

Geheimnisschutzrechtliche Grenzen und datenschutzrechtliche Implikationen des Cloud Computing in der anwaltlichen Praxis

A. Einleitung¹

Die Digitalisierung durchdringt seit der Jahrtausendwende² sukzessive alle Wirtschaftssektoren. Digitale Technologien und Serviceangebote prägen im privaten wie im geschäftlichen Bereich unseren Alltag. Auch im Rechtsdienstleistungsmarkt hält die digitale Transformation Einzug. Eine Vielzahl dieser digitalen Dienste wird über das sog. Cloud Computing bereitgestellt – ohne dass dies dem Nutzer regelmäßig bewusst sein wird.³ Obwohl der Begriff „Cloud“ mittlerweile fest im allgemeinen Sprachgebrauch verankert ist, wird er häufig noch eindimensional als Synonym für einen Online-Datenspeicher verstanden. Insbesondere Privatnutzer assoziieren mit der „Datenwolke“ in erster Linie einen jederzeit und von überall erreichbaren Speicherort, etwa für Fotos, Dokumente oder andere Dateien.⁴ Diese eingeschränkte Sichtweise findet sich teilweise auch im rechtswissenschaftlichen Diskurs wieder.⁵

Cloud Computing umfasst jedoch weit mehr als die bloße Speicherung von Daten.⁶ Ein Großteil moderner Softwareanwendungen wird heute über Cloud-Architekturen bereitgestellt.⁷ Auch in der anwaltlichen Praxis sind cloudbasierte Softwaredienste inzwischen weit verbreitet.⁸ Sie bieten den Vorteil des ortsunabhängigen Arbeitens

¹ Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern das generische Maskulin verwendet. Diese Begriffe beziehen sich gleichermaßen auf alle Geschlechter. Die gewählte Sprachform dient ausschließlich der Vereinfachung und stellt keine Wertung dar.

² Greiner/Riepl/Kittelberger, in: Kieninger, Digitalisierung der Unternehmenssteuerung, S. 20.

³ Mina/Zerres/Zerres, Legal-Tech-Dienste in Deutschland, S. 61; Degen/Emmert, Elektronischer Rechtsverkehr, S. 1; Reinemann, in: Remmert, Legal Tech, S. 4; Hähnchen/Bommel, AnwBl 2018, 600.

⁴ Vgl. Hennrich, Cloud Computing nach der DSGVO, S. 21ff.

⁵ So etwa: Cierniak/Niehaus, in: MüKo-StGB, § 203 Rn. 60; Heger, in: Lackner/Kühl/Heger, StGB, § 203 Rn. 25a.

⁶ Siehe zu den einzelnen Services, S. 8.

⁷ In der deutschen Wirtschaft erfolgt dies bereits bei rund der Hälfte aller IT-Anwendungen – mit steigender Tendenz, KPMG, Cloud-Monitor 2024, abrufbar unter: <https://hub.kpmg.de/de/cloud-monitor-2024> (zuletzt abgerufen am 24.04.2026).

⁸ Schwarzenegger/Thouvenin/Stiller, Nutzung von Cloud-Diensten durch Anwälte, VII; Zunker, Die Kanzlei in der Cloud, AnwBl. Digital v. 07.07.2023, abrufbar unter: <https://anwaltsblatt.anwaltverein.de/de/themen/kanzlei-praxis/cloud-kanzlei> (zuletzt abgerufen am 24.04.2026); vgl. Weiss, in: Hilber, HdB Cloud Computing, S. 25.

und reduzieren den Bedarf an kostenintensiver IT-Infrastruktur.⁹ Aber auch abseits spezieller Anwaltssoftware spielt Cloud Computing im anwaltlichen Berufsalltag eine fast unumgängliche Rolle. E-Mail und Kalenderdienste, digitale Diktier- und Spracherkennung oder die bloße Synchronisation von Kontakten erfolgen oftmals mittels Cloud Computing.¹⁰

Diese Nutzung cloudbasierter Dienste stellt Anwälte vor rechtliche Herausforderungen.¹¹ Als Berufsgeheimnisträger sind sie gem. § 43a Abs. 2 BRAO, § 2 BORA zur Verschwiegenheit verpflichtet. Eine Verletzung ist nicht zuletzt strafbewehrt (§ 203 StGB). Zusätzliche zu dieser besonderen berufsrechtlichen Dimension ergeben auch für den Anwalt als für die Datenverarbeitung Verantwortlichen datenschutzrechtliche Implikationen bei der Verwendung von Cloud Services.¹²

B. Cloud Computing

Die einerseits praktische und andererseits berufs- und datenschutzrechtliche Relevanz der anwaltlichen Nutzung cloudbasierter Dienste macht ein Grundverständnis aufseiten der anwaltlichen Praxis erforderlich, was unter Cloud Computing zu verstehen ist und wie die zugrundeliegenden technischen Prozesse – rudimentär – ablaufen. Erst hierdurch ist der Anwalt als Nutzer befähigt, seine berufs- und datenschutzrechtlichen Pflichten verantwortungsvoll zu erfüllen.

I. Etymologie und Begriffsverständnis

Der Ursprung des Begriffes „Cloud-Computing“ wird unterschiedlich verortet.¹³ Überwiegend wird der Begriff *Rammah Chellappa* zugeschrieben, der ihn im Rahmen eines wissenschaftlichen Vortrages auf einer Konferenz in Dallas verwendete. Dabei umschrieb er Cloud Computing als ein neues Computerparadigma, bei dem die Grenzen der Datenverarbeitung durch wirtschaftliche Überlegungen und nicht allein durch technische Grenzen bestimmt werden.¹⁴ Seither finden sich in der wissenschaftlichen Literatur unterschiedliche Definitionsansätze, die den Begriff

⁹ Vgl. *Henrich*, Cloud Computing nach der DSGVO, S. 17.

¹⁰ Vgl. *Davis*, in: EPRS, Cloud Computing, S. 5, abrufbar unter: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA\(2016\)583786_DE.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_DE.pdf) (zuletzt abgerufen am 24.04.2026).

¹¹ Vgl. *Hartung*, in: Leupold/Wiebe/Glossener, IT-Recht, Teil 11.4.2 Rn. 1.

¹² Siehe S. 21f.

¹³ Teilweise verweisen Stimmen auf das IT-Unternehmen Netcentric, das 1997 den Versuch unternahm die Wortmarke „cloud computing“ in den USA schützen zu lassen, vgl. *Yukvaraj*, Cloud Computing, S. 12.

¹⁴ *Hentschel/Leyh*, in: Reinheimer, Cloud Computing, S. 4, *Yukvaraj*, Cloud Computing, S. 12.

des Cloud Computing vornehmlich vor dem Hintergrund seiner wirtschaftlichen Funktion in Form der Auslagerung von Informationstechnologien (IT-Outsourcing) bestimmen.

So beschreiben *Buya et al.* Cloud-Computing als Erweiterungen, bei denen die Funktionen von Geschäftsanwendungen als hochentwickelte Dienste dargestellt werden, auf die über ein Netz zugegriffen werden kann. Im Fokus steht hierbei die Zugänglichkeit kommerzieller Anwendungen, die unabhängig vom Standort des Nutzers flexibel genutzt werden können.¹⁵ *Jha, Merzky* und *Fox* erweitern diesen Ansatz um technische Aspekte, indem sie Cloud Computing als Sammelbegriff für Technologien beschreiben, die eine verbesserte Kontextualisierung, Virtualisierung und insbesondere eine vereinfachte Nutzung von IT-Ressourcen ermöglichen.¹⁶ Auch *Weiss* betont die Bereitstellung leistungsstarker Dienste und Anwendungen, die in das Web integriert und dort als flexible Angebote „verpackt“ werden.¹⁷ *Repschläger, Pannicke* und *Zarnechow* definieren Cloud Computing wiederum vor dem Hintergrund seiner wirtschaftlichen Dimension als „Ansammlung von Diensten, Anwendungen und Ressourcen [...], die dem Nutzer flexibel und skalierbar über das Internet angeboten werden, ohne eine langfristige Kapitalbindung und IT-spezifisches Know-how vorauszusetzen. Es handelt sich um eine Form des IT-Sourcings, bei der der komplette Betrieb und Wartungsaufwand beim Anbieter verbleibt und ausschließlich die Leistung vom Kunden angemietet und verbrauchsunabhängig bezahlt wird“.¹⁸

Bei der Begriffsbestimmung bedeutsam ist die Definition des National Institute of Standards and Technology (NIST).¹⁹ Sie wurde lange Zeit auch durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) verwendet.²⁰ In ihrer Publikation aus dem September 2011 mit dem Titel „The NIST Definition of Cloud Computing“ entwickelten die Autoren *Mell* und *Grance* fünf Wesenselemente, die für das Cloud Computing charakteristisch sind²¹:

¹⁵ *Buyya/Venugopal/Broberg/Brandic*, Cloud Computing and emerging IT platforms, S. 599.

¹⁶ *Jha/Merzky/Fox*, in: *Concurrency and Computation*, S. 1088.

¹⁷ *Weiss*, *ACM NetWorker* 2007, 16ff.

¹⁸ *Repschläger/Pannicke/Zarnechow*, *HMD Praxis der Wirtschaftsinformatik* 2016, S. 6.

¹⁹ *Krcmar*, in: *Borges/Meents*, *Cloud Computing*, § 1 Rn. 31.

²⁰ *Hentschel/Leyh*, in: *Reinheimer*, *Cloud Computing*, S. 4.

²¹ *Mell/Grance*, *The NIST Definition of Cloud Computing*, S. 2, abrufbar unter: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf> (zuletzt abgerufen am: 24.06.2026).

1. Selbstbedienung nach Bedarf (On-Demand Self-Service):

Nutzer können IT-Ressourcen wie Rechenleistung, Speicherplatz oder Netzwerkkapazitäten bei Bedarf eigenständig und automatisiert anfordern und nutzen, ohne dass dafür ein manueller Eingriff oder eine direkte Interaktion mit dem Cloud-Anbieter notwendig ist.

2. Breiter Netzwerkzugang (Broad Network Access):

Die angebotenen Cloud-Dienste sind über das Netzwerk – typischerweise das Internet – erreichbar und können mit verschiedensten Endgeräten wie Laptops, Smartphones oder Tablets genutzt werden. Der Zugriff erfolgt über standardisierte Schnittstellen und Protokolle, was eine ortsunabhängige und plattformübergreifende Nutzung ermöglicht.

3. Ressourcenpooling²²:

Die IT-Ressourcen des Cloud-Anbieters werden in einem Pool gebündelt und mehreren Nutzern (sog. Mandanten²³) dynamisch zugewiesen. Die Ressourcenverteilung erfolgt automatisiert und flexibel je nach Bedarf der einzelnen Nutzer.

4. Schnelle Elastizität (Rapid Elasticity):

Cloud-Ressourcen können schnell und in nahezu beliebigem Umfang bereitgestellt oder wieder freigegeben werden. Diese „Elastizität“ erlaubt es, die Kapazitäten dynamisch an den aktuellen Bedarf anzupassen. Für den Nutzer erscheint die verfügbare Ressource nahezu unbegrenzt und jederzeit verfügbar.

5. Messbarer Service (Measured Service):

Die Nutzung der Cloud-Ressourcen wird kontinuierlich überwacht, gemessen und transparent abgerechnet. Nutzer zahlen in der Regel nur für die tatsächlich in Anspruch genommenen Leistungen („Pay-per-Use“).

Mell und *Grance* ergänzen damit die service- und anwendungsorientierte Definition des Cloud Computing i.S.e. niederschweligen, hochverfügbaren und dezentralisierten Zugangs zu IT-Ressourcen um die wesentlichen technischen Aspekte einer Cloud Computing Architektur (Virtualisierung, Pooling, etc.).

²² Siehe hierzu B. II. 2.

²³ Im Cloud Computing beschreibt der Begriff Mandant (englisch: Tenant) eine eigenständige Organisation oder Nutzergruppe, die innerhalb einer gemeinsamen IT-Infrastruktur oder Softwareinstanz logisch von anderen Mandanten getrennt ist und deren Daten und Einstellungen isoliert verwaltet werden. Der Begriff ist damit abzugrenzen von der Person, die einen Anwalt beauftragt, sie rechtlich zu vertreten bzw. zu beraten.

Mit der ISO/IEC 22123-2 besteht seit 2023 nunmehr ein international anerkannter Standard zur Terminologie und Definition des Cloud Computing.²⁴ Er basiert ausweislich seines Inhaltes auf der NIST-Definition; ergänzt diese jedoch um das Merkmal der Mandantenfähigkeit.²⁵ Diese im Englischen als Multi-Tenancy bezeichnete technische Komponente ist notwendig, um sicherzustellen, dass mehrere unabhängige Nutzer (sog. Mandanten) einen Cloud-Service²⁶ gleichzeitig nutzen können, während ihre Daten und Konfigurationen strikt voneinander getrennt bleiben.²⁷

Kombiniert man die unterschiedlichen Definitionsansätze, so lässt sich Cloud Computing als eine mittels Virtualisierungstechnologien bedarfsgerechte und orts-unabhängige Bereitstellung von flexibel skalierbaren sowie gemeinsam nutzbaren gepoolten IT-Ressourcen (insb. Rechenleistung, Speicher, Anwendungen und Diensten) definieren, die über einen breiten Netzwerkzugang (typischerweise das Internet) abrufbar sind. Nutzer können diese Ressourcen strikt voneinander getrennt in Echtzeit abrufen, ohne sich um die zugrundeliegende Infrastruktur oder deren Wartung kümmern zu müssen. Die Verwaltung und Abrechnung erfolgt dabei automatisiert und nutzungsbasiert (On-Demand Self-Service).

II. Technische Funktionsweise

Cloud Computing ist somit keine einzelne, abgrenzbare Technologie, sondern ein technisches Modell, das auf der Integration von Schlüsseltechnologien basiert, mit dem Ziel einer dynamischen, skalierbaren und bedarfsgerechten Bereitstellung von IT-Ressourcen.²⁸

Im Sinne einer groben Systematisierung lässt sich das technische Konstrukt des Cloud Computing in vier, logisch aufeinander aufbauende Ebenen unterteilen.²⁹ Ausgangspunkt ist die Bereitstellung von Hardwareressourcen als physisches

²⁴ Vgl. BSI, Cloud Computing Grundlagen, Was ist Cloud Computing, abrufbar unter: <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html> (zuletzt abgerufen am 24.04.2026).

²⁵ Vgl. *Henrich*, Cloud Computing nach der DSGVO, S. 24; *Schorer*, in: Hilber, HdB Cloud Computing, S. 72.

²⁶ Zu den einzelnen Service-Modellen: S. 8.

²⁷ *Krcmar*, in: Borges/Meents, Cloud Computing, § 1 Rn. 33; *Schorer*, in: Hilber, HdB Cloud Computing, S. 72; vgl. auch *Rückert*, in: MüKo-StPO, § 100b Rn. 33; *Cornelius*, StV 2016, 380.

²⁸ Vgl. *Krcmar*, in: Borges/Meents, Cloud Computing, § 1 Rn. 29 ff.

²⁹ Vgl. *Cerroni/Gharbaoui/Martini/Campi/Castoldi/Callegati*, Computer Networks 2015, 16; *Abdallah/Boudriga*, in: Mouftah/Kantarci, Communication Infrastructures für Cloud Computing, S. 123; *Schorer*, in: Hilber, HdB Cloud Computing, S. 72.

Fundament (Infrastrukturebene).³⁰ Diese physische Hardwareinfrastrukturen in Form von Festspeichern, Prozessoren und RAM oder Switches werden in einer zweiten Schicht durch Virtualisierungstechnologien (insb. Hypervisoren) in flexible, logisch getrennte Ressourcen verwandelt (Virtualisierungsebene).³¹ Eine darüberliegende dritte, softwarebasierte Schicht automatisiert und koordiniert Workflows, Ressourcen und Dienste über die verschiedenen virtualisierten IT-Ressourcen, um deren Bereitstellung effizient, zuverlässig und ohne manuelle Eingriffe zu ermöglichen (Orchestrierungsebene).³² Auf der vierten und letzten Ebene (Softwareebene) erfolgt sodann die Bereitstellung der visualisierten und orchestrierten Ressourcen als konkrete Dienste an die Nutzer in ihren entsprechenden Erscheinungsformen (IaaS, PaaS und SaaS).³³

1. Infrastrukturebene

Die Infrastrukturebene ist die physische Grundlage der Cloud Computing Architektur. Im Kern besteht sie aus auf der ganzen Welt verteilten Rechenzentren, die mit Hochleistungsservern, Speicherarrays und Netzwerkgeräten ausgestattet sind.³⁴ Diese physischen Komponenten sind redundant ausgelegt. Das bedeutet, dass die Systeme aus zusätzlichen, gleichartigen Hardwarekomponenten bestehen, die bei einem Ausfall sofort einspringen können.³⁵ In der Cloud-Infrastruktur heißt das: Wenn ein Teil (z. B. ein Server, eine Festplatte, ein Stromversorgungsgerät oder ein Netzwerkanschluss) ausfällt, übernimmt ein identisches, parallel bereitgestelltes Ersatzsystem sofort dessen Aufgabe. So wird sichergestellt, dass der Betrieb weiterläuft und keine Daten oder Dienste verloren gehen.³⁶

2. Virtualisierungsebene

Diese nativen Hardwareressourcen werden in einem ersten Schritt durch eine Software (den sog. Hypervisor) virtualisiert.³⁷ Durch die Basistechnologie der Virtualisierung können mehrere Hardwareressourcen als eine einzige große virtuelle Ressource erscheinen (sog. Aggregation) oder umgekehrt eine große reale Hardwareressource als mehrere kleine individuelle Ressourcen (sog. Partitionierung).³⁸

³⁰ Siehe hierzu S. 6.

³¹ Siehe hierzu S. 6.

³² Siehe hierzu S. 8.

³³ Siehe hierzu S. 8.

³⁴ *Hennrich*, Cloud Computing nach der DSGVO, S. 25f.

³⁵ *Vaquero/Rodero-Merino/Caceres/Lindner*, ACM SIGCOMM 2009, 50 (53).

³⁶ *Armbrust/Fox/Griffith/Joseph/Katz/Konwinski/Lee/Patterson/Rabkin/Stoica/Zahria*, Communication of the ACM 2010, 50 (53).

³⁷ *Matros*, Cloud Computing IT-Dienstleister, S. 35.

³⁸ *Lehmann/Giedke*, CR 2013, 608 (611).

Je nachdem, welche Hardware-Ressource virtualisiert wird, spricht man von virtuellem Volume (bei virtualisierten Speichern), virtuellen Maschinen (bei virtualisierter Rechenleistung) oder von virtuellen Switches (kurz: vSwitches).³⁹ Virtualisierung ermöglicht somit die Abstraktion physischer Hardware in logische Einheiten. Der Hypervisor⁴⁰ fungiert hierbei als Softwareschicht zwischen der physischen Hardware und den virtuellen Maschinen. Er übernimmt die Verwaltung und Zuteilung von Rechenressourcen wie CPU, Arbeitsspeicher und Festspeicher an die einzelnen virtuellen Maschinen.⁴¹ Moderne Hypervisor-Technologien arbeiten nach dem Prinzip der Ressourcenabstraktion und erstellen für jede virtuelle Maschine eine isolierte Umgebung. Durch diese Isolation können verschiedene Betriebssysteme gleichzeitig auf derselben physischen Hardware ausgeführt werden, ohne sich gegenseitig zu beeinträchtigen.⁴² Der Hypervisor ordnet physischen Speicherblöcken virtuelle Speicheradressen zu und sorgt dafür, dass jede virtuelle Maschine nur auf ihren eigenen Speicherbereich zugreifen kann.⁴³ Diese strikte Trennung bildet die Grundlage für das sog. Pooling. Hierbei werden die physischen Ressourcen – wie Rechenleistung, Speicher und Netzwerk – zu einem gemeinsamen Pool zusammengefasst, aus dem virtuelle Maschinen und Anwendungen je nach Bedarf dynamisch bedient werden.⁴⁴ Ein solches Pooling macht jedoch eine konsequente Mandantentrennung (Multi-Tenancy) erforderlich, da mehrere Kunden dieselbe Infrastruktur und oft auch dieselbe Softwareinstanz nutzen, während ihre Daten und Anwendungen logisch voneinander isoliert bleiben müssen. Diese Mandantentrennung ist zwingend notwendig, um sicherzustellen, dass jeder Nutzer ausschließlich Zugriff auf seine eigenen Daten und Ressourcen hat und keine unbeabsichtigten oder unberechtigten Zugriffe auf die Daten anderer Mandanten möglich sind.⁴⁵ Neben virtuellen Maschinen spielen Containertechnologien eine immer größere Rolle in modernen Cloud Computing Architekturen.⁴⁶ Container sind eine besonders schlanke Form der Virtualisierung. Sie enthalten nur die Anwendung und alle notwendigen Abhängigkeiten, teilen sich

³⁹ Siehe hierzu Abbildung auf S. 55.

⁴⁰ Teilweise auch als Virtual Machine Monitor [VMM] bezeichnet, *Kohne*, Cloud-Föderationen, S. 2.

⁴¹ *Hennrich*, Cloud Computing nach der DSGVO, S. 24; *Tanenbaum/Bos*, Modern Operating Systems, S. 477f.; *Kohne*, Cloud-Föderationen, S. 21.

⁴² *Matros*, Cloud Computing IT-Dienstleister, S. 35; vgl. *Lisdorf*, Grundlagen des Cloud Computing, S. 134f.; *Liu/Tong/Mao/Bohn/Messina/Badger/Leaf*, NIST Cloud Computing Reference Architecture, S. 13.

⁴³ *Hennrich*, Cloud Computing nach der DSGVO, S. 28; *Schorer*, in: Hilber, HdB Cloud Computing, S. 70f.

⁴⁴ *Schorer*, in: Hilber, HdB Cloud Computing, S. 70.

⁴⁵ *Schorer*, in: Hilber, HdB Cloud Computing, S. 72; *Kremer*, in: Borges/Meents, § 1 Rn, 33.

⁴⁶ *Hennrich*, Cloud Computing nach der DSGVO, S. 30.

aber den Kernel (also den Kern) des Host-Betriebssystems.⁴⁷ Die Erstellung dieser Container erfolgt softwarebasiert. Die wohl bekannteste freie Software zur Containervisualisierung ist Docker.⁴⁸

3. Orchestrierungsebene

Während der Hypervisor für die Virtualisierung und direkte Kontrolle der physischen Hardwareressourcen zuständig ist, dient die dritte softwarebasierte⁴⁹ Ebene dazu, die verschiedenen virtuellen Ressourcen sinnvoll zu verwalten. Sie sorgt dafür, dass Container oder virtuelle Maschinen automatisch bereitgestellt, skaliert, gestartet oder gestoppt werden, je nachdem, wie viel Rechenleistung oder Ressourcen gerade benötigt werden.⁵⁰

4. Serviceebene

Die Serviceebene der Cloud-Computing-Architektur stellt die virtualisierten Ressourcen sodann als flexibel konsumierbare Dienste bereit und abstrahiert die darunterliegenden Schichten.⁵¹ Nutzer erhalten von dem Anbieter des Cloud-Dienstes (Cloud Service Provider) Infrastrukturleistungen (IaaS⁵²), Softwareanwendungen (SaaS⁵³) oder Entwicklungsumgebungen (PaaS⁵⁴), die ortsunabhängig nutzbar sind. IaaS-Dienste umfassen dabei die Bereitstellung skalierbarer Rechenleistung und Speicher durch Cloud Service Provider wie AWS oder Azure. Im SaaS-Modell betreiben Cloud Service Provider Software zentral und stellen sie per Internet zur Verfügung. Spezielle SaaS-Diensten für die anwaltliche Praxis sind etwa Kanzlei-Software oder KI-Dokumentenanalysetools. Aber auch allgemeine Tools, wie Videokonferenz- und Kollaborationslösungen sind i.d.R. SaaS-Dienste und werden in der anwaltlichen Praxis verwendet.⁵⁵

⁴⁷ Dadurch sind Container wesentlich ressourcenschonender und schneller als klassische virtuelle Maschinen. Sie ermöglichen es, Anwendungen – *stateless* – zu betreiben, solange der Kernel kompatibel ist, vgl. *Mouat*, Docker, S. 3ff; *Schenker*, Learn Docker, S. 11ff.; *Hennrich*, Cloud Computing nach der DSGVO, S. 30.

⁴⁸ *Hennrich*, Cloud Computing nach der DSGVO, S. 30; Software Docker: <https://www.docker.com/company/> (zuletzt abgerufen am 27.07.2025).

⁴⁹ Bekannte Softwaretools für diese Orchestrierung sind Kubernetes für Container oder OpenStack für virtuelle Maschinen, *Hennrich*, Cloud Computing nach der DSGVO, S. 30.

⁵⁰ *Abdalla/Rashid*, in: Hashim/Ahmed/Khalifa/Saeed, Cloud Computing's Transformative Power, S. 17; *Hennrich*, Cloud Computing nach der DSGVO, S. 30.

⁵¹ *Liu/Tong/Mao/Bohn/Messina/Badger/Leaf*, NIST Cloud Computing Reference Architecture, S. 13.

⁵² Infrastructure as a Service, *Krcmar*, in: Borges/Meents, Cloud Computing, § 2 Rn. 20.

⁵³ Software as a Service, *Krcmar*, in: Borges/Meents, Cloud Computing, § 2 Rn. 31.

⁵⁴ Plattform as a Service, *Krcmar*, in: Borges/Meents, Cloud Computing, § 2 Rn. 25.

⁵⁵ Vgl. *Zunker*, Die Kanzlei in der Cloud, AnwBl. Digital v. 07.07.2023, abrufbar unter: <https://anwaltsblatt.anwaltverein.de/de/themen/kanzlei-praxis/cloud-kanzlei> (zuletzt abgerufen am 24.06.2026).

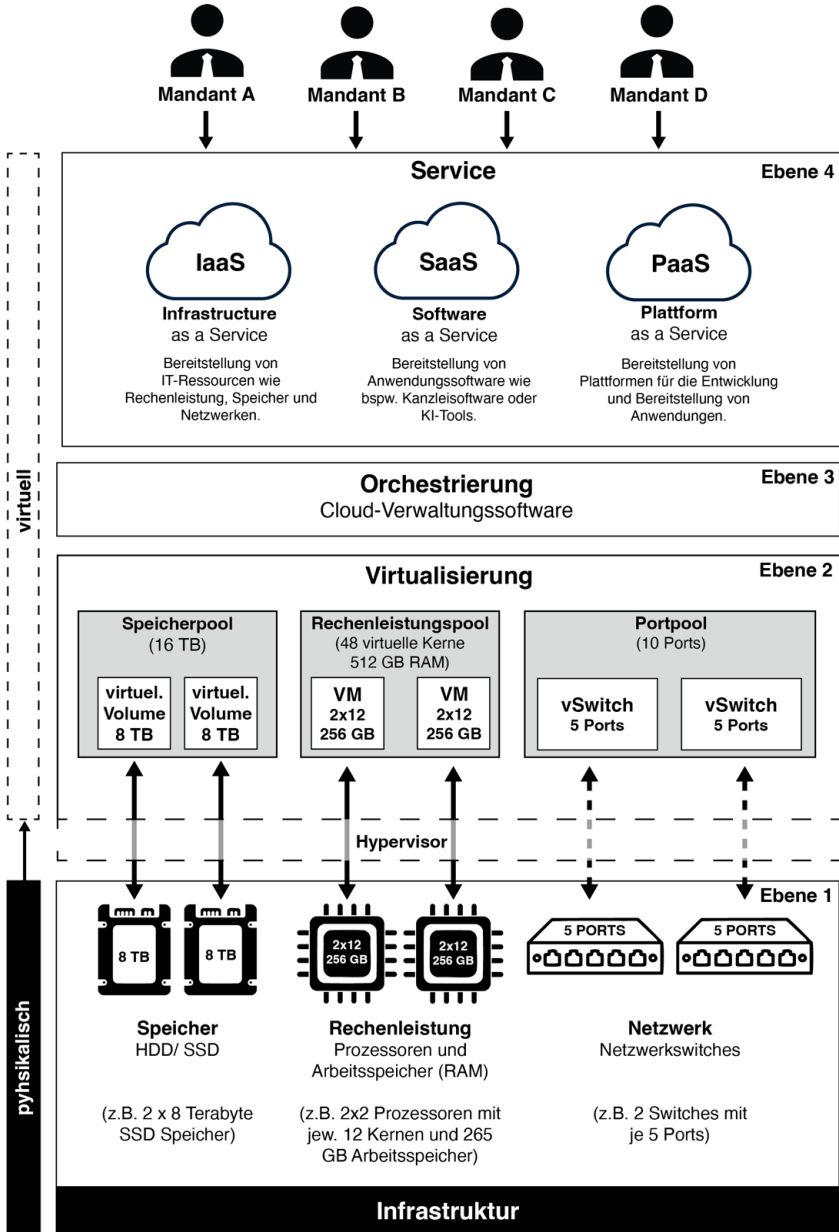


Abbildung: Vier Ebenen des Cloud-Computing-Modells (vereinfacht)⁵⁶

⁵⁶ Angelehnt an: Schorer, in: Hilber, HdB Cloud Computing, S. 67.

C. Geheimnis- und datenschutzrechtliche Anforderungen

Der Anwalt ist gem. § 43a Abs. 2 S. 1 BRAO zur Verschwiegenheit verpflichtet. Dieses Anwaltsgeheimnis bildet den Kern der Vertrauensbeziehung zwischen Rechtsanwalt und Mandant und ist eine der tragenden Säulen des Anwaltsberufs.⁵⁷ Die Funktion der Verschwiegenheitspflicht besteht insbesondere in der Gewährleistung einer vertrauensvollen Kommunikation. Eine solche ist für eine sachgerechte Rechtsberatung und -vertretung unerlässlich. Nur wenn der Mandant darauf vertrauen kann, dass seine Mitteilungen vertraulich behandelt werden, wird er dem Rechtsanwalt alle für die Mandatsführung relevanten Informationen offenbaren.⁵⁸ Verletzt der Rechtsanwalt seine Verschwiegenheitspflicht, steht neben anwaltsgerichtlichen Maßnahmen (§ 113 Abs. 1 i.V.m. § 114 Abs. 1 BRAO) eine strafrechtliche Verantwortlichkeit im Raum (§ 203 Abs. 1 Nr. 3 StGB).

I. Gegenstand und Reichweite der Verschwiegenheitspflicht

In sachlicher Hinsicht bezieht sich die Verschwiegenheitspflicht auf „alles“, was dem Anwalt in Ausübung seines Berufes bekannt geworden ist (§ 43a Abs. 2 S. 2 BRAO). Dazu zählt neben der Identität des Mandanten bereits die Tatsache, dass überhaupt ein Mandatsverhältnis besteht.⁵⁹ Darüber hinaus sind sämtliche Details des zugrundeliegenden Sachverhalts grds. geschützt.⁶⁰ Dies betrifft bspw. die persönlichen und wirtschaftlichen Verhältnisse⁶¹ des Mandanten, steuerliche Informationen, den getätigten Schriftwechsel, Strategieüberlegungen oder rechtliche Bewertungen. Aber auch Informationen über Dritte und selbst interne Abläufe innerhalb der Kanzlei können – soweit sie das Mandat betreffen – von der Verschwiegenheitspflicht umfasst sein.⁶² Sie gilt im Außenverhältnis gegenüber jedermann und zeitlich unbegrenzt, wirkt mithin auch nach Beendigung des Mandats fort (§ 2 Abs. 1 S. 2 BORA).⁶³

⁵⁷ Henssler, AnWB 2019, 216; Bauckmann, in: Feuerich/Weyland, BRAO, § 43a Rn. 12; Peitscher, Anwaltsrecht, § 18 Rn. 11; BVerfG, Beschl. v. 14-07-1987 - 1 BvR 537/81, NJW 1988, 191.

⁵⁸ Henssler, AnWB 2019, 216; ders., in: Henssler/Prütting, BRAO, § 43a Rn. 58; Kleine-Cosack, BRAO, § 43a Rn. 5.

⁵⁹ BGH, Urt. v. 17.05.1995 – VIII ZR 94/94, NJW 1995, 2026; Peitscher, Anwaltsrecht, § 18 Rn. 14; Henssler, in: Henssler/Prütting, BRAO, § 43a Rn. 62f.

⁶⁰ Peitscher, Anwaltsrecht, § 18 Rn. 14.

⁶¹ AG Hamm, Urt. v. 02.02.2018 – 2 AGH 12/17, NJW-RR 2018, 632.

⁶² Peitscher, Anwaltsrecht, § 18 Rn. 14.

⁶³ Peitscher, Anwaltsrecht, § 18 Rn. 20, 21; Henssler, in: Henssler/Prütting, BRAO, § 43a Rn. 79; Kleine-Cosack, BRAO, § 43a Rn. 66.

Maßgeblich ist gleichwohl, dass der Anwalt die Kenntnis im Rahmen seiner beruflichen Tätigkeit – also nicht privat⁶⁴ – erlangt hat und es sich nicht um offenkundige bzw. unbedeutende Tatsachen handelt (§ 43 Abs. 2 S. 3 BRAO).⁶⁵ Offenkundig ist eine Tatsache, wenn verständige und erfahrene Menschen sie per se kennen oder sich jederzeit und ohne Schwierigkeiten aus allgemein zugänglichen Quellen Kenntnis von ihr verschaffen könnten.⁶⁶ Hierzu zählen etwa Informationen, die Gegenstand einer öffentlichen Gerichtsverhandlung waren.⁶⁷ Handelt es sich um eine Information, die nach subjektiver Bewertung des Mandanten belanglos ist (Bagatelle), so erstreckt sich die anwaltliche Verschwiegenheitspflicht auf diese unbedeutende Tatsache ebenfalls nicht.⁶⁸

Der sachliche Anwendungsbereich des § 43a Abs. 2 BRAO entspricht dem strafrechtlichen Schutz des Privatgeheimnisses (§ 203 StGB), nach dem eine Tatsache nur dann ein fremdes Geheimnis darstellt, wenn sie nicht offenkundig ist, also einem lediglich beschränkten Personenkreis bekannt und ein berechtigtes und schutzwürdiges Interesse beinhaltet, das nach dem Willen des Betroffenen geheim zu halten ist.⁶⁹ Der objektive Tatbestand des § 203 Abs. 1 Nr. 3 StGB und die berufsrechtlichen Anforderungen an die anwaltliche Verschwiegenheit aus § 43a Abs. 2 BRAO und § 2 BORA laufen insoweit synchron.⁷⁰

II. Verbotswidriges Offenbaren

Seine Verschwiegenheitspflicht verletzt der Geheimnisträger, wenn er geschützte Tatsachen rechtswidrig offenbart. Ein solches verbotswidriges Offenbaren liegt vor, wenn der Anwalt es ermöglicht, dass ein Dritter von einer geheim zu haltenden Tatsache erfährt, die diesem bisher nicht oder zumindest nicht mit Sicherheit bekannt ist und nach dem Wunsch des Betroffenen auch ggü. diesem Dritten geheim zu halten war.⁷¹ Eine verbotswidrige Preisgabe setzt jedoch eine jedenfalls mittelbar

⁶⁴ Vgl. *Henssler*, in: *Henssler/Prütting*, BRAO, § 43a Rn. 72.

⁶⁵ *Peitscher*, *Anwaltsrecht*, § 18 Rn. 15.

⁶⁶ EGStGB BT-Dr 7/550, S. 242; BGH, Urt. v. 08.10.2002 – 1 StR 150/02, NJW 2003, 226 (227); *Peitscher*, *Anwaltsrecht*, § 18 Rn. 16; *Henssler*, in: *Henssler/Prütting*, BRAO, § 43a Rn. 75.

⁶⁷ BGH, Urt. v. 14.11.1963 – III ZR 19/63, BGHZ 40, 288 (292) = NJW 1964, 449 (450); *Henssler*, in: *Henssler/Prütting*, BRAO, § 43a Rn. 75 mwN.

⁶⁸ *Henssler*, in: *Henssler/Prütting*, BRAO, § 43a Rn. 77; *Gasteyer*, in: *Hartung/Scharmer/Holl*, BORA, § 2 Rn. 55.

⁶⁹ BGH, Urt. v. 10.05.1995 – 1 StR 764/94, BGHSt 41, 140 (142); *Cierniak/Niehaus*, in: *MüKo-StGB*, § 203 Rn. 13.

⁷⁰ *Peitscher*, *Anwaltsrecht*, § 30 Rn. 107.

⁷¹ *Kleine-Cosack*, BRAO, § 43a Rn. 66; *Peitscher*, *Anwaltsrecht*, § 18 Rn. 22; *Cornelius*, StV 2016, 380; *Henssler*, in: *Henssler/Prütting*, BRAO, § 43a Rn. 79ff.; *Weidemann*, in: *BeckOK-StGB*, § 203 Rn. 34ff.

mögliche Identifizierung des Mandanten voraus. Teilt der Anwalt Tatsachen einem Dritten mit, ohne den Namen des Mandanten zu nennen und ohne eine Identifizierung aufgrund der im Einzelfall mitgeteilten Informationen zu ermöglichen, so scheidet ein verbotswidriges Offenbaren sowohl berufs- als auch strafrechtlich aus.⁷² Strafbar macht sich der Rechtsanwalt nur dann, wenn er seine Verschwiegenheitspflicht vorsätzlich verletzt hat. § 203 StGB setzt mindestens dolus eventualis voraus.⁷³ Positives Tun ist hingegen nicht erforderlich. Eine Verletzung des Geheimnisschutzes kann aufgrund der Garantenstellung des Berufsgeheimnisträgers auch durch ein Unterlassen erfolgen (§§ 203, 13 StGB).⁷⁴ § 43a Abs. 2 BRAO enthält kein subjektives Element. Ein fahrlässiges Offenbaren ist damit ausschließlich zivil- und berufsrechtlich relevant.⁷⁵

In der straf-, wie auch in der berufsrechtlichen Literatur ist weiterhin umstritten, ob ein Offenbaren i.S.d. § 203 StGB bzw. § 43a Abs. 2 BRAO eine tatsächliche Kenntniserlangung der geschützten Tatsache voraussetzt oder ob es ausreicht, wenn der Anwalt die bloße Möglichkeit einer Kenntniserlangung durch Dritte geschaffen hat (Offenbarungsgefahr).⁷⁶ Übertragen auf das Cloud-Computing stellt sich die Frage, ob der Anwalt seine Verschwiegenheitspflicht bereits dann verletzt, wenn die (technische) Möglichkeit besteht, dass der Cloud Service Provider bzw. dessen Vertragspartner von geschützten Tatsachen Kenntnis erlangen könnten.

Mit Ausnahme von *Henssler*⁷⁷ und *Kleine-Cosack*⁷⁸ wird in der berufsrechtlichen Literatur eine tatsächliche Kenntniserlangung für ein fahrlässiges Offenbaren überwiegend nicht vorausgesetzt und § 43a Abs. 2 BRAO insoweit als Gefährdungstatbestand verstanden.⁷⁹ Auch in der strafrechtlichen Literatur finden sich Stimmen, die eine Offenbarungsgefahr für ausreichend erachten.⁸⁰ Jedenfalls im Kontext der für das Cloud Computing relevante Einbeziehung sonstiger mitwirkender Personen

⁷² *Weiss*, in: Hilber, HdB Cloud Computing, S. 25; *Peitscher*, Anwaltsrecht § 18 Rn. 23; *Cornelius*, StV 2016, 380 (383f.); *Barnitzke/Bock*, GRUR-Prax 2025, 415.

⁷³ *Weidemann*, in: BeckOK-StGB, § 203 Rn. 50.

⁷⁴ *Cierniak/Niehaus*, in: MüKo-StGB, § 203 Rn. 58; *Bosch*, in: Schönke/Schröder, StGB, § 13 Rn. 31.

⁷⁵ *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 82; *Kleine-Cosack*, BRAO, §43a Rn. 36.

⁷⁶ *Peitscher*, Anwaltsrecht, § 18 Rn. 24 mwN.

⁷⁷ *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 82.

⁷⁸ *Kleine-Cosack*, BRAO, §43a Rn. 36.

⁷⁹ So: *Kilian*, in: Kilian/Koch, Rn. 893; *Peitscher*, Anwaltsrecht, § 18 Rn. 24 a.A. *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 82; *Kleine-Cosack*, BRAO, §43a Rn. 36.

⁸⁰ *Fischer*, StGB, § 203 Rn. 35; *Heger*, in: Lackner/Kühl/Heger, StGB, § 203 Rn. 17; zum Streitstand im Zusammenhang des Cloud Computing vor der Novellierung des § 203 StGB: *Cornelius*, StV 2016, 380 (382f.) m.w.N.

nach § 203 Abs. 3 S. 2 StGB hat sich der Gesetzgeber diesbezüglich klar positioniert. Die Begründung des Gesetzes zur Neuregelung des Geheimnisschutzes⁸¹ stellt ausdrücklich fest, „dass ein Offenbaren bereits dann gegeben ist, wenn die *Möglichkeit* der Kenntnisnahme von Geheimnissen besteht. Eine tatsächliche Kenntnisnahme ist insoweit nicht erforderlich.“⁸² Aufgrund des weitgehenden Gleichlaufs der Tatbestände ist diese gesetzgeberische Wertung auf die berufsrechtlichen Vorschriften (§ 43a Abs. 2 StGB, § 2 BORA) zu übertragen.⁸³ Für die aufgeworfene Frage der anwaltlichen Nutzung von Cloud Computing-Diensten bedeutet dies, dass bereits in der bloßen Zugänglichmachung von geheimnisschutzrelevanten Daten dem Grunde nach ein straf- und berufsrechtlich verbotenes Offenbaren liegt.⁸⁴ Eine tatsächliche Kenntnisnahme durch Mitarbeiter des Cloud Service Providers ist mithin nicht erforderlich.

III. Offenbarungsrisiken und Anforderungen an die anwaltliche Nutzung

Damit fordern § 43a Abs. 2 BRAO und § 203 StGB bei der Nutzung cloudbasierter Dienste zunächst eine technische Lösung zur Sicherstellung der anwaltlichen Verschwiegenheitspflicht. Denn der Geheimnisschutz setzt auf einer ersten Ebene voraus, dass der Cloud Service Provider bereits technisch keine Möglichkeit hat, auf die geschützten Informationen zugreifen zu können. Da dies in der Praxis jedoch derzeit nicht bei jedem Serviceangebot umsetzbar ist bzw. angeboten wird und selbst bei entsprechender Umsetzung weiterhin ein – ggf. erhebliches – Offenbarungsrisiko verbleibt⁸⁵, eröffnen sowohl die berufsrechtlichen Vorschriften (§§ 43a Abs. 2, 43e BRAO, § 2 BORA) als auch die Strafnorm des § 203 StGB (siehe § 203 Abs. 3 StGB) die Möglichkeit der Zugangseröffnung ggü. dem Cloud Service Provider. Diese rechtliche Lösung wurde mit dem Gesetz zur Neuregelung des Geheimnisschutzes erstmalig u.a. mit Blick auf die Möglichkeit zur anwaltlichen Nutzung von auf cloudbasierten Diensten geschaffen.⁸⁶

1. Technische Schutzverfahren und risikoadäquate Organisation

Technisch können Verschlüsselungsverfahren ein Offenbaren geschützter Informationen vermeiden und damit den Geheimnisschutz auf einer ersten Ebene

⁸¹ Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen v. 30.10.2017, BGBl. I, S. 3618.

⁸² BT Drs. 18/11936 S. 28 (zu § 203 Abs. 3 S. 2 StGB-E), Hervorhebung durch Verfasser.

⁸³ So auch *Henssler*, in: *Henssler/Prütting*, BRAO, § 43e BRAO Rn. 7.

⁸⁴ *Cornelius*, StV 2016, 380 (382).

⁸⁵ Hierzu sogleich S. 14f.

⁸⁶ *Hartung*, in: *Hilber, HdB Cloud Computing*, Teil 8D Rn. 35ff.; *Cornelius*, StV 2016, 380 (384).

sicherstellen.⁸⁷ Dies ist jedenfalls bei solchen Diensten das Mittel der Wahl, bei denen ein Mitlesen der geschützten Daten durch den Cloud Service Provider zur Bereitstellung des Serviceangebotes nicht notwendig ist.⁸⁸ Etwa bei der Nutzung von Cloud-Infrastruktur (IaaS) – wie Cloud-Speichern – kann dies der Fall sein, da im Kern eine Bereitstellung von Speicherplatz Gegenstand des Dienstes ist.⁸⁹ Technisch ist hierbei jedoch sicherzustellen, dass die Daten sowohl bei der Übertragung als auch bei der Speicherung in der Cloud (etwa mittels Ende-zu-Ende-Verschlüsselung [E2EE]) verschlüsselt sind.⁹⁰ Diese Verschlüsselung darf sich nicht nur auf den Dateiinhalt beschränken, sondern muss sich auch auf die Dateinamen und Metadaten⁹¹ erstrecken. Weist bspw. die Dateibezeichnung einen Mandantenbezug auf oder finden sich solche Informationen in den Metadaten, etwa weil eine Datei in einem Ordner gespeichert wurde, der den Namen des Mandanten trägt und daher in den Metadaten als Speicherort (Pfad) unverschlüsselt einzusehen ist, steht eine Verletzung der Verschwiegenheitspflicht im Raum.⁹²

Eine Verschlüsselung der Dateibezeichnung und Metadaten ist jedoch nicht bei jedem IaaS-Anbieter standardmäßig gegeben, da sie teilweise zur Verwaltung und zum Betrieb des Speicherdienstes genutzt werden.⁹³ Diesem Risiko kann der Anwalt durch eine eigene Verschlüsselung und/oder Pseudonymisierung⁹⁴ der Informationen begegnen.⁹⁵

⁸⁷ *Gasteyer/Säljemar*, NJW 2020, 1768 (1770f.).

⁸⁸ *Cornelius*, StV 2016, 380 (384).

⁸⁹ *Barnitzke/Bock*, GRUR-Prax 2025, 415; *Hartung*, in: Hilber, HdB Cloud Computing, Teil 8D Rn. 38.

⁹⁰ *Cornelius*, StV 2016, 380 (384).

⁹¹ *Kroschwald*, ZD 2014, 75 (80).

⁹² Bereits die Information, dass ein Mandatsverhältnis möglicherweise besteht, ist eine nach § 203 StGB und § 43a Abs. 2 BRAO geschützte Tatsache; siehe zum sachlichen Schutzbereich der Verschwiegenheitspflicht, BGH, Urt. v. 17.05.1995 – VIII ZR 94/94, NJW 1995, 2026, hierzu auch S. 10.

⁹³ Anbieter wie bspw. TeamDrive bewerben ihr IaaS-Angebot explizit mit der Sicherheitszusage einer Verschlüsselung der Metdaten, siehe <https://teamdrive.com/blog-de/metadaten-in-der-cloud/> (zuletzt abgerufen am 24.04.2026); AWS bietet die Möglichkeit neben den Inhalten auch die Metadaten mithilfe eines AES-256-Verschlüsselungsalgorithmus nach Industriestandard zu verschlüsseln; Diese Funktion muss jedoch aktiviert werden, vgl. AWS-Whitepaper, Verschlüsseln von Dateidaten mit Amazon Elastic File System, abrufbar unter: https://docs.aws.amazon.com/de_de/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-at-rest.html#:~:text=AWS%20bietet%20Ihnen%20die%20Tools%20zum%20Erstellen,Meta-daten%20mithilfe%20eines%20AES%20256%2DVerschlüsselungsalgorithmus%20nach%20Industriestandard%20verschlüsselt (zuletzt abgerufen am 24.04.2026).

⁹⁴ Zum Begriff der Pseudonymisierung vgl. Art. 4 Nr. 5 DSGVO.

⁹⁵ *Hartung*, in: Hilber, HdB Cloud Computing, Teil 8D Rn. 35ff.

Bei SaaS-Diensten gibt es oftmals keine technische Möglichkeit zur Sicherstellung des Geheimnisschutzes.⁹⁶ Zwar liegen die seitens des nutzenden Anwalts bereitgestellten Daten und Informationen auf der Infrastrukturebene (also dem IaaS-Anbieter) ebenfalls verschlüsselt. Der Cloud Service Provider, der seinen SaaS-Dienst dem Anwalt (etwa in Form cloudbasierter Kanzleisoftware) zur Verfügung stellt, ist jedoch im Besitz der Schlüssel und hat damit Zugriff auf geschützte Informationen. Diese Zugriffsmöglichkeit ist in einem bestimmten Umfang auch notwendig, da der Cloud Service Provider zur Bereitstellung seines SaaS-Services Zugriff auf bestimmte geschützte Informationen zwingend benötigt.⁹⁷ Im Verhältnis zwischen SaaS-Anbieter und Mandant ist daher eine – jedenfalls vollumfängliche – Verschlüsselung regelmäßig nicht möglich. Zwar existieren Modelle wie die Fully Homomorphic Encryption (FHE), die eine Berechnung verschlüsselter Daten ermöglichen soll, ohne diese zuvor entschlüsseln zu müssen, jedoch ist dieser technische Durchbruch von einem flächendeckenden Einsatz noch weit entfernt.⁹⁸

2. Rechtliche Lösung (Erlaubtes Offenbaren)

Bedingt durch diese teilweise nur eingeschränkten technischen Möglichkeiten zur Wahrung des Geheimnisschutzes kommt der rechtlichen Lösung bei der anwaltlichen Nutzung cloudbasierter Serviceangebote eine maßgebliche Rolle zu. Der nach alter Rechtslage diskutierten Frage, ob die Nutzung von Cloud Computing Diensten grds. eine von der Allgemeinheit gebilligte Verhaltensweise im sozialen Leben darstellt und aufgrund dieser Sozialadäquanz kein Verstoß gegen die Verschwiegenheitspflicht bei der Nutzung gegeben ist, ist mit der Einführung des § 43e BRAO durch das Gesetz zur Neuregelung des Geheimnisschutzes⁹⁹ die Grundlage entzogen. Entsprechend verweist § 2 Abs. 4 lit. c) BORA de lege lata auf solche Arbeitsabläufe der Kanzlei, die außerhalb des Anwendungsbereichs des § 43e BRAO liegen.¹⁰⁰

Als rechtliche Lösung sind damit die Entbindung des Anwaltes von der Schweigepflicht und/oder eine vertragliche Erweiterung des Geheimnisschutzes entsprechend den berufs- und strafrechtlichen Anforderungen (§ 43e BRAO. § 203 Abs. 3 StGB)

⁹⁶ *Hartung*, in: Hilber, HdB Cloud Computing, Teil 8D Rn. 38.

⁹⁷ *Cornelius*, StV 2016, 380 (384); *Hartung*, in: Hilber, HdB Cloud Computing, Teil 8D Rn. 38.

⁹⁸ *Deusch/Eggendorfer*, in: Taeger/Pohle, HdB Computerrecht, 50.1 Rn. 182 ff; vgl. auch *baffle*, Why Is Homomorphic Encryption Not Ready For Primetime?, abrufbar unter: <https://baffle.io/blog/why-is-homomorphic-encryption-not-ready-for-primetime/> (zuletzt abgerufen am 24.06.2026).

⁹⁹ Siehe Fn. 81.

¹⁰⁰ Zur Sozialadäquanz nach § 2 BORA nach altem Recht: *Cornelius*, StV 2016, 380.

möglich. Hierbei spielen auch datenschutzrechtliche Implikationen der Nutzung cloudbasierter Dienste eine maßgebliche Rolle.¹⁰¹

a) Einwilligung

Einer Verletzung der Verschwiegenheitspflicht durch die anwaltliche Nutzung von Cloud-Services kann durch eine Einwilligung¹⁰² des Mandanten verhindert werden, indem sich der Anwalt die Befugnis zur Zugangseröffnung gegenüber dem Cloud Service Provider erteilen lässt (Entbindung von der Schweigepflicht).¹⁰³ Als Träger des höchstpersönlichen Rechtsguts steht dem Mandanten die Dispositionsbefugnis über seine Geheimnisse zu.¹⁰⁴ Die Einwilligung kann ausdrücklich oder konkludent erfolgen.¹⁰⁵ Ein Formerfordernis besteht hierfür weder nach Straf- noch nach Berufsrecht.¹⁰⁶

bb) Konkludente Einwilligung

Im Kontext internetbasierter Kommunikation wird eine konkludente Einwilligung angenommen, wenn der Mandant selbst die elektronische Kommunikation – bspw. per E-Mail – initiiert oder fortsetzt, nachdem der Anwalt ihn zumindest allgemein auf die bestehenden Risiken hingewiesen hat (§ 2 Abs. 2 S. 6 BORA).¹⁰⁷ Auch bei der Nutzung von Cloud Computing Diensten ist eine Einwilligung durch mandantenseitige Eröffnung des digitalen Kommunikationsweges denkbar. Allerdings

¹⁰¹ Siehe hierzu S. 21f.

¹⁰² Ob es sich bei der vorherigen Zustimmung des Betroffenen um eine rechtfertigende Einwilligung handelt oder um ein tatbestandsausschließendes Einverständnis ist umstritten; sich für ein tatbestandsausschließendes Einverständnis aussprechend: OLG Köln, NJW 1962, 686; *Eisele*, in: Schönke/Schröder, § 203, Rn. 29; *Cierniak/Niehaus*, in: MüKo-StGB § 203 Rn. 57; *Wiedemann*, in: BeckOK-StGB § 203, Rn. 38; *Gasteyer* in: Scharmer/Hartung/Holl, BORA, § 2 Rn. 27; für die Einordnung als rechtfertigende Einwilligung plädierend: OLG Köln NJW 2000, 3656 (3657), *Heger*; in: *Lackner/Kühl/Heger*, Vorbm. § 201, Rn. 2; Für die gegenständliche Frage ist dies insoweit unbeachtlich, als dass in beiden Fällen eine Strafbarkeit nach § 203 StGB ausgeschlossen ist; Zum Streitstand im Kontext des § 203 StGB: *Cierniak/Niehaus*, in: MüKo-StGB, § 203 Rn. 63 m.w.N.

¹⁰³ *Hartung*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 11.4.2 Rn. 125.; *Cierniak/Niehaus*, in: MüKo-StGB, § 203 Rn. 57ff; Zu den allgemeinen Anforderungen der Einwilligung im datenschutzrechtlichen Kontext des Cloud Computing: *Borges*, in: Borges/Meents, Cloud Computing, § 8 Rn. 2ff;

¹⁰⁴ *Cornelius*, StV 2016, 380 (384).

¹⁰⁵ *Fischer*, StGB, § 203 Rn. 66; *Hartung*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 11.4.2 Rn. 126.

¹⁰⁶ *Hartung*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 11.4.2 Rn. 126.

¹⁰⁷ *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 92; *Bauckmann*, in: Feuerich/Weyland, BRAO, § 43a Rn. 25b.

setzt die Wirksamkeit einer konkludenten Einwilligung voraus, dass dem Mandanten das Risiko einer möglichen Kenntnisnahme geschützter Informationen durch Dritte bewusst ist.¹⁰⁸ Während dieses Bewusstsein im Falle einer E-Mail-Kommunikation als gesellschaftlich anerkannte elektronische Entsprechung der klassischen Briefpost unterstellt werden kann¹⁰⁹, ist es bei (anderen) Cloud Services – insbesondere bei komplexeren Service-Modellen wie SaaS – deutlich weniger selbstverständlich. Stellt der Anwalt seine Internetpräsenz bspw. über einen klassischen Hosting-Service (IaaS) bereit und ermöglicht diese Webseite mittels eines Formulars eine Kontaktaufnahme, wird dem durchschnittlichen Nutzer nicht bewusst sein, dass es – im Falle einer unverschlüsselten Übermittlung – zu einer Kenntnisnahme geschützter Informationen durch den IaaS-Anbieter kommen könnte. Noch undurchsichtiger ist die Lage bei der Nutzung von SaaS-Diensten (wie z.B. Webseiten-Baukastenlösungen). Hier wird dem Mandanten zumeist verborgen bleiben, dass die Webseite des Anwalts über einen externen SaaS-Anbieter betrieben wird und ggü. welchen Akteuren eine Offenbarungsgefahr besteht. Eine konkludente Einwilligung wird bei cloudbasierten Diensten daher regelmäßig nicht anzunehmen sein.

cc) *Ausdrückliche Einwilligung*

Die Komplexität moderner Cloud-Computing-Architekturen¹¹⁰ stellt auch an die Wirksamkeit einer ausdrücklichen Einwilligung hohe Anforderungen. Damit der Ratsuchende bzw. Mandant wirksam über sein Rechtsgut disponieren kann, muss er die Tragweite und Bedeutung seiner Entscheidung erfassen können (Einsichts- und Urteilsfähigkeit).¹¹¹ Dies setzt eine zumindest grundlegende Aufklärung durch den Anwalt über die Funktionsweise des eingesetzten Cloud-Dienstes und der beteiligten Akteure voraus. Sie muss den Mandanten befähigen, sein Selbstbestimmungsrecht angemessen wahrzunehmen. Nur ein ordnungsgemäß aufgeklärter Nutzer kann wirksam einwilligen.¹¹² Erfolgt diese Aufklärung und Entbindung von der Schweigepflicht formularmäßig, ist – mit Blick auf § 305c BGB und eine

¹⁰⁸ Vgl. *Henssler*, in: Henssler/Prütting, BRAO § 43a Rn. 90, 92; *Hartung*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 11.4.2 Rn. 126; BGH, Urt. v. 20.05.1992 – VIII ZR 240, 91, NJW 1992, 2348.

¹⁰⁹ *Bauckmann*, in: Feuerich/Weyland, BRAO, § 43a Rn. 25b; teilweise wird bei der elektronischen Übermittlung vertraulicher Informationen generell – also auch im Falle der E-Mail-Kommunikation – eine ausdrückliche Einwilligung verlangt, hierzu *Henssler*, in: Henssler/Prütting, BRAO, § 43a Rn. 92.

¹¹⁰ Zu den technischen Grundlagen siehe S. 5ff.

¹¹¹ *Henssler*, in: Henssler/Prütting, BRAO § 43a Rn. 96; *Kargl*, in: NK-StGB, § 203 Rn. 103.

¹¹² Vgl. im Falle der Einwilligung in medizinische Behandlungen: *Wollersheim*, in: Clausen/Schroeder-Prinzen, AnWdB Medizinrecht, § 6 Rn. 143.

Klauselkontrolle¹¹³ – sorgfältig zu arbeiten. Ein rein pauschaler Verweis auf den genutzten Cloud-Service wird regelmäßig nicht ausreichen, um eine wirksame Aufklärung des Einwilligenden annehmen zu können.¹¹⁴ Jedenfalls ist auf die konkreten Risiken, die beteiligten Akteure, die zugrundeliegende Servicestruktur und den Umfang der Offenbarung einzugehen, damit der Einwilligende ein Bild davon erhält, wo, wem und in welchem Umfang unverschlüsselte, geschützte Informationen eröffnet werden.

Die Einwilligung ist damit zwar ein mögliches rechtliches Mittel zur rechtskonformen anwaltlichen Nutzung cloudbasierter Dienste, jedoch zugleich mit nicht unerheblichen Risiken behaftet.

d) Vertragliche Erweiterung des Geheimnisschutzes und datenschutzrechtliche Implikationen

Beauftragt der Anwalt einen Cloud Service Provider im Rahmen seiner Berufsausübung (§ 43e Abs. 1 S. 2 BRAO) und ist ein Offenbaren geschützter Informationen für die Inanspruchnahme des Cloud-Dienstes erforderlich (§ 43e Abs. 1 S. 1 Hs. 2 BRAO), kann der Anwalt dem Cloud Service Provider unter den weiteren Voraussetzungen des § 43e BRAO bzw. § 203 Abs. 3 StGB den Zugang zu geschützten Tatsachen eröffnen. Es liegt dann ein befugtes Offenbaren vor, das weder berufs- noch strafrechtliche Konsequenzen nach sich zieht. Dienstleister i.S.d. § 43e BRAO ist jede andere Person bzw. Stelle, die vom Anwalt im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird (§ 43e Abs. 1 S. 2 BRAO) und damit auch Anbieter von cloudbasierten Diensten.¹¹⁵

Neben der Erforderlichkeit setzt die Zugangseröffnung eine sorgfältige Auswahl des Cloud Service Providers voraus, der darüber hinaus durch vertragliche Vereinbarung in den Kreis der Geheimnisschutzverpflichteten nach Maßgabe des § 43e Abs. 3 BRAO aufzunehmen ist. Ergeben sich für den Anwalt Anhaltspunkte, die Zweifel an der Zuverlässigkeit des Cloud Service Providers begründen, hat er die Zusammenarbeit unverzüglich zu beenden (§ 43 Abs. 2 S. 2 BRAO).

¹¹³ Zu den Anforderungen an formularvertragliche Vereinbarungen im Anwaltsvertrag: *Blattner*, AnwBl. 2012, 237.

¹¹⁴ *Henssler*, in: Henssler/Prütting, BRAO § 43a Rn. 97; vgl. BGH, Urt. v. 20.05.1992 – VIII ZR 240, 91, NJW 1992, 2348.

¹¹⁵ *Offermann-Burckart*, in: Remmert, Legal-Tech, § 2 Rn. 230; *Peitscher*, Anwaltsrecht, § 18 Rn. 29ff; *Henssler*, in: Henssler/Prütting, BRAO § 43e Rn. 9.

e) Erforderlichkeit der Zugangseröffnung

Die Erforderlichkeit einer Zugangseröffnung (§ 43e Abs. 1 S. 1 Hs. 2 BRAO; § 203 Abs. 3 S. 2 Hs. 1 StGB) ist tätigkeitsbezogen zu ermitteln und kann bereits unter Berücksichtigung des Wortlauts („soweit [...] erforderlich“) nicht pauschal für jeglichen Cloud-Dienst beantwortet werden. An die Erforderlichkeit der Zugangseröffnung sind nach dem Willen des Gesetzgebers jedoch strenge Anforderungen zu setzen.¹¹⁶ Der Wortlaut ist dementsprechend restriktiv auszulegen.¹¹⁷

Ob eine Zugangseröffnung ggü. dem Cloud Service Provider erforderlich ist, kann nur im Einzelfall unter genauerer Betrachtung des cloudbasierten Dienstes ermittelt werden. Jedenfalls nicht mehr erforderlich ist eine Zugangseröffnung aus Sicht des Gesetzgebers dann, wenn eine technische Lösung zum Geheimnisschutz durch Verschlüsselung möglich ist. In der Gesetzesbegründung wird in diesem Zusammenhang das Beispiel eines Cloud-Speichers (IaaS) herangezogen und darauf verwiesen, dass die Daten in diesen Fällen „regelmäßig [...] verschlüsselt gespeichert werden“ können.¹¹⁸ Der anwaltlichen Praxis ist somit bereits hinsichtlich der Erforderlichkeit zu raten, bei der Nutzung von IaaS-Diensten den Cloud Service Provider sorgfältig auszuwählen und darauf zu achten, dass dieser eine vollumfängliche Datenverschlüsselung einerseits anbietet und dieses Feature andererseits auch aktiviert ist.¹¹⁹ Zwar steht dem Anwalt bei der Beurteilung der Erforderlichkeit ein Ermessensspielraum zu, denn nach Ansicht des Gesetzgebers ist ihm „ein Spielraum für verantwortliche unternehmerische Entscheidungen“ zu eröffnen.¹²⁰ Letztlich wird damit die Verantwortung für die Einschätzung des „Ob“ der Zugangseröffnung jedoch schlicht auf den anwaltlichen Berufsstand abgewälzt und versäumt, klare Vorgaben für ein Non Legal Outsourcing zu etablieren.¹²¹ Bei der Nutzung von IaaS-Angeboten (insb. Cloud Speichern) durch die Anwaltschaft sollte daher von einer Zugangseröffnung nach § 43e BRAO de lege lata abgesehen und eine technische Lösung angestrebt werden. Soweit dies im Einzelfall nicht möglich ist und eine Zugangseröffnung nach § 43e BRAO vorgenommen werden muss, sollten die hinter der Entscheidung stehenden Gründe vor dem Hintergrund der voll gerichtlich

¹¹⁶ BT Drs. 18/11936, S. 34.

¹¹⁷ *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 8; *Peitscher*, *Anwaltsrecht*, § 18 Rn. 29.; *Hartung*, *AnwBl.* 2018, 460 (462).

¹¹⁸ BT Drs. 18/11936, S. 34.

¹¹⁹ Zu den technischen Schutzverfahren siehe C. III. 1.

¹²⁰ BT Drs. 18/11936, S. 34; *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 8; *Offermann-Burckart*, in: *Remmert*, *Legal-Tech*, § 2 Rn. 235

¹²¹ Kritisch auch *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 8; *Grupp*, *AnwBl.* 2017, 816 (820), *Kleine-Cosack*, BRAO, §43e Rn. 2.

überprüfbar¹²² anwaltlichen Erforderlichkeitsprüfung dokumentiert werden. Zur Risikominimierung kann darüber hinaus eine ausdrückliche Einwilligung des Mandanten zur Speicherung der Daten beim IaaS-Dienstleister eingeholt werden.¹²³

Unter Berücksichtigung dieser gesetzgeberischen Wertung ist für die anwaltliche Nutzung von SaaS-Diensten in der Regel eine Zugangseröffnung erforderlich, da bei diesen Cloud-Services derzeit keine technische Lösung für eine vollverschlüsselte Verarbeitung geschützter Informationen besteht.¹²⁴ Damit ergibt sich im Umkehrschluss jedoch die berufsrechtliche Pflicht des Anwaltes, sich über den aktuellen Stand der Technik in regelmäßigen Abständen – in den Grenzen der Zumutbarkeit – zu informieren. Denn mit der Marktreife einer technischen Möglichkeit zur vollverschlüsselten Datenverarbeitung und einem tatsächlichen Angebot solcher SaaS-Dienste intendiert jedenfalls das Merkmal der Erforderlichkeit in § 43e Abs. 1 S. 1 Hs. 2 BRAO, der Wille des Gesetzgebers¹²⁵ und nicht zuletzt der Sinn und Zweck des Geheimnisschutzes¹²⁶ die Pflicht einer Nutzung solcher cloudbasierten Dienste, die eine Zugangseröffnung nach § 43e BRAO aufgrund einer technischen Lösung erst gar nicht erforderlich machen.

f) Sorgfältige Auswahl des Cloud Service Providers (§ 43e Abs. 2 S. 1 BRAO)

Ist die Zugangseröffnung erforderlich, darf der Anwalt nur „geeignete Dienstleister“ beauftragen.¹²⁷ Welche konkrete Anforderungen an die Geeignetheit zu stellen sind, ist nicht abschließend geklärt.¹²⁸ Die Gesetzesbegründung verweist auf die „fachliche Eignung und Zuverlässigkeit des Dienstleisters“ und stellt fest, dass hierfür „Zertifizierungen und sonstige Qualifikationsnachweise [...] eine Hilfe“ sein „können“. Welche Zertifizierungen bzw. Qualifikationsnachweise hilfreich sind und inwieweit eine bestehende Zertifizierung überhaupt für die Überprüfung der fachlichen Eignung und Zuverlässigkeit des Dienstleisters ausreichend ist, wird nicht festgestellt.¹²⁹ Der Gesetzgeber verweist diesbezüglich pauschal auf die Anforderungen im Rahmen der datenschutzrechtlichen Auftragsdatenverarbeitung nach Art. 28 DSGVO.

¹²² Henssler, in: Henssler/Prütting, BRAO § 43e Rn. 8.

¹²³ Zur Einwilligung siehe S. 17ff.

¹²⁴ Siehe hierzu: S. 15f.

¹²⁵ BT Drs. 18/11936, S. 34.

¹²⁶ Siehe hierzu S. 11.

¹²⁷ BT Drs. 18/11936, S. 34.

¹²⁸ So wohl auch Offermann-Burckart, in: Remmert, Legal-Tech, § 2 Rn. 237; Henssler, in: Henssler/Prütting, BRAO § 43e Rn. 12.

¹²⁹ Offermann-Burckart, in: Remmert, Legal-Tech, § 2 Rn. 237.

(1) Art. 28 DSGVO

Aufgrund des vergleichbaren Schutzniveaus¹³⁰ wird damit die Brücke zu den obligatorischen datenschutzrechtlichen Anforderungen an ein IT-Outsourcing durch die DSGVO geschlagen. Die DSGVO ist als Verordnung unmittelbar geltendes Recht (Art. 288 AEUV) und auch auf die anwaltliche Datenverarbeitung grundsätzlich anwendbar.¹³¹ Die nach alter Rechtslage strittige Frage, ob der Anwalt aufgrund seiner Stellung als Geheimnisträger überhaupt Normadressat des Datenschutzrechts ist, hat mit der Neuordnung durch die DSGVO keinen Bestand mehr.¹³² Auch ein Anwalt verarbeitet personenbezogene Daten (Art. 2 Abs. 1, Art. 4 Nrn. 1, 2 DSGVO) unabhängig davon, ob es sich um geheime Informationen handelt oder nicht.¹³³ Die Zulässigkeit dieser Verarbeitung ergibt sich aus Art. 6 Abs. 1 lit. b DSGVO bzw. – bei sensiblen Daten¹³⁴ – aus Art. 9 Abs. 2 lit. f DSGVO.¹³⁵

Gleichwohl entsteht aufgrund der Geheimhaltungspflichten im Falle der anwaltlichen Datenverarbeitung ein Spannungsfeld zwischen den datenschutzrechtlichen Anforderungen und den letztlich strafbewehrten berufsrrechtlichen Pflichten. Ein genereller Anwendungsvorrang des Berufsrechts, wie er in der Subsidiaritätsklausel des § 1 Abs. 2 S. 3 BDSG anklingt, ist aufgrund des Anwendungsvorrangs¹³⁶ der DSGVO gegenüber dem BDSG abzulehnen.¹³⁷ Auf Basis der Öffnungsklausel (Art. 23 Abs. 1 lit. i; Art. 90 Abs. 1 DSGVO) hat der nationale Gesetzgeber gleichwohl in den §§ 29 ff. für die Anwaltschaft relevante Ausnahmetatbestände geschaffen, die im Wesentlichen die Anwendbarkeit der Rechte Betroffener und Dritter adressieren. Damit gelten im Ausgangspunkt die Grundsätze für die Verarbeitung personenbezogener Daten und insbesondere die Anforderungen einer Auftragsdatenverarbeitung nach Art. 28 DSGVO auf die die Gesetzesbegründung zu § 43e Abs. 2 S. 1 BRAO recurriert.

¹³⁰ Vgl. *Gasteyer/Säljemar*, NJW 2020, 1768 (1769).

¹³¹ *Eichfeld/Hagen/James/James*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 15.3 Rn. 17.

¹³² Hierzu: *Weichert*, NJW 2009, 550.

¹³³ *Uwer*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK-Datenschutzrecht, Syst. F. Rn. 11.

¹³⁴ Zum Konzept sensibler Daten und Schutzerfordernissen: *Albers/Veit*, in: BeckOK-Datenschutzrecht, Art. 9 Rn. 18ff.

¹³⁵ Zur Erforderlichkeit i.S.d Art. 6 Abs. 1 lit b): *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 6 Rn. 24ff.

¹³⁶ EUGH, Urt. v. 05.02.1963 – C 26/62, ECLI:EU:C:1963:1 (Van Gend en Loos), S 23; EUGH, Urt. v. 15.07.1964 – C 6-64, ECLI:EU:C:1964:66 (Costa/ENEL), S. 1270.

¹³⁷ *Uwer*, in: BeckOK-Datenschutzrecht, Syst. F. Rn. 11; *Zikesch/Kramer*, ZD 2015, 565.

(2) Auftragsdatenverarbeitungsvertrag und sorgfältige Auswahl

Datenschutzrechtlich handelt es sich bei Cloud Computing regelmäßig um eine Auftragsdatenverarbeitung. Denn der Cloud Service Provider agiert in diesen Fällen als juristische Person, die personenbezogene Daten des Mandanten (betroffene Person) im Auftrag des für die Datenverarbeitung weiterhin verantwortlichen Anwalts¹³⁸ verarbeitet (Art. 4 Nr. 7 DSGVO).¹³⁹ Erlaubt ist eine solche Zugänglichmachung personenbezogener Daten durch den Anwalt an den Cloud Provider als Auftragsverarbeiter nur auf Basis eines Vertrags nach Maßgabe des § 28 Abs. 3 lit. a)–h) (Auftragsdatenverarbeitungsvertrag [AVV], engl. Data Processing Agreement [DPA]). Der AVV muss Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen¹⁴⁰ festlegen. Der Umfang der Weisungsbefugnisse des Verantwortlichen ist zu regeln, ebenso wie die Verpflichtung zur Verschwiegenheit der zur Verarbeitung befugten Personen (Art. 28 Abs. 3 lit. b, d). Darüber hinaus müssen durch den Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen (TOMs) zum Schutz der Daten nach Art. 32 DSGVO vereinbart werden (Art. 28 Abs. 3 lit. c). Die hinreichende Garantie zur Sicherstellung der TOMs begründet im Regelfall die Feststellung der fachlichen Eignung des Cloud Service Providers und damit eine sorgfältige Auswahl i.S.d. Art. 28 Abs. 1 DSGVO.¹⁴¹ Damit wird die hinreichende Garantie zur Sicherstellung geeigneter technischer und organisatorischer Maßnahmen für eine DSGVO-konforme Datenverarbeitung aufgrund des Verweises in der Gesetzesbegründung¹⁴² auch ausreichend zur Erfüllung der berufsrechtlich angeordneten sorgfältigen Auswahl nach § 43e Abs. 2 S. 1 BRAO sein. Die TOMs werden regelmäßig dem AVV als Anhang beigefügt. Fehlt ein entsprechender Appendix, sollte von einem Vertragsschluss zunächst abgesehen und die TOMs angefordert werden. Inhaltlich ist eine Plausibilitätsprüfung ausreichend. Eine darüber hinausgehende Pflicht zur inhaltlichen Prüfung ist dem regelmäßig allenfalls technikaffinen Anwalt nicht zumutbar.¹⁴³ Eine Pflicht zur Vor-Ort-Prüfung beim Cloud Service Provider durch den Anwalt, wie es § 11 Abs. 2 S. 4 BDSG a.F. noch vorsah wird nur in Ausnahmefällen anzunehmen sein, da sie in der Praxis im Regelfall nicht zumutbar ist.¹⁴⁴ Zu Beweis Zwecken sollte das Auswahlverfahren dokumentiert werden.¹⁴⁵

¹³⁸ Zum Begriff des Verantwortlichen i.S.d. DSGVO siehe Art. 4 Nr. 7 DSGVO.

¹³⁹ *Hessel/Schneider*, ZD 2024, 620 (621).

¹⁴⁰ *Hennrich*, Cloud Computing nach der DSGVO, S. 136.

¹⁴¹ *Hartung*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 11.4.2 Rn. 51f; *Offermann-Burckart*, in: Remmert, Legal-Tech, § 2 Rn. 242.

¹⁴² BT Drs. 18/11936, S. 34.

¹⁴³ So auch *Hennrich*, Cloud Computing nach der DSGVO, S. 135.

¹⁴⁴ So auch: *Henssler*, in: Henssler/Prütting, BRAO § 43e Rn. 18.

¹⁴⁵ Ebenso: *Offermann-Burckart*, in: Remmert, Legal-Tech, § 2 Rn. 241.

Der Nachweis zur Einhaltung der TOM kann gem. Art. 32 Abs. 3 DSGVO auch durch eine Zertifizierung i.S.d. Art. 42 DSGVO erfolgen. Seit Mitte 2024 existiert mit dem Zertifizierungsverfahren AUDITOR erstmals eine für Cloud Computing i.S.d. Art. 42 DSGVO anerkannte Zertifizierung. Der häufig zitierte Cloud Computing Compliance Criteria Catalogue – C5:2020 (C5 Testat)¹⁴⁶ des BSI ist keine Zertifizierung nach Art. 42 DSGVO.¹⁴⁷ C5:2020 dient als anerkannter Sicherheitsstandard und wird insbesondere in regulierten Branchen als Nachweis für die Einhaltung hoher IT-Sicherheitsanforderungen genutzt.¹⁴⁸ Das Testat nach C5 kann daher im Rahmen einer Risikoabwägung und bei der Auswahl von Cloud Service Providern als starkes Indiz für ein angemessenes Sicherheitsniveau herangezogen werden.

Die vertragliche Sicherstellung der TOMs nach Maßgabe des Art. 32 DSGVO durch den Auftragsverarbeiter entbinden den weiterhin für die Datenverarbeitung verantwortlichen Anwalt nicht davon, seinerseits technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes zu treffen.¹⁴⁹ Hierzu ist er als verantwortlicher Datenverarbeiter innerhalb seiner Sphäre weiterhin verpflichtet (Art. 24 DSGVO). Der auftragsverarbeitende Cloud Service Provider ist vertraglich zu verpflichten, den Anwalt hierbei im Kontext der Auftragsdatenverarbeitung zu unterstützen (Art. 28 Abs. 3 lit. e, f).¹⁵⁰ Der AVV muss darüber hinaus die Bedingungen für die Hinzuziehung von Subunternehmern regeln und die Unterstützungspflichten des Auftragsverarbeiters hinsichtlich Betroffenenrechten, Datensicherheit, Meldepflichten bei Datenschutzverletzungen und Datenschutz-Folgenabschätzungen festlegen. Zudem ist zu vereinbaren, wie nach Abschluss der Verarbeitung die Daten zurückgegeben oder gelöscht werden, wie Kontroll- und Nachweispflichten ausgestaltet sind und dass der Auftragsverarbeiter den Verantwortlichen informiert, falls eine Weisung gegen Datenschutzrecht verstößt (Art. 28 Abs. 3 lit. g, h).

¹⁴⁶ BSI Kriterienkatalog C5, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html (zuletzt abgerufen am 24.06.2026).

¹⁴⁷ Das BSI selbst weist darauf hin, dass C5:2020 und die DSGVO-Zertifizierungsverfahren (wie AUDITOR) komplementär zu sehen sind, C5 aber keine DSGVO-Zertifizierung darstellt: Vgl. BSI, FAQ C5, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5-FAQ/kriterienkatalog-c5-faq_node.html, (zuletzt abgerufen am 24.06.2026), siehe auch BMW, Pressemitteilung zur Vorstellung des C5:2020 v. 21.01.2020, abrufbar unter: <https://www.trusted-cloud.de/news/das-bsi-stellt-die-neue-version-c52020-vor/> (zuletzt abgerufen am 24.06.2026).

¹⁴⁸ Vgl. *Offermann-Burckart*, in: Remmert, Legal-Tech, § 2 Rn. 198ff.

¹⁴⁹ Vgl. *Hartung*, in: Leupold/Wiebe, Glossner, IT-Recht, Teil 11.4.2 Rn. 57.

¹⁵⁰ *Henrich*, Cloud Computing nach der DSGVO, S. 138.

c) Anforderungen an den Vertragsinhalt (§ 43e Abs. 3 BRAO)

Zusätzlich zum AVV ist mit dem ausgewählten Cloud-Provider eine Vereinbarung nach Maßgabe des § 43e Abs. 3 S. 1 Nrn. 1–3 BRAO (Geheimnisschutzvereinbarung [GSV]) zu treffen. Die Vorschrift beinhaltet Anforderungen an den dem Cloud-Dienst zugrundeliegenden Cloud Service Vertrag. Dies ergibt sich einerseits aus dem Wortlaut „Der Vertrag mit dem Dienstleister“ und andererseits aus dem Sinn und Zweck der Vorschrift.¹⁵¹ Die zur Zugangseröffnung geschützter Informationen notwendige Erweiterung des Geheimnisschutzes muss mit der Unterzeichnung des Cloud Service Vertrages erfolgen, da ab diesem Zeitpunkt ein Anspruch auf die Serviceleistung besteht. Wohl auch aus diesem Grund lässt der Gesetzgeber die Textform (§ 126b BGB) ausreichen, um Medienbrüche zu vermeiden.¹⁵² Eine vom Hauptvertrag getrennte GSV sollte zeitgleich oder unverzüglich nach Abschluss des Cloud Service Vertrages vereinbart werden. Eine Einbeziehung in den Hauptvertrag ist zu empfehlen.

In der GSV ist der Cloud Service Provider unter Belehrung der strafrechtlichen Folgen des § 203 Abs. 4 StGB zur Verschwiegenheit zu verpflichten (§ 43e Abs. 3 S. 1 Nr. 1 BRAO). Daneben hat der Anwalt ihn dahingehend vertraglich zu binden, seinen Zugriff auf geheime Informationen auf das für die Bereitstellung des Services notwendige Maß zu beschränken (§ 43 Abs. 3 S. 1 Nr. 2 BRAO). Wortlaut und Gesetzesbegründung dieser Inhaltsbestimmung lassen eine rein deklaratorische Vertragsklausel zwar zu. Vor dem Hintergrund des Telos ist gleichwohl zu empfehlen, im Rahmen der vertraglichen Begrenzung zur Kenntnisverschaffung des Cloud Service Providers den konkreten Dienst hinsichtlich Gegenstand, Art und Zwecks der Datenverarbeitung – ähnlich den Anforderungen an den AVV – zu bestimmen, sofern dies im Cloud-Service-Vertrag nicht bereits erfolgt ist.¹⁵³ Denn § 43e Abs. 3 Nr. 2 BRAO ergänzt die Pflicht des Anwaltes zur Erforderlichkeitsprüfung (§ 43e Abs. 1 BRAO) – also das „Ob“ der Zugangseröffnung – um den Umfang der Zugangseröffnung. Dies setzt eine Konkretisierung des zugrundeliegenden Cloud-Dienstes und seiner Funktion voraus.

In der GSV ist darüber hinaus aufzunehmen, ob der Cloud Service Provider befugt ist, weitere Personen zur Erfüllung des Vertrages hinzuzuziehen (§ 43e Abs. 3

¹⁵¹ Vgl. *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 20.

¹⁵² BT-Drs. 18/11936, S. 35; *Offermann-Burckart*, in: *Remmert*, Legal-Tech, § 2 Rn. 246ff; *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 21.

¹⁵³ So erfolgt die nähere Beschreibung eines SaaS-Services im Cloud-Service-Vertrag etwa durch eine Funktionsbeschreibung (als Anlage), vgl. *Krück*, in: *BeckOF-IT- und Datenrecht*, 1.15 Cloud Services Vertrag (SaaS).

Nr. 3 BRAO). Insbesondere bei der Inanspruchnahme von SaaS-Diensten wird dies regelmäßig notwendig sein, da SaaS-Anbieter ihrerseits auf (cloudbasierte) Dienste zur Bereitstellung ihres Angebotes zurückgreifen.¹⁵⁴ Der Cloud Service Provider ist dann zu verpflichten, die weiteren Personen seinerseits zur Verschwiegenheit zu verpflichten. Die Mitarbeiter des Cloud Service Providers sind keine „weiteren Personen“ i.S.d. § 43e Abs. 3 Nr. 3 BRAO.¹⁵⁵

d) Unverzügliche Beendigung bei Unzuverlässigkeit

Ergeben sich für den Anwalt nach Vertragsschluss mit dem Cloud Service Provider Anhaltspunkte, dass der durch die GSV getroffene Pflichtenkatalog nicht gewährleistet ist, hat der Anwalt „die Zusammenarbeit unverzüglich zu beenden“ (§ 43 Abs. 2 S. 2 BRAO). Der Gesetzgeber lässt hierbei bereits „konkrete Zweifel an der mit Blick auf die Verschwiegenheitspflicht erforderlichen Zuverlässigkeit“ genügen.¹⁵⁶ Der Anwalt ist damit berufsrechtlich verpflichtet, bei Bestehen verbleibender Zweifel an der Zuverlässigkeit zur Einhaltung der GSV nach einer Überprüfung des Cloud Service Providers den Cloud-Service-Vertrag durch Ausübung seiner Gestaltungsrechte ohne schuldhaftes Zögern (§ 121 BGB analog) zu beenden. Hierfür wird eine Frist von bis zu 14 Tage für angemessen erachtet.¹⁵⁷ Im Falle von Cloud Service Verträgen, die kein 14-tägiges ordentliches Kündigungsrecht vorsehen, stellt sich die Frage, ob dem Anwalt ein außerordentliches Kündigungsrecht zusteht. Dies hängt zunächst von der vertragstypologischen Einordnung von Cloud Service Verträgen ab, die nicht abschließend geklärt ist.¹⁵⁸ Ordnet man die cloudbasierte Bereitstellung von Hard- bzw. Software dem Mietvertragsrecht zu, so bemisst sich das außerordentliche Kündigungsrecht nach § 543 Abs. 1 BGB.¹⁵⁹ Unter Berücksichtigung der disziplinar- und strafrechtlichen Risiken des Anwaltes im Falle eines unbefugten Offenbarens wird eine Unzumutbarkeit zur Fortsetzung des Cloud Service Vertrages nach § 543 Abs. 1 BGB zwar regelmäßig anzunehmen sein, gleichwohl müssen die eine Unzuverlässigkeit nach § 43e Abs. 2 S. 2 BRAO begründenden

¹⁵⁴ Zu beachten ist eine mögliche Entbehrlichkeit nach § 43e Abs. 5 und 7 BRAO, die im Falle der Nutzung von Cloud Computing Diensten im Regelfall jedoch nicht einschlägig sind.

¹⁵⁵ BT-Drs. 18/11936, S. 35.

¹⁵⁶ BT-Drs. 18/11936, S. 34.

¹⁵⁷ *Gasteyer*, in: Hartung/Scharmer/Holl, BORA, § 43e BRAO, Rn. 12; wohl auch *Henssler*, in: Henssler/Prütting, BRAO § 43e Rn. 18.

¹⁵⁸ Für SaaS-Dienste wird regelmäßig ein Vergleich mit der Rechtsprechung des BGH zum Applikation Software Providing (ASP) gezogen, siehe: *Stögmüller*, in: Leupold/Wiebe/Glossner, IT-Recht, 11.4.3 Rn. 6.

¹⁵⁹ Zur mietvertraglichen Einordnung: *Meents*, in: Borges/Meents, Cloud Computing, § 4 Rn. 113f; *Stögmüller*, in: Leupold/Wiebe/Glossner, IT-Recht, 11.4.3 Rn. 6f.

Umstände hinreichend konkret sein. Eine bloße allgemeine Unzuverlässigkeit des Cloud Service Providers reicht nicht aus.¹⁶⁰ An dieser Stelle liegt das Risiko im Spannungsfeld zwischen unwirksamer Ausübung von Gestaltungsrechten und der Einhaltung berufs- und strafrechtlicher Anforderungen beim Anwalt. De lege lata sollte beim Abschluss von Cloud Service Verträgen daher die Nichteinhaltung der GSV als Regelbeispiel für ein außerordentliches Kündigungsrecht zum Vertragsinhalt gemacht werden. Ein solches Regelbeispiel kann durch gegenseitige Informations- und Aufklärungspflichten zur Sicherstellung der Erfüllung des Vertragszwecks flankiert werden.

D. Fazit

Die Nutzung cloudbasierter Dienste ist für die anwaltliche Praxis – neben den datenschutzrechtlichen Implikationen – mit erheblichen berufsrechtlichen und strafrechtlichen Herausforderungen verbunden. Rechtlich möglich wird die Nutzung cloudbasierter Dienste durch die Zugangseröffnung gemäß § 43e BRAO und § 203 StGB – bleibt aber risikobehaftet und erfordert eine stetige Kontrolle des nutzenden Anwaltes. Maßnahmen für die rechtssichere Nutzung sind konsequente Verschlüsselung vertraulicher Daten dort, wo es technisch möglich ist, strenge Zugriffskontrollen, eine umfassende Protokollierung sowie klare und den berufsrechtlichen Anforderungen entsprechende vertragliche Regelungen. Ergänzend sollten sensible Informationen möglichst pseudonymisiert verarbeitet werden, um Risiken zu minimieren. Die Einholung einer ausdrücklichen Einwilligung des Mandanten kann ein zusätzliches sicherndes rechtliches Instrument darstellen. Nur durch die konsequente Einhaltung der im Rahmen dieser Arbeit dargestellten geheimnisschutz- und datenschutzrechtlichen Anforderungen lässt sich eine rechtskonforme anwaltliche Nutzung von Cloud-Diensten realisieren.

¹⁶⁰ Vgl. hierzu: LG Köln, Urt. v. 16.02.2022 – 28 O 303/20, ZD 2022, 390 (392); *Henssler*, in: *Henssler/Prütting*, BRAO § 43e Rn. 18.