheidend ist zudem ein Nebeneffekt: Betrachtet man das Zusammenwirken der vom Gesetz umfassten straf- und strafverfahrensrechtlichen sowie berufsausübungs- und berufsordnungsrechtlichen Normen im Zusammenspiel mit der Datenschutzgrundverordnung, so ergeben

---

* Prof. Dr. Carsten Momsen leitet den Arbeitsbereich „Strafrecht, Strafverfahrensrecht, Wirtschafts- und Umweltstrafrecht“ an der Freien Universität Berlin, Laura Savić ist wissenschaftliche Mitarbeiterin am Arbeitsbereich.

1 Am 22.9.2017 hat der Bundesrat den bestehenden Entwurf v. 14.4.2017 (= BT-Drs. 18/11936) gebilligt. Es bedarf lediglich der Gegenzeichnung sowie der Ausfertigung und Verkündung durch den Bundespräsidenten.

2 BT-Drs. 18/11936, S. 1.

3 A.a.O.

4 Vgl. auch *Hartung/Weberstaed,* NJW 2016, 2209.

5 Die Übertragung juristischer mandatsbezogener Tätigkeiten ausschließlich durch Angehörige der rechtsberatenden Berufe oder Unternehmen an externe Dritte, *Hartung/Weberstaed*, NJW 2016, 2209 (2210).

6 *Kargl* nennt als Beispiele einer notgedrungenen Kenntnis von Daten durch Diensteanbieter: Papierstau im Drucker, »eingefrorene« Bildschirme oder den Ausfall eines Servers: StV 2017, 482.

7 *Hartung/Weberstaed*, NJW 2016, 2209.

sich dezidierte und teilweise weitreichende Anforderungen an die IT-Compliance für Berufsgeheimnisträger.

II. Strafrechtliche Perspektive – Strafbarkeitsrisiko

Bezogen auf die Tätigkeit eines Rechtsanwaltes dient § 203 StGB dem Schutz von Mandantengeheimnissen, die der Mandant dem Rechtsanwalt im Rahmen seiner Tätigkeit anvertraut hat. Die in § 203 StGB normierte Schweigepflicht des Rechtsanwalts gehört zum Kernbestand seines Berufsrechts (§ 43a BRAO, § 2 BORA). Möchte der Rechtsanwalt diese Geheimnisse weitergeben, bedarf es zunächst einer Einwilligung durch den Mandanten, auch wenn externe Dienstleister beauftragt werden und im Rahmen der Beauftragung vertrauliche Mandatsgeheimnisse weitergegeben werden müssen. Die Übertragung der Mandatstätigkeit auf den externen Auftraggeber ohne Einverständnis des Mandanten barg derzeit noch das Strafbarkeitsrisiko des § 203 Abs. 1 und 2 S. 1 StGB. Damit konnte das unbefugte Offenbaren eines fremden Geheimnisses, das ihm in bestimmter beruflicher Eigenschaft anvertraut oder sonst bekannt geworden sei, erfüllt sein. Um diesem Strafbarkeitsrisiko entgegenzuwirken, wird bei dem demnächst zu verkündenden Gesetz direkt an der Tathandlung des „Offenbarens“ angesetzt. Nach § 203 Abs. 3 Satz 1 StGB liegt gerade kein „Offenbaren“ vor, wenn bei dem Rechtsanwalt „berufsmäßige Gehilfen oder bei diesem zur Vorbereitung auf den Beruf tätige Personen“ Zugang zu den Geheimnissen bekommen. Externe Dienstleister zählen jedoch nicht dazu, weil sie nicht in den organisatorischen und weisungsgebundenen internen Bereich mit einbezogen sind. Nach § 203 StGB wird ein „Offenbaren“ bei solchen Personen nicht mehr erfüllt sein, die an der beruflichen oder dienstlichen Tätigkeit des Rechtsanwaltes mitwirken (Abs. 3 S. 2), auch wenn das Geheimnis den Kreis der ursprünglich „zur Kenntnis Berufenen“ verlässt. Exemplarisch für solche „mitwirkenden Personen“, die nicht der Sphäre des Berufsträgers zuzuordnen sind, sind bspw. Personen, die auf Seiten eines Cloud-Diensteanbieters mit den Informationen in Kontakt kommen, zu nennen. Dadurch werden externe Dienstleister (Auftragnehmer) als Gehilfen qualifiziert und somit in den (neuen) Kreis der Verpflichteten aufgenommen. Dafür entscheidend ist, dass sie in irgendeiner Art und Weise in die berufliche Tätigkeit eingebunden sein müssen und dazu Beiträge leisten müssen. Eine Eingliederung in die Sphäre des Berufsgeheimnisträgers ist hingegen nicht mehr erforderlich. Folglich ist eine Weitergabe mandatsbezogener Informationen an diesen Personenkreis damit zwar tatbestandsmäßig, aber erlaubt, mithin nicht unbefugt, wie es das Gesetz fordert.

Greift man sich in diesem Kontext nur die im privaten und unternehmerischen Alltag nicht mehr wegzudenkende – trotz der damit verbundenen Risiken zumindest in weiten Bereichen als sozialadäquat eingeordnete – Möglichkeit der Nutzung dezentraler IT-Ressourcen (Cloud)[8] heraus, so muss klar sein, ob der Auftraggeber und der Auftragnehmer sich nach § 203 StGB strafbar machen, wenn diese Daten in die Cloud übermitteln bzw. übermitteln lassen.

Von einer erlaubten Weitergabe mandatsbezogener Informationen sind Anbieter von Cloud-Plattformen, die eine verschlüsselte Speicherung zulassen, nunmehr erfasst. Dabei muss zwischen Transportverschlüsselung und der verschlüsselten Speicherung unterschieden werden, siehe dazu den BSI Anforderungskatalog Cloud-Computing (C5).[9] Aus dem Gesetz geht nicht hervor, ob alle Cloud-Lösungen[10] darunter zu fassen sind, weil keine Differenzierung möglicher Cloud-Anwendungen vorgenommen wird (unklar bleibt, wie bspw. „Software as a Service“ Angebote zu behandeln wären). Darüber hinaus gibt es keine Hinweise darauf, wie Cloud-Lösungen auszugestalten sind,[11] damit sie in den Anwendungsbereich fallen bzw. gerade davon ausgenommen bleiben. Rechtlich muss davon ausgegangen werden, dass es sich bei den Vorgaben des BSI um den „Stand der Technik“ handelt, der etwa nach § 13 Abs. 7 TMG bereits heute von jedem Diensteanbieter beachtet werden muss.[12] Stand der Technik ist die Verschlüsselung vor dem Ablegen in der Cloud beim Rechtsanwalt und zudem eine Transportverschlüsselung, denn dann kann der Cloud-Anbieter die Daten nicht zur Kenntnis nehmen.[13] Ein entscheidendes Abgrenzungskriterium wäre sicherlich darin zu sehen, ob die Berufsgeheimnisträger selbst oder deren Gehilfen unabhängig vom Cloud-Anbieter auf die gespeicherten Daten zugreifen können, was der Regelfall sein dürfte. Weiterhin gilt zu differenzieren, ob und in welcher Form der Cloud-Anbieter zugangsberechtigt ist, sowie, ob eine differenzierte Zugangsberechtigung in der Sphäre des Berufsträgers gegeben ist.[14]

Die Verlagerung vorhandener Informationen in die Cloud sowie die Nutzung dieser Informationen bedingt spezifische Sicherheitsstandards.[15] Als Beispiel kann auf den Anforderungskatalog Cloud-Computing (C5) „Kriterien zur Beurteilung der Informationssicherheit von Cloud-

---

8 *Conrad/Fechtner*, CR 2013, 137 ff.; *Hilgendorf,* in: Hilgendorf (Hrsg.), Informationsstrafrecht und Rechtsinformatik, 2004, S. 83; *Leupold,* Münchener Anwalthandbuch IT-Recht, 3. Aufl. (2013), 4/18 ff.; *Preuß*, DuD 2016, 802 ff.

9 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cloud Computing/Anforderungskatalog/Anforderungskatalog.pdf?__ blob=publicationFile&v=7 (zuletzt abgerufen am 25.9.2017).

10 Zu verschiedenen Erscheinungsformen näher *Preuß*, DuD 2016, 802 f.

11 Dazu näher *Cornelius*, StV 2016, 380.

12 Vgl. wiederum BSI –C5 (Fn. 9).

13 Die etwa ehemals von DAVIT empfohlene Lösung „doculife“, hinter der ein Schweizer Anbieter steht und die von der Telekom vermarktet wurde, übermittelte das „Master-Secret“, also den „privaten Schlüssel“ (sic!) bei jedem Aufruf des Dienstes an den Dienstleister zur Entschlüsselung der beim Dienstleister liegenden Dokumente und Daten. Zum „Security-Konzept doculife“: https://www.t-systems.com/blob/651436/b57154598372f8dbfb3a3adde0d32c3c/DL_ Doculife_Dokumentenmanagement.pdf. (zuletzt abgerufen am 25.9.2017).

14 Vgl. *Preuß*, DuD 2016, 802 (803).

15 https://www.heise.de/newsticker/meldung/BSI-setzt-Regeln-fuer-Cloud-Kunden-3704637.html? (zuletzt abgerufen am 25.9.2017); vgl. auch *Kemmerich/Agrawal/Momsen*, in: Ryan Ko/Raymond Choo (Hrsg.), The Cloud Security Ecosystem Technical, Legal, Business and Management Issues, Oxford (2015) S. 205-230.

Diensten“ verwiesen werden.

Das neue Gesetz legt richtigerweise eine Differenzierung zwischen den Gehilfen des Berufsträgers zugrunde, an welche auch bislang eine Weitergabe prinzipiell straflos erfolgen konnte, und anderen mitwirkenden Personen, welche nicht der Sphäre des Berufsträgers zuzuordnen sind. Im Grunde führt die Erweiterung des Personenkreises zu einer Verringerung des strafrechtlichen Geheimnisschutzes, trägt aber den technischen Bedürfnissen im digitalen Zeitalter Rechnung, sowie dem bestehenden Problem, dass nach überwiegender Ansicht externe Personen für den Bereich des § 203 Abs. 1 StGB gerade nicht als berufsmäßige Gehilfen gelten. Dieses relativ restriktive Ergebnis wird zumindest teilweise dadurch kompensiert, dass die für den Berufsgeheimnisträger tätig werdenden Dienstleister, die von diesem auf eine Geheimhaltung verpflichtet wurden, nunmehr selbst von dem Anwendungsbereich der Norm erfasst werden und sich ebenfalls strafbar machen können, § 203 Abs. 4 S.1 StGB. Dahingehend wird also der Täterkreis auf externe Dienstleister erweitert. Diese Neuregelung führt damit in einem ersten Schritt zu einer erheblichen Ausweitung der Strafbarkeit auf einen Personenkreis, der keine berufsspezifischen Tätigkeiten ausübt und bis dato keinem vergleichbaren Strafbarkeitsrisiko ausgesetzt war. Anpassungen bspw. im Bereich der Angebote von IT-Dienstleistungen an Berufsgeheimnisträger sowie bei der Ausgestaltung entsprechender Verträge werden notwendig (s.u. IV.).

Zusätzlich treffen den Berufsgeheimnisträger bei der Beauftragung Dritter weitere (Sorgfalts-) Pflichten. Der Berufsgeheimnisträger macht sich strafbar, wenn eine sonstige mitwirkende Person ein Geheimnis offenbart, er aber nicht dafür Sorge getragen hat, dass die Person zur Geheimhaltung verpflichtet ist (Abs. 4 S. 2). Trotz des Fehlverhaltens einer dritten Person, die die eigentliche Tathandlung (Offenbaren eines Geheimnisses) begangen hat, wird der Berufsgeheimnisträger also dann bestraft, wenn er den Dritten nicht zur Geheimhaltung verpflichtet hat. Aus dem Wortlaut des Gesetzes „nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person […] zur Geheimhaltung verpflichtet wurde“ lässt sich dahingehend eine einmalige Pflicht entnehmen. Wann die Verschwiegenheitsverpflichtung vorzunehmen ist, regelt § 203 StGB nicht, ebenso wenig wie konkret die Sorgfaltspflicht ausgestaltet ist. Soweit spezifisches Berufsrecht gilt (vgl. § 43e BRAO, s.u.D.) sind die Pflichten teilweise weitergehend konkretisiert.

Die Befugnis, sich der Inanspruchnahme von Dienstleistern zu bedienen, tritt aber nur dann ein, wenn gewährleistet ist, dass die Verschwiegenheitspflicht bei diesen Dienstleistern *vertraglich sichergestellt* ist. Der Gesetzgeber normiert damit strafbewehrte Sorgfaltspflichten für die Berufsgeheimnisträger, die bei der Einbeziehung dritter Dienstleister zu beachten sind (s.u.). Regelungstechnisch deutet Abs. 4 S. 2 auf ein sog. „echtes Unterlassungsdelikt“[16] hin. Nr. 1 und 2 beschreiben eine Pflichtenkaskade, wonach eine Unterlassensstrafbarkeit bspw. des Rechtsanwalts auch dann besteht, wenn er seine Hilfspersonen nicht über die abgeleitete Pflichtenstellung i.S.v. Nr. 2 belehrt. Begrüßenswert erscheint, dass der Berufsgeheimnisträger die Pflicht nicht nur erfüllt, wenn er die erforderliche Verpflichtung selbst vornimmt, sondern dies auch durch einen Dritten geschehen kann, da sich die strafbewehrte Verpflichtung zur Geheimhaltung insbesondere in mehrstufigen Verhältnissen bis zur letztlich tätig werdenden Person fortsetzt, § 203 Abs. 4 Nr. 2 StGB. Somit kann ein weitgehend lückenloser Schutz des fremden Geheimnisses erreicht werden.

III. Strafprozessuale Perspektive

§ 53a StPO gewährleistet für das Verhältnis zwischen Mandant und Rechtsanwalt ein gewisses Maß an Schutzstandards. Im Bereich des thematisierten Datenoutsourcings wird dies in den Fällen relevant, in denen sowohl strafrechtlich gegen den Mandanten ermittelt wird, als auch die vom Mandanten beauftragte Kanzlei, die für das Zivilverfahren mandatiert wurde, Rechtsdienstleistungen auslagert. Es wäre fatal, wenn die mandatsbezogenen Privilegien beim Datenoutsourcing nicht greifen würden. Diese Situation wird unter anderem durch das Zeugnisverweigerungsrecht nach §§ 53, 53a StPO reguliert. Der Wortlaut des § 53 StPO bezieht sich auf Strafverteidiger, Rechtsanwälte und Steuerberater. § 53a StPO erweitert diesen umfassenden Schutz für Gehilfen, die an der berufsmäßigen Tätigkeit des geschützten Personenkreises teilnehmen („Berufshelfer“). Insoweit stellt sich die Frage, ob der Gehilfenbegriff des § 203 StGB und der des § 53a StPO gleichzusetzen sind. Um in Genuss des durch § 53a StPO intendierten Schutzes des Vertrauensverhältnisses zu gelangen, fordert die Rechtsprechung, dass zwischen der Tätigkeit des Berufsträgers (Auftraggeber) und der Hilfsperson (Auftragnehmer) ein innerer funktionaler Zusammenhang bestehen muss.[17] Dieser umfasst dann ebenfalls die vom § 203 StGB umfassten Gehilfen, jedoch nicht unbedingt Dritte (externe Diensteanbieter), die selbstständige Einzelaufträge ausführen, wie Cloud-Anbieter. Denn diese Personengruppe unterfällt nicht dem bisherigen Wortlautverständnis des § 53a StPO. Im Zusammenhang des Datenoutsourcings im Hinblick auf § 203 StGB muss daher auch die Reichweite des Gehilfenbegriffs aus § 53a StPO neu diskutiert werden, um einen umfassenden Schutz zu gewährleisten. Sollte ein funktionsbezogener Interpretationsansatz bei Gehilfen maßgeblich sein, könnte dem Abhilfe geschaffen werden. Danach ist Gehilfe jede Person, die vom Hauptberufsträger für die in § 53 Abs. 1 Nr. 1 bis 4 StPO bezeichneten Tätigkeiten herangezogen wird und umfasst jede Wahrnehmung, die dem Berufshelfer in dieser Eigenschaft anvertraut oder bekannt wird. Danach wäre der selbstständig auftretende Cloud-Anbieter Gehilfe im Sinne des § 53a StPO, sowie eine „sonstige mitwirkende Person“ nach § 203 StGB. Angesichts der bisherigen Handhabung des § 53a StPO folgt dieses erweiterte funktionsbezogene Verständnis jedoch nicht aus der Änderung des § 203 StGB. Zudem müsste klargestellt werden, dass (bzw. unter welchen Voraussetzungen) insoweit auch Mandanten

[16] Vgl. BT-Drs. 18/11936, S. 28.

[17] *BGH*, Urt. v. 7.4.2005 – 1 StR 326/04; BGHSt 50, 64 = NJW 2005, 2406; *Percic*, in: MüKo-StPO (2014), § 53a Rn. 2 m.w. N.

funktionsbezogen Kenntnis erlangen können.

Aus Sicht der Mandanten, der Berufsgeheimnisträger und Dritter involvierter Personen bedarf es daher insgesamt einer einheitlichen und in sich konsistenten Regelung der §§ 53, 53a StPO und § 203 StGB. Dass diese im Rahmen der Gesetzesänderung nicht umfassend in Angriff genommen wird, ist nicht nur eine lässliche Sünde, sondern führt zu erheblichen Verwerfungen. Dies wird deutlich, wenn der Blick auf das parallele Gesetzgebungsverfahren zum „Entwurf eines Gesetzes zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens[18] gerichtet wird. Im Zusammenhang mit den Ermittlungsmaßnahmen „Online-Durchsuchung“ und „Staatstrojaner“ wird insbesondere infolge der Neuregelung des § 100d Abs. 5 StPO der Schutz stark relativiert, da Ermittlungsmaßnahmen gegen Hilfspersonen, welche häufig den Hauptteil der Kommunikation bestreiten, einer weitreichenden Abwägung geöffnet werden.

Zwischen beiden Konzeptionen entsteht, worauf u.a. *Conen* zutreffend hinweist, ein erheblicher Wertungswiderspruch: Materiell-rechtlich soll mit dem Gesetz zu § 203 StGB zum einen die Erweiterung des Personenkreises, der mit Geheimnissen des Berufsgeheimnisträgers befasst wird, erleichtert und der heutigen Arbeitswelt angepasst, andererseits der Schutz dieser Geheimnisse bei Dritten unverändert durch Strafbarkeit der Offenbarung auch durch den erweiterten Personenkreis gewährleistet werden. Während also hier der Kreis von potentiellen Berufshelfern ausgedehnt wird und dabei der Schutz der Geheimnisse materiell-rechtlich in vergleichbarer Weise wie beim Berufsgeheimnisträger erreicht werden soll, führt das andere Vorhaben u. a. auch dahin, den Schutz dieser Geheimnisse bei Dritten zu relativieren, sofern sie staatlicherseits durch Quellen-TKÜ oder Onlinedurchsuchungen von den Ermittlungsbehörden heimlich, ggf. auch zielgerichtet erlangt werden. Der Änderungsvorschlag des BMJV zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11936 – konnte hier keine ausreichende Abhilfe schaffen.

IV. Berufsrecht, Datenschutzrecht und Compliance

Für Rechtsanwälte soll die bislang nur satzungsrechtlich bestehende Verpflichtung, Personal und mitwirkende Personen zur Verschwiegenheit zu verpflichten, nunmehr ins Gesetz übernommen werden, § 4a Abs. 2 BRAO.[19] Dabei ergibt sich erst aus § 203 StGB-E in Verbindung mit § 43e BRAO, dass eine Belehrung nicht ausreicht, sondern regelmäßig auch eine Überwachung erforderlich ist. Nur dann stehen die neuen Regelungen im Einklang mit Art. 35 DSGVO und den allgemeinen Anforderungsprofilen im Bereich der IT-Compliance.

Sofern also der Berufsgeheimnisträger dritte Personen an seiner Berufsausübung mitwirken lässt, ist er im Interesse des Geheimnisschutzes nunmehr dazu verpflichtet, diese Dritten als Dienstleister in schriftlicher Form *zur Verschwiegenheit zu verpflichten*, diese über die strafrechtlichen Folgen einer Pflichtverletzung *zu belehren*, in geeigneter Weise *auf die Einhaltung der Verschwiegenheit hinzuwirken* und im Hinblick auf ihre Vertrauenswürdigkeit *sorgfältig auszuwählen* und *zu überwachen*.

Die Formulierung aus § 43e Abs. 2 S. 1 BRAO[20] ist als Compliance Vorschrift zu werten, bzw. als gesetzlicher Auftrag, entsprechende Compliance-Strukturen zu schaffen. Derartige Compliance-Strukturen bzw. prognostischen Prüfungen verlangt in der Sache bereits die Datenschutz Grundverordnung (siehe Datenschutz-Folgenabschätzung; Art. 35 DSGVO).

Denkbar wäre es, analog zu entsprechenden Verfahrensweisen im Compliance-Sektor, auf eine Zertifizierung[21] des Diensteanbieters abzustellen, welche u.a. eine regelmäßige Schulung der Mitarbeiter nachweisen.[22] Allerdings müssten entsprechende verbindliche Standards geschaffen werden und im Einklang mit datenschutzrechtlichen Anforderungen stehen.[23] Denkbar wäre auch eine einzelvertragliche Ausgestaltung i.S. § 43e Abs. 3 Nr. 3 BRAO. Problematisch daran ist, dass diese die vertraglichen oder nichtvertraglichen Auftragsverhältnisse mit Arbeitnehmern oder Dritten auf Seiten des Dienstleisters nicht umfänglich erfassen kann.[24] Mit Blick auf eine strafrechtlich einheitliche Handhabung erscheint jedenfalls eine weitergehende Konkretisierung unabhängig vom Einzelfall erstrebenswert.[25]

Entscheidend für die Rechtssicherheit wird damit die Entwicklung verbindlicher IT-Sicherheitsstandards. Solange diese fehlen, wird das Risiko, den neuen gesetzlichen Anforderungen genügende IT-Konzepte vorzuhalten, auf die Berufsgeheimnisträger abgewälzt, ohne dass valide Informationsquellen zur Verfügung gestellt werden.[26]

Im Hinblick auf eine mögliche Konkretisierung der Pflicht kann dies insoweit vorgenommen werden, als das hinsichtlich der Adressaten und des jeweiligen Gefahrenpotenzials differenziert wird. Insoweit erlangt eine Differenzierung der „mitwirkenden Personen“ Bedeutung. Um

---

18 BT-Drs. 18/11277.

19 „Der Rechtsanwalt hat die von ihm beschäftigten Personen in schriftlicher Form zur Verschwiegenheit zu verpflichten und sie dabei über die strafrechtlichen Folgen einer Pflichtverletzung zu belehren. Zudem hat er bei ihnen in geeigneter Weise auf die Einhaltung der Verschwiegenheitspflicht hinzuwirken.“

20 „Der Rechtsanwalt ist verpflichtet, den Dienstleister sorgfältig auszuwählen.“

21 *Traudes*, Zertifizierung als Maßnahme der (Criminal) Compliance, 2017.

22 Entsprechende Angebote, wie etwa „Trusted Cloud – Datenschutzprofil für Cloud-Dienste“ (http://www.tcdp.de/index.php) bestehen. Jedoch müssten die Zertifizierungen allgemeine Verbindlichkeit beanspruchen können, um strafrechtliche Wirkung zu entfalten.

23 Vgl. *Preuß*, DuD 2016, 804.

24 Zu § 53a StPO s.o. III. am Ende.

25 Zu Großprojekten unter Einbindung externer Dritter zweifelnd *Raschke*, BB 2017, 579 (580).

26 Dies mag für große Teilnehmer auf dem Markt, welche eine eigene IT-Abteilung unterhalten können, tolerabel sein. Kleinere und mittlere Kanzleien droht hier allerdings ein nicht zu unterschätzender Wettbewerbsnachteil. Sinnvoll erschiene es, bspw. hierauf zugeschnittene BSI-Richtlinien zu erlassen. Ebenfalls müsste differenziert festgelegt werden, wann bzw. welche ausländischen Anbieter die Standards erreichen. Für den Verwender ist es i.d.R. nicht zu erkennen, ob die Dienstleistungen ganz oder zum Teil im Ausland erbracht werden. Vertragliche Regelungen werden hier auch vielfach nicht in adäquater Form erfolgen können.

keine hypertrophe gesetzliche Regelung zu schaffen, bietet sich eine funktionsbezogene Betrachtungsweise an, die jedenfalls im Gesetz angelegt werden könnte.[27] Funktionsbezug wäre jedenfalls gegeben, wenn der „sonstige Mitwirkende" bei Ausübung der ihm übertragenen Aufgaben „bestimmungsgemäß" oder „regelmäßig" mit Geheimnissen in Berührung kommt.

Die in § 43e BRAO genannte Prüfungs- und Sorgfaltspflicht ist gegenüber der „Dienstleister" anzuwenden, wohingegen § 203 StGB diese auf „sonstige mitwirkende Personen" als tatsächlich tätige natürliche Personen bezieht.

Die berufs- bzw. strafrechtlichen Vorgaben finden parallel zu den datenschutzrechtlichen Regelungen des BDSG Anwendung. Aus datenschutzrechtlicher Perspektive ist § 11 BDSG zu beachten. Eine Reihe von Outsourcing-Fällen lässt sich mit vertraglichen Vereinbarungen lösen, die die Anforderungen des § 11 BDSG erfüllen.[28] In vielen Fällen kann eine datenschutzrechtliche Vereinbarkeit erzielt werden, auch wenn nicht grundsätzlich jedes Outsourcing von Datenverarbeitungsdienstleistungen per se als Auftragsdatenverarbeitung i.S.v. § 11 BDSG zu werten ist.[29] So wird beispielsweise die Nutzung von Cloud Computing überwiegend als Auftragsdatenverarbeitung i.S.d. § 11 BDSG eingeordnet.[30]

Im Hinblick auf die datenschutzrechtliche Wertung muss in strafrechtlicher Hinsicht beachtet werden, dass wenn datenschutzrechtlich eine Auftragsdatenverarbeitung (ADV) vorliegt, sich keine Rechtfertigung nach § 203 StGB herleiten lässt, da die ADV sich nicht auf Geheimnisse bezieht. Das StGB und das BDSG haben diesbezügliche unterschiedliche Schutzbereiche (Geheimnisse von natürlichen und juristischen Personen – personenbezogene Daten von natürlichen Personen). Nach § 1 Abs. 3 S. 2 BDSG bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten vom Datenschutzrecht vielmehr unberührt und § 11 BDSG ist nicht als Rechtfertigungsgrund formuliert.[31] Somit kann sich ein Wertungswiderspruch zwischen Straf- und Datenschutzrecht ergeben, der durchaus praktische Bedeutung hat.[32]

V. Fazit

Die Neuregelung des Gesetzes ist ein notwendiger Baustein, um den Geheimnisschutz der Berufsausübung im IT-Zeitalter anzupassen. Zu begrüßen ist neben der generellen Zielrichtung auch die faktische Schaffung von Compliance-Standards. Hier allerdings bedarf es weiterer Regelungen, damit die Standards von den Berufsgeheimnisträgern erfüllt werden können sowie einer Abstimmung mit datenschutzrechtlichen Regelungen. Dringlicher Nachsteuerungsbedarf besteht zudem im Bereich des § 53a StPO.

---

27 Dazu ausf. *Cornelius*, StV 2016, 384 ff.

28 *Fechtner*, https://www.cr-online.de/blog/2017/01/06/geplante-neuregelung-in-§-203-stgb-erleichterte-einbindung-externer-dienstleister-fuer-berufsgeheimnistraeger/ (zuletzt abgerufen am 25.9.2017).

29 *Fechtner* (Fn. 28); zur Abgrenzung *Conrad/Fechtner*, CR 2013, 137 ff.

30 *Preuß*, DuD 2016, 803 m.w.N.

31 *Cornelius*, StV 2016, 381.

32 Dazu ausführlich *Preuß*, DuD 2016, 804.