Trusted Cloud

Kompetenzzentrum Trusted Cloud

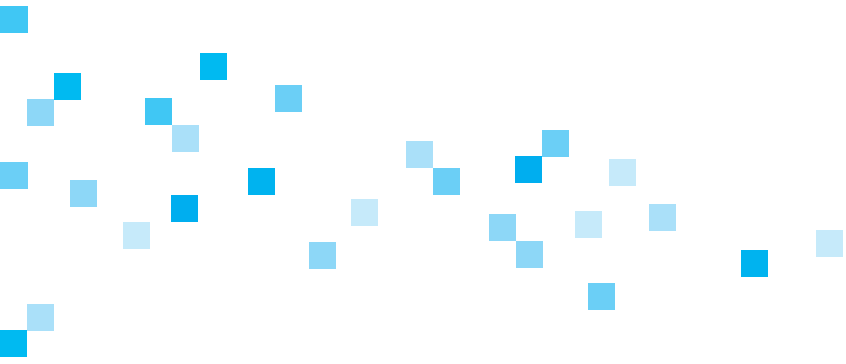
Thesenpapier – Schweigepflicht bei der Auslagerung von IT-Dienstleistungen

Nr. 7

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“

Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das Bundesministerium für Wirtschaft und Energie (BMWi) daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen.

In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Sie wird geleitet von Prof. Dr. Georg Borges. Themenschwerpunkte sind u. a. Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten durchgeführt, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.



Inhaltsverzeichnis

Einführung

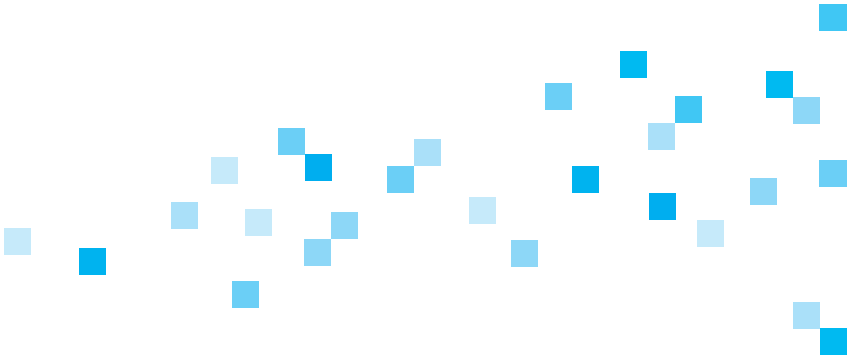
Auch Angehörige von Berufsgruppen, die einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, lagern IT-Dienstleistungen an externe Spezialisten aus (sogleich Ziff. 1). Dies gilt nicht nur für etablierte IT-Dienstleistungen wie die (Fern-) Wartung von EDV-Systemen, sondern zunehmend auch für innovative IT-Angebote. So eröffnet Cloud Computing auch Berufsgeheimnisträgern wesentlich erweiterte Möglichkeiten, externe IT-Dienstleistungen in Anspruch zu nehmen und dadurch ihre eigenen Dienste zu verbessern.

Allerdings besteht bei Berufsgeheimnisträgern erhebliche Rechtsunsicherheit, ob die Auslagerung von IT-Dienstleistungen mit der strafbewehrten Schweigepflicht vereinbar ist. Das Papier erörtert die Probleme der geltenden Rechtslage (Ziff. 2–3) anhand relevanter Fallgruppen von IT-Dienstleistungen (Ziff. 4) und plädiert aufgrund der hohen Bedeutung für die Praxis (Ziff. 5–6) für eine Änderung des Gesetzes (Ziff. 7). Schließlich werden mögliche Optionen für eine Gesetzesänderung dargestellt (Ziff. 8).

1 Zunehmende Inanspruchnahme von externen IT-Dienstleistern durch Berufsgeheimnisträger

Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB, zu denen unter anderem Ärzte, Rechtsanwälte, Steuerberater und Angehörige von Unternehmen der privaten Kranken-, Unfall- und Lebensversicherung gehören, bedienen sich zur Erfüllung ihrer Aufgaben bzw. zum Betrieb ihres Unternehmens zunehmend externer Dienstleister. Grund für solche Auslagerungen sind teils die Einsparung von Kosten oder begrenzte räumliche Kapazitäten, vor allem aber die Erforderlichkeit von besonderem Fachwissen, über das häufig nur spezialisierte Dienstleister verfügen. Dies gilt angesichts der ständig wachsenden Bedeutung der elektronischen Datenverarbeitung insbesondere für Dienstleistungen im IT-Bereich. So werden an externe Spezialisten Aufgaben ausgelagert, die in Zeiten manueller Datenverarbeitung in den Praxen, Kanzleien und Unternehmen selbst erbracht worden sind.

Grundlage für die Auslagerung war die Entwicklung der Informations- und Kommunikationstechnik, die eine zunehmende Vernetzung ermöglicht. Bedient sich Informations- und Kommunikationstechnik öffentlicher Netze, eröffnen sich Möglichkeiten des Zugriffs aber auch für Unbefugte. Werden mithilfe von Informations- und Kommunikationstechnik IT-Leistungen ausgelagert, könnten vertrauliche Informationen an einen weiteren Personenkreis – beispielsweise an die Mitarbeiter des IT-Dienstleisters – gelangen. Der Einsatz von Informations- und Kommunikationstechnik birgt folglich Risiken. Um den Betroffenen derartiger Informationsverarbeitung, also etwa den Patienten oder Mandanten, zu schützen, hat der Gesetzgeber die Weitergabe von Daten datenschutzrechtlich streng reglementiert und sie unter bestimmten Voraussetzungen sogar unter Strafe gestellt.



2 Datenschutzrechtliche Vorgaben bezüglich der Einschaltung von externen Dienstleistern

Schaltet ein Unternehmen beispielsweise zur Speicherung von Daten oder zur Wartung von EDV-Anlagen einen externen Dienstleister ein, werden dem Dienstleister häufig personenbezogene Daten von Kunden überlassen; zumindest kann ein Zugriff des Dienstleisters auf solche Daten dabei nicht immer ausgeschlossen werden. Das Unternehmen verschafft somit dem externen Dienstleister die Möglichkeit, von Daten Kenntnis zu nehmen, die dem BDSG unterliegen.

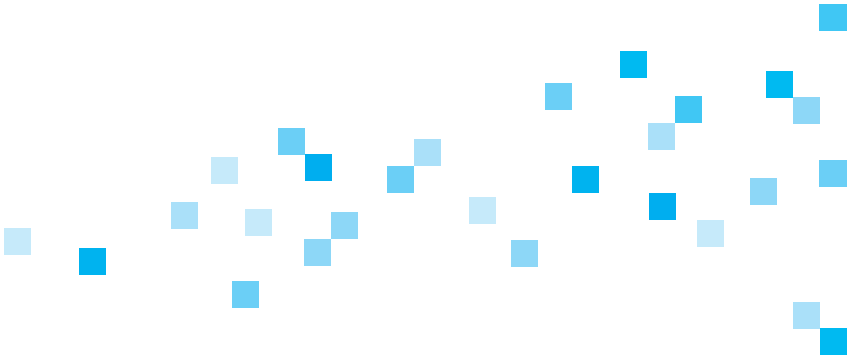
Auf rein datenschutzrechtlicher Ebene, d.h. bei Sachverhalten, die nicht dem strafrechtlichen Berufsgeheimnisschutz unterliegen, kann die Datenweitergabe gegebenenfalls durch einen Vertrag mit dem Dienstleister über eine sogenannte Auftragsdatenverarbeitung nach § 11 BDSG rechtmäßig ausgestaltet werden: Unter bestimmten, im Gesetz näher geregelten Voraussetzungen wird der Dienstleister datenschutzrechtlich als eine Art interne Stelle des Auftraggebers angesehen, sodass eine Datenweitergabe an ihn keine Übermittlung im datenschutzrechtlichen Sinne darstellt (vgl. § 3 Abs. 8 Satz 3 BDSG).

§ 11 BDSG wird als allgemeine Regelung jedoch verdrängt, wenn bereichsspezifische Vorschriften zur Auftragsdatenverarbeitung den Sachverhalt abschließend regeln. So enthalten beispielsweise die meisten Landeskrankenhausgesetze für den Bereich der Krankenhäuser gegenüber § 11 BDSG vorrangige Regelungen, die für die Einschaltung externer Dienstleister zum Teil besonders strenge Vorgaben vorsehen oder eine Verarbeitung nur durch andere Krankenhäuser zulassen (z. B. Art. 27 Abs. 4 Satz 6 des Bayerischen Krankenhausgesetzes). Eine weitere Spezialregelung stellt beispielsweise für Sozialdaten § 80 SGB X dar. Handelt es sich beim Auftraggeber um eine öffentliche Stelle, sind statt § 11 BDSG zudem die entsprechenden Vorschriften des jeweiligen Landesdatenschutzgesetzes anzuwenden, soweit nicht auch diese gegenüber speziellen Regelungen zurücktreten. Sollen externe Dienstleister mit der Verarbeitung von Daten beauftragt werden, ist daher im Einzelfall zu prüfen, welche datenschutzrechtlichen Bestimmungen auf den Auftraggeber und den betroffenen Sachverhalt Anwendung finden und welche Vorgaben dementsprechend für die vorgesehene Auftragsdatenverarbeitung zu beachten sind.

Soweit die Überlassung personenbezogener Daten im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG erfolgt und daher keine Übermittlung im datenschutzrechtlichen Sinne darstellt (s.o.), ist zu berücksichtigen, dass diese Privilegierung auf den Bereich des Datenschutzrechts beschränkt ist. Eine etwaige Strafbarkeit nach § 203 Abs. 1 StGB bleibt hiervon jedoch unberührt (vgl. § 1 Abs. 3 Satz 2 BDSG). Auch soweit sich eine datenschutzrechtliche Rechtfertigung nach § 28 BDSG oder Spezialnormen (z. B. Forschung) ergibt, berührt dies die etwaige Strafbarkeit nach § 203 StGB nicht.

3 Strafbarkeitsrisiko bei der Einschaltung von externen Dienstleistern

Unabhängig von der datenschutzrechtlichen Beurteilung einer Auftragsdatenverarbeitung sowie den berufsrechtlichen Regelungen besteht die strafrechtliche Problematik, dass die Beauftragung externer Dienstleister als eine unbefugte Offenbarung von Berufsgeheimnissen angesehen werden kann, die – auch bei Vorliegen einer Auftragsdatenverarbeitung – nach § 203 Abs. 1 StGB strafbar ist.[1] Zur Frage, unter welchen Umständen von einer Offenbarung von Berufsgeheimnissen auszugehen ist, insbesondere ob hierfür bereits die Möglichkeit der Kenntnisnahme ausreicht oder ob der Dienstleister tatsächlich von den Daten Kenntnis nehmen muss, bestehen unterschiedliche Auffassungen. Da sich Berufsgeheimnisträger deshalb nicht sicher sein können, unter welchen Voraussetzungen die Einschaltung eines externen Dienstleisters eine unbefugte Offenbarung darstellt, unterliegen sie zumindest latent einem ständigen Strafbarkeitsrisiko, das in erster Linie die Geschäftsleitung und die sonst verantwortlich handelnden Personen trifft. In der Praxis führt dieses Risiko häufig dazu, dass Unternehmen, vor allem Kranken-, Lebens- und Unfallversicherungen, Krankenhäuser und andere Einrichtungen im Gesundheitswesen sowie Rechtsanwälte und Steuerberater, so weit wie möglich von der Einschaltung externer Dienstleister absehen, wenn diese mit vom Berufsgeheimnis geschützten Daten in Berührung kommen könnten. Dieser Umstand trägt wohl mit dazu bei, dass im Bereich der Verarbeitung von durch § 203 StGB geschützten Daten kaum Rechtsprechung zum Einsatz externer Dienstleister existiert (s. hierzu auch unten Ziff. 6). Dies führt dazu, dass moderne Technologien, wie z. B. Cloud Computing, in den betroffenen Wirtschaftsbereichen kaum zum Einsatz kommen und dadurch Wettbewerbsnachteile entstehen.



1 Werden Dienstgeheimnisse verletzt, kommt in besonderen Fällen darüber hinaus eine Strafbarkeit nach § 353b StGB in Betracht.

4 Exemplarische Darstellung von Fallkonstellationen im Bereich von IT-Dienstleistungen

Die Komplexität der Datenverarbeitung in Computersystemen und -netzwerken nimmt auch bei Berufsgeheimnisträgern kontinuierlich zu. Die Vertreter dieser Berufe und ihre Angestellten sind daher häufig nicht in der Lage, die technische Betreuung ihrer IT-Systeme selbst zu übernehmen bzw. auftretende technische Probleme selbst zu lösen. Nachfolgend wird für einige praxisrelevante Fallgruppen das Problem des Strafbarkeitsrisikos beim Einsatz von IT-Dienstleistern dargestellt.

→ Wartung durch externe Dienstleister

Eine Wartung der IT durch externe Techniker vor Ort ist oftmals zeit- und kostenaufwendig. Über elektronische Kommunikationsmittel, insbesondere über das Internet, ist es allerdings möglich, aus der Ferne auf die Systeme zuzugreifen und die erforderliche Wartung durchzuführen.[2] Um technische Anlagen fernwarten zu können, muss ein Zugriff von einem entfernten Arbeitsplatz des Technikers auf die Anlage des Arztes, Anwalts oder Steuerberaters über eine Telekommunikationsverbindung ermöglicht werden (sogenannter Remote Access). Dabei kann der Techniker aber beispielsweise auch auf die im System abgelegten Datenordner und Daten zugreifen (Remote Terminal). Er kann sogar ganz die Kontrolle über das System übernehmen und z. B. die Benutzeroberfläche des Nutzers (inkl. Maus- und Tastatureingaben) einsehen oder selbst steuern (Remote Desktop).

Im Rahmen der Fernwartung können auch geschützte Geheimnisse im Sinne des § 203 StGB über öffentliche Kommunikationswege übertragen werden. Indem die Fernwartung ausschließlich über gesicherte Verbindungen, beispielsweise unter Nutzung von VPN-Tunneln, durchgeführt wird, kann der Berufsgeheimnisträger zwar einen Zugriff unbefugter Dritter auf die Datenübertragung zwischen seinem System und dem Fernwartungstechniker verhindern. Nicht auszuschließen ist allerdings, dass der Techniker selbst im Rahmen seiner Tätigkeit – beabsichtigt oder unbeabsichtigt – die auf dem System des Berufsgeheimnisträgers vorgenommenen Eingaben und gespeicherten Daten einsieht und dabei Berufsgeheimnisse zur Kenntnis nimmt. Indem der Berufsgeheimnisträger eine Fernwartung in Auftrag gibt und dadurch den Zugriff auf sein System eröffnet, ermöglicht er die Kenntnisnahme von Berufsgeheimnissen zumindest potenziell. Bereits hierin kann eine strafbare Offenbarung von Berufsgeheimnissen (gegebenenfalls durch Unterlassen) durch den Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB liegen.

Die gleichen Probleme ergeben sich bei traditionellen Formen der IT-Wartung, bei denen ein Techniker in den Räumen des Berufsgeheimnisträgers auf dessen IT-Systeme Zugriff nimmt. Auch hier kommt eine Strafbarkeit des Berufsgeheimnisträgers nach § 203 StGB in Betracht.

2 Als Wartung definiert beispielsweise § 3 Abs. 3 Nr. 5 BbgDSG die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware. Nach § 3 Abs. 3 Nr. 6 BbgDSG ist Fernwartung die Wartung der Soft- und Hardware von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtungen zur Datenübertragung vorgenommen wird.

→ Cloud-Storage-Dienste

In den letzten Jahren sind zahlreiche Dienste auf den Markt gekommen, mit denen Nutzer Daten von einem PC oder Smartphone auf einem entfernten Rechnersystem speichern, dort bearbeiten und Dritten zugänglich machen können. Der bekannteste dieser Dienste stammt vom US-amerikanischen Anbieter Dropbox. Es gibt mittlerweile zahlreiche derartige Dienste in verschiedensten Ausprägungen. Insbesondere haben auch die großen Hersteller von mobilen Betriebssystemen derartige Funktionen in ihre Angebote integriert (etwa iCloud® und Google Drive®). Ebenso bietet Microsoft mit seinem Angebot „OneDrive“ eine ebenfalls integrierte Synchronisationslösung für Daten an und versucht, mit dem Produkt „Office 365“ sogar die IT-Ressourcen seiner Kunden in seinen Rechenzentren zu bündeln, statt dass diese auf den Endgeräten der Kunden vorgehalten werden müssten. Auch wenn sich einige der bekannten Dienste nicht für den Einsatz durch Berufsgeheimnisträger eignen, gibt es daneben auch zahlreiche spezifische Cloud-Speicherdienste für Berufsgeheimnisträger.

Die Gemeinsamkeit solcher Cloud-Storage-Dienste ist die Möglichkeit, eine einmal über das Internet im System des Dienstleisters abgelegte Datei grundsätzlich von jedem mit dem Internet verbundenen geeigneten Endgerät abzurufen. Ein Nutzer kann die von ihm hochgeladenen Dateien regelmäßig anderen Nutzern zugänglich machen, z. B. durch das Versenden eines durch den Cloud-Storage-Dienst bereitgestellten Internetlinks. Möglich ist es in vielen Fällen auch, Dateien oder ganze Ordner insgesamt öffentlich zugänglich zu machen.

Die Grundidee solcher Dienste ist es, die Übertragung von größeren Datenmengen zu ermöglichen und dabei die technischen und praktischen Begrenzungen von beispielsweise E-Mails oder lokalen Speichermedien zu umgehen. Dies ist bislang auch der Hauptanwendungsfall von Cloud-Lösungen, wobei sogenannte „Collaboration“-Funktionen, also das gemeinsame, gleichzeitige Betrachten und Bearbeiten von Dateien, z.B. von Textdokumenten oder Präsentationen, in der allgemeinen Unternehmenspraxis stetig zunehmen.

Das Verwenden von Cloud-Storage-Diensten eröffnet verschiedene Anknüpfungspunkte für eine mögliche Strafbarkeit nach § 203 Abs. 1 StGB. So kann ein „Offenbaren“ schon im Hochladen einer Datei in die Systeme eines Cloud-Storage-Dienstleisters gesehen werden, denn dadurch wird sie zumindest dem Cloud-Storage-Dienstleister zugänglich gemacht. Zwar geben viele Anbieter an, das Hochladen über den Browser oder die entsprechende App auf mobilen Endgeräten erfolge über verschlüsselte, also durch Dritte nicht ohne weiteres einsehbare Verbindungen. Allerdings erfolgt in aller Regel weder die Speicherung noch die Verarbeitung der Daten in den Systemen des Cloud-Storage-Dienstleisters vollständig verschlüsselt; dies gilt insbesondere für die zahlreichen kostenlos angebotenen Dienste. Hinzu kommt, dass – soweit erkennbar – die Mehrheit der Cloud-Storage-Dienstleister ihrerseits Kapazitäten bei (weiteren) Rechenzentrumsbetreibern bezieht, um ihre Cloud-Dienste anbieten zu können. Damit besteht aus Sicht des Nutzers regelmäßig die Gefahr, dass es zu einer Kenntnisnahme der nach § 203 Abs. 1 StGB geschützten Daten durch noch andere Personen als den eigentlichen Vertragspartner kommt.

Man wird sicherlich einwenden können, dass es Berufsgeheimnisträgern zumutbar ist, im Rahmen ihrer Berufsausübung auf qualitativ höherwertige Anbieter von Cloud-Storage-Diensten zurückzugreifen. Die oben erwähnte Unsicherheit über die praktische Reichweite von § 203 Abs. 1 StGB einerseits und der Mangel an Diensten, die eine Ende-zu-Ende-Vollverschlüsselung enthalten, andererseits führen allerdings dazu, dass den von § 203 Abs. 1 StGB erfassten Berufsgruppen die Effizienzvorteile und Arbeitserleichterungen durch Cloud-Storage-Dienste faktisch nicht zur Verfügung stehen.

→ Konfliktprüfungen

Insbesondere Steuerberater und Rechtsanwälte sind verpflichtet, widerstreitende Interessen bei der Beratung zu vermeiden. Für Steuerberater folgt dies aus § 6 BOStB, für Rechtsanwälte aus § 43a BRAO i.V.m. § 3 BORA. Dabei gilt diese Pflicht nicht nur für den einzelnen Berater, sondern im rechtsanwaltlichen Umfeld grundsätzlich auch für rechtsanwaltliche Berufsausübungs- oder Bürogemeinschaften gleich welcher Art (§ 3 Abs. 2 Satz 1 BORA) sowie im Steuerberatungskontext auch für Sozietäten, Steuerberatungsgesellschaften, Partnerschaftsgesellschaften, Anstellungsverhältnisse oder sonstige Formen der Zusammenarbeit (§ 6 Abs. 3 BOStB). Die Pflicht zur Vermeidung widerstreitender Interessen ist also sehr weit gefasst. Dies bestätigt auch § 33 BORA, wonach diese Pflicht auch dann gilt, wenn etwa Rechtsanwälte mit Steuerberatern kooperieren.

Gerade im Umfeld von Großkanzleien, die überregional, gegebenenefalls sogar international über Niederlassungen, gesonderte Gesellschaften und/oder Kooperationspartner tätig werden, führt die Erfüllung dieser Pflicht zu erheblichen Herausforderungen. So ist trotz der häufig fehlenden Kenntnis der Einzelmandate im überregionalen oder internationalen Netzwerk sicherzustellen, dass keine Tätigkeit für mehrere Mandanten in derselben Rechtssache erfolgt. Denn eine solche wäre nur nach umfassender Information des Mandanten zulässig, wenn dieser sich sodann mit der Vertretung ausdrücklich einverstanden erklärt und die Belange der Rechtspflege nicht entgegenstehen (vgl. exemplarisch § 3 Abs. 2 Satz 2 BORA). Eine solche Aufklärung ist aber wiederum nur möglich, wenn feststeht, dass ein potenzieller Interessenkonflikt besteht.

Aus diesen Gründen lässt sich die Konfliktprüfung im Umfeld überregional agierender Kanzleien, Sozietäten und sonstiger Formen der überörtlichen Zusammenarbeit in der Regel nur durch den Einsatz technischer Lösungen realisieren, sogenannter Conflict-Check-Software. Diese muss vor der Mandatsaufnahme naturgemäß die Mandatsinformationen aller Beratungspartner miteinander abgleichen, um sicherstellen zu können, dass der Gegner des potenziellen Mandanten nicht bereits durch einen anderen Berater des Netzwerkes vertreten wird. Die Conflict-Check-Software wird dabei in aller Regel zentral gehostet sein, wobei sich hierzu vor allem Cloud-Lösungen anbieten. Denn bereits heute werden solche Softwareanwendungen regelmäßig entweder zentral bei einer (Berufs-) Gesellschaft der Beratungsgruppe gehostet oder es wird hierfür die Infrastruktur eines externen IT-Dienstleisters genutzt. Größere Beratungsgruppen verfügen mitunter auch

über eine eigene IT-Gesellschaft, die die Software als zentraler IT-Dienstleister in der Gruppe bereitstellt bzw. auf ihren Systemen im Auftrag der Gruppengesellschaften betreibt. Unabhängig aber davon, ob die Software gruppenintern oder -extern gehostet wird, unterhalten international oder überregional tätige Kanzleien heute oft keine eigenen Server mehr. Eine technische Offenlegung der bestehenden Mandatsbeziehungen gegenüber der hostenden Gruppengesellschaft oder dem IT-Dienstleister – und damit einem Dritten – ist in aller Regel unumgänglich. Bereits hierin kann aber wiederum eine strafbare Offenbarung von Berufsgeheimnissen im Sinne des § 203 Abs. 1 StGB durch die beteiligten Berufsgeheimnisträger gesehen werden.

→ Cloud-Lösungen für medizinische Versorgung und Forschung

Krankenhäuser sind mittelständische regionale Unternehmen oder auch Einrichtungen in öffentlicher Trägerschaft mit eigenen IT-Infrastrukturen, deren Betrieb aufwendig ist. Der Bedarf an nutzerorientierter Unterstützung der medizinischen Leistungserstellung durch Systeme der Informations- und Kommunikationstechnik ist hoch, seine Befriedigung aber kostenintensiv. Innovation scheitert daher oft an den verfügbaren Budgets (Kostenträgerschaft und anteilige Infrastrukturkosten im Gesundheitswesen). Cloud-Computing stellt eine Alternative dar, vorausgesetzt, die hohen Anforderungen an Datenschutz und Datensicherheit, Interoperabilität, Skalierbarkeit sowie Verfügbarkeit werden erfüllt.

Dienste für softwaregestützte Bewertungs- und Analyseaufgaben im Bereich der medizinischen Diagnostik (z. B. Mustererkennung, Patternvergleiche) oder auch für die Beurteilung von Bildmaterial durch einen Spezialisten, ferner behandlungsbegleitende Services, wie z. B. AMTS[3]-Prüfungsprogramme, ließen sich mittels Cloud so bereitstellen, dass jederzeit auf sie zugegriffen werden kann und Ergebnisse ohne Zeitverzug abgerufen werden können.

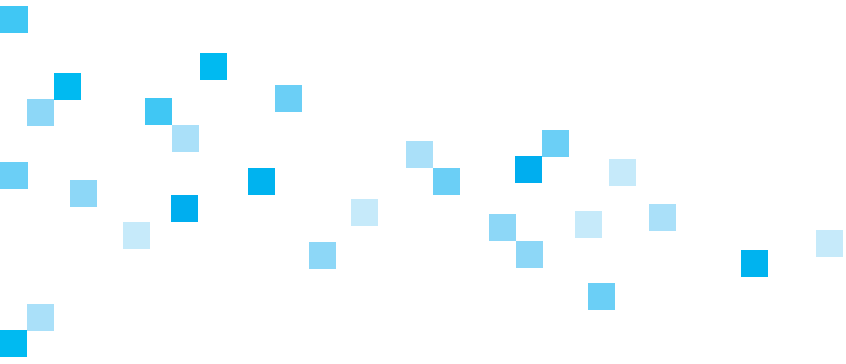
Diese Dienste werfen Schwierigkeiten auf, wenn die Daten nicht nur über eine Cloud übertragen, sondern in der Cloud unverschlüsselt verarbeitet werden. Aber gerade die Verarbeitung von Daten in der Cloud erspart sowohl dem Anbieter der Services als auch den Krankenhäusern als Kunden den Betrieb eines eigenen Rechenzentrums mit der erforderlichen Performanz und Redundanz und ermöglicht den Nutzern einen flexibleren Zugriff auf eine professionell betriebene Wirkumgebung. Ein zusätzliches Add-on ist die sichere Archivierung. Gleichzeitig können solche Services vielen Krankenhäusern zur Verfügung gestellt werden, z. B. für die Verbesserung der Patientensicherheit. Durch sehr hohe technische Sicherheitsmaßnahmen (Verschlüsselung, Zwei-Faktor-Authentifizierung beim Zugriff) ist eine Offenbarung wesentlich unwahrscheinlicher, als das im stationären Alltag der Krankenhäuser möglich ist.

3 AMTS = Arzneimitteltherapiesicherheit.

Das Risiko einer unbefugten Offenbarung medizinischer Daten durch Nutzung eines Cloud-Dienstes hat sich auch im Rahmen der Forschungen des Trusted-Cloud-Programms als schwer überwindbare Hürde erwiesen. So kann die Gestaltung einer geschlossenen und institutsübergreifenden Prozesskette mit einer medienbruchfreien und durchgängigen Verlaufsdokumentation, wie sie für eine klinikübergreifende stationäre Versorgung von Patienten erforderlich wäre, nicht ohne den standardisierten Austausch medizinischer Daten zwischen stationären und ambulanten Einrichtungen umgesetzt werden. Zwingend benötigt wird ein auf IHE-Konzepten[4] basierender „Master Patient Index“ (MPI), der alle Indices eines Patienten aus verschiedenen Krankenhäusern referenziert und dazu dient, die Informationen aus den verschiedenen Quellen unter einer gemeinsamen Identität zusammenführen zu können. Er prüft Patientendaten auf Übereinstimmung. Dazu müssen sie entschlüsselt sein. Ist der MPI in der Cloud lokalisiert, findet eine Verarbeitung von Patientendaten außerhalb des Krankenhauses statt. Somit ist der Tatbestand der Offenbarung erfüllt bzw. die ärztliche Schweigepflicht gebrochen worden, selbst wenn durch geeignete technische Maßnahmen sichergestellt ist, dass keine andere Person Kenntnis von diesen Daten erlangt, außer diejenige, die vom Krankenhaus beauftragt ist, die Zusammenführung der Daten zu überwachen.

Es verwundert daher nicht, dass Bundesärztekammer und Kassenärztliche Bundesvereinigung die Nutzung von Cloud-Diensten kritisch sehen und sie nur unter Bedingungen als zulässig erachten, die eine Entwicklung zukunftsorientierter Cloud-Lösungen für das Gesundheitswesen erschweren.

Weitere relevante Felder mit stark wachsendem Bedarf an IT-Unterstützung sind die Entwicklung der individualisierten Medizin und die Erforschung und Behandlung seltener Krankheiten. In der Forschung auf diesen Feldern ist schon heute die Verarbeitung und Zusammenführung großer Mengen medizinischer Daten erforderlich, was die IT-Kapazitäten vieler Krankenhäuser übersteigt. Dabei ist davon auszugehen, dass die heute für die Forschung geltenden Anforderungen an IT-Unterstützung morgen auch den Standard in der Versorgung charakterisieren.



4 IHE = Integrating the Healthcare Enterprise Initiative.

5 De lege lata keine rechtssicheren Lösungen möglich

Eine Beauftragung externer Dienstleister ist zwar auch im Hinblick auf die strafbewehrte Schweigepflicht möglich, wenn der Patient, Mandant bzw. Kunde den zur Verschwiegenheit Verpflichteten von seiner Schweigepflicht entbindet. Die Einholung einer Schweigepflichtentbindung ist in der Regel aber nicht praktikabel. So würde bereits die Entscheidung eines einzigen Patienten, der eine solche Entbindung ablehnt, dazu führen, dass der Arzt im Ergebnis für alle seine Patienten auf die Einschaltung eines externen Dienstleisters verzichten muss; denn eine Differenzierung nach einzelnen Patienten ist beispielsweise bei der externen Betreuung oder Wartung eines EDV-Systems nicht möglich. Würde der Arzt den Dienstleister wechseln wollen, müsste er unter Umständen zudem für alle Patienten eine neue Einwilligung hinsichtlich des neuen Dienstleisters einholen. Dies würde beispielsweise bei der externen Archivierung von Unterlagen auch diejenigen Patienten betreffen, deren Behandlung schon Jahre zurückliegt, deren Daten aber wegen entsprechender Aufbewahrungspflichten noch gespeichert sind. Deshalb stellt eine Einwilligung keine ausreichende Lösung dar, um Berufsgeheimnisträgern die Einbeziehung externer Dienstleister rechtssicher zu ermöglichen. Auch wenn in Einzelfällen durch technische und organisatorische Lösungen eine Offenbarung verhindert werden kann, ist eine flächendeckende Lösung dadurch nicht möglich.

Vor diesem Hintergrund werden in der juristischen Beratungspraxis verschiedene Argumente vorgetragen, um den Tatbestand einer unbefugten Offenbarung auszuschließen. So wird beispielsweise versucht, den Begriff des berufsmäßig tätigen Gehilfen, dem Berufsgeheimnisse zulässigerweise offenbart werden dürfen, dahingehend auszuweiten, dass darunter auch externe Dienstleister zu verstehen sind. Ein anderer Ansatz bemüht sich, durch eine Kombination von technischen und organisatorischen Maßnahmen – angelehnt an § 11 BDSG – das mögliche Offenbaren von Berufsgeheimnissen so weit einzuschränken, dass eine Strafbarkeit nach § 203 StGB im Ergebnis zu verneinen wäre. Da jedoch alle bisher entwickelten Argumentationsansätze umstritten sind, schaffen sie den Berufsgeheimnisträgern keine sichere Rechtsgrundlage für den Einsatz externer Dienstleister. Daher verbleibt für Berufsgeheimnisträger stets das Risiko, durch die Einbeziehung externer Dienstleister die Schweigepflicht zu verletzen und daher strafrechtliche Konsequenzen fürchten zu müssen.

6 Große Bedeutung für die Praxis

Aus dem Umstand, dass aus der Praxis kaum Strafverfahren zu § 203 StGB wegen des Einsatzes von IT-Dienstleistern bekannt sind, darf nicht der Schluss gezogen werden, dass es sich bei dieser Rechtsunsicherheit um ein rein akademisches Problem handelt, dem in der Praxis keine Bedeutung zukommt.[5] Dass es zu § 203 StGB nur wenig Rechtsprechung gibt, dürfte insbesondere damit zusammenhängen, dass es sich bei diesem Straftatbestand um ein sogenanntes Antragsdelikt handelt, d.h. um ein Delikt, dessen Verfolgung einen Strafantrag des Betroffenen voraussetzt. An einem solchen Strafantrag wird es in der Regel aber fehlen. Denn den Betroffenen wird eine Offenbarung ihrer Geheimnisse oftmals nicht bekannt sein, da sie regelmäßig keinen Einblick in die interne Organisation der Praxis bzw. Kanzlei haben. Andere werden bewusst von einem Strafantrag absehen, da sie weiterhin beabsichtigen, den Arzt oder Rechtsanwalt aufzusuchen, und daher das Vertrauensverhältnis nicht zusätzlich belasten wollen oder weil sie eine außergerichtliche Lösung anstreben. Selbst wenn im Einzelfall ein Strafverfahren eingeleitet werden sollte, kann dies gegebenenfalls trotz eines Strafantrags durch eine Einstellung beendet werden.

Das entscheidende Problem für die Praxis besteht darin, dass wegen des Strafbarkeitsrisikos IT-Projekte unterlassen werden und Effizienzvorteile durch Nutzung von IT-Diensten nicht erzielt werden können. In der Praxis werden im Vorfeld von IT-Projekten häufig Anfragen bei Datenschutzbeauftragten, Kanzleien und Aufsichtsbehörden gestellt, ob das Vorhaben rechtskonform umgesetzt werden kann. Werden die Anfragenden auf die oben geschilderten Schwierigkeiten hingewiesen, nehmen sie nicht selten Abstand von den geplanten Projekten. Dass in solchen Fällen die Umsetzung mangels tragfähiger Strukturen unterbleibt, zeigt, dass noch größerer Bedarf an Regelungen besteht, die eine rechtssichere Lösung solcher Fallgestaltungen erlauben. Auch aus Sicht der Praxis wird demnach die derzeitige Ausgestaltung der Schweigepflicht den komplexen Strukturen der heutigen Arbeitswelt nicht mehr gerecht. Sie ist insbesondere nicht in der Lage, den Schutz des Rechts auf informationelle Selbstbestimmung mit den Erfordernissen der Berufswelt in Einklang zu bringen, und führt zu erheblicher Rechtsunsicherheit für alle Beteiligten.

Diese Problematik verschärft sich durch aktuelle gesetzliche Entwicklungen. So gibt der Gesetzgeber bestimmten Berufsgruppen (z.B. den Rechtsanwälten) über das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013 (BGBl. I S. 3786) die elektronische Kommunikation vor. Dabei fehlt diesen Berufsgruppen die rechtliche Möglichkeit, sich hierzu externe technische Unterstützung zu verschaffen, ohne die Verwirklichung des Tatbestands des § 203 StGB zu riskieren. Für den Bereich des Gesundheitswesens ist der Entwurf für ein E-Health-Gesetz angekündigt, um die Chancen der Telemedizin zu nutzen. Dabei soll eine Telematikstruktur die Beteiligten im Gesundheitswesen so verbinden, dass sie die für die Behandlung wichtigen medizinischen Informationen schnell, sicher und unbürokratisch austauschen können. Wenn Ärzte dabei die technische Hilfe externer Dienstleister benötigen, laufen sie jedoch ebenfalls Gefahr, sich nach § 203 Abs. 1 StGB strafbar zu machen. Die in § 203 StGB genannten Berufsgruppen benötigen deshalb Rechtssicherheit bei der Einbindung externer Kräfte.

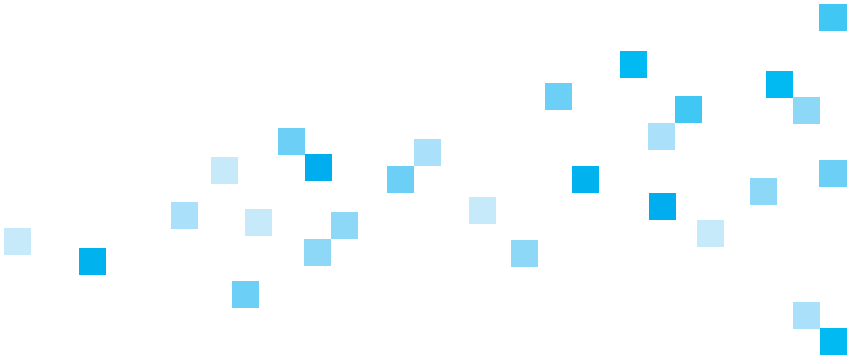
5 Als aktuelles Beispiel ist das Urteil des Landgerichts Flensburg vom 05.07.2013 (Az.: 4 O 54/11) zu nennen, in dem das (Zivil-)Gericht die Beauftragung eines externen Dritten mit der Pflege und Wartung der EDV-Anlage einer Arztpraxis als Verstoß gegen die ärztliche Schweigepflicht nach § 203 Abs. 1 StGB angesehen hat.

7 Notwendigkeit einer Gesetzesänderung

Vor diesem Hintergrund empfiehlt die AG „Rechtsrahmen des Cloud Computing“, die im Rahmen des Technologieprogramms „Trusted Cloud“ eingerichtet wurde, durch eine Änderung der rechtlichen Rahmenbedingungen die nötige Rechtssicherheit zu schaffen. Denn nur durch eine Gesetzesänderung kann sichergestellt werden, dass Berufsgeheimnisträger, die den Schutz der ihnen anvertrauten Geheimnisse ernst nehmen wollen, sich auch bei der Auslagerung von (IT-)Dienstleistungen gesetzeskonform verhalten können.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit wiederholt auf dieses Problem aufmerksam gemacht. So hat sie zuletzt Ende 2013 an die Regierungen und Parlamente von Bund und Ländern appelliert, für die zunehmende Einschaltung technischer Dienstleister, insbesondere durch Ärzte, angewiesene datenschutzgerechte Regelungen zu verabschieden.

Das Strafbarkeitsrisiko, das Berufsgeheimnisträger derzeit bei der Einschaltung von externen Dienstleistern zwangsläufig eingehen müssen, ist ihnen nicht länger zumutbar. Eine Änderung der rechtlichen Rahmenbedingungen erscheint dabei nicht nur im Hinblick auf die in § 203 StGB und § 353b StGB normierte Strafbarkeit, sondern auch in Bezug auf damit zusammenhängende strafprozessuale Vorschriften wie die Regelungen zum Zeugnisverweigerungsrecht und insbesondere zum Beschlagnahmeverbot erforderlich.



8 Potenzielle Lösungsansätze im Rahmen einer Gesetzesänderung

Für eine Gesetzesänderung sieht die AG „Rechtsrahmen des Cloud Computing“ derzeit im Wesentlichen vier Optionen. Diese sollen im Folgenden als Lösungsansätze zur Rechtsgestaltung in Grundzügen dargestellt werden.

→ Gesetzliche Änderung des Gehilfenbegriffs

Vorstellbar wäre, externe IT-Dienstleister in den Kreis der Gehilfen im Sinne des § 203 Abs. 3 Satz 2 StGB mit einzubeziehen. Nach § 203 Abs. 3 Satz 2 StGB stehen den Berufsgeheimnisträgern ihre berufsmäßig tätigen Gehilfen gleich. Hieraus wird mehrheitlich der Umkehrschluss gezogen, dass der Berufsgeheimnisträger Geheimnisse an seine Gehilfen (typischerweise etwas seine Praxis- und Kanzleihilfen) weitergeben darf, ohne die Geheimnisse zu offenbaren und sich strafbar zu machen.

Allerdings setzt § 203 Abs. 3 Satz 2 StGB den berufsmäßig tätigen Gehilfen dem Berufsgeheimnisträger in erster Linie insofern gleich, als eine Offenbarung von Geheimnissen durch ihn ebenso strafbar sein soll wie für den Berufsgeheimnisträger. § 203 Abs. 3 Satz 2 StGB ist insofern eine Strafnorm und kein strafrechtlicher Entlastungstatbestand für die Berufsgeheimnisträger.[6] Die Erweiterung des Gehilfenkreises um einen Dienstleister würde z. B. den Cloud-Anbieter ebenfalls einem Strafbarkeitsrisiko aussetzen. Unklar ist, inwieweit eine Erweiterung des Gehilfenkreises den cloud-nutzenden Berufsgeheimnisträger von seiner Strafbarkeit befreien würde. Überdies müssten beim Cloud Computing nur deutsche Cloud-Anbieter und nicht die vermutlich viel zahlreicheren ausländischen Cloud-Anbieter eine effektive Strafverfolgung fürchten.

→ Bezugnahme zur datenschutzrechtlichen Auftragsdatenverarbeitung

In § 203 StGB oder auch im Datenschutzrecht könnte eine Auftragsdatenverarbeitung auch für Berufsgeheimnisse vorgesehen werden, die sich mit § 11 BDSG deckt oder zumindest in den Tatbestandsmerkmalen daran anlehnt. Diskutiert wird deshalb auch eine entsprechende Anwendung des § 11 BDSG auf den Berufsgeheimnisschutz im Strafrecht. Die Weitergabe von Berufsgeheimnissen an einen Dienstleister wäre dann nicht strafbar, wenn dieser unter Weisungs- und Kontrollanforderungen beauftragt wurde, die mit den Vorgaben von § 11 BDSG vergleichbar sind.

Gegen eine solche Lösung können allerdings rechtssystematische Einwände erhoben werden. Eine Regelung im Datenschutzrecht wäre nicht ausreichend. Nach § 1 Abs. 3 Satz 2 BDSG bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, von den Regelungen des Bundesdatenschutzgesetzes „unberührt“. Zumindest hinsichtlich konkurrierender Zulässigkeitsfragen verdrängt das strafbewehrte Verbot der Offenbarung von Geheimnissen nach § 203 StGB die Zulässigkeit einer Datenweitergabe

6 Die Einbindung in den Kreis der zum Wissen Berufenen durch die herrschende Meinung ist nur insofern nachvollziehbar, als durch die Strafandrohung gegenüber dem Gehilfen der Schutz für den Betroffenen wohl derart gewährleistet wird, dass von seiner mutmaßlichen Einwilligung ausgegangen werden kann.

nach § 11 BDSG. Das Datenschutzrecht und seine Auftragsdatenverarbeitung einerseits sowie der strafbewehrte Berufsgeheimnisschutz andererseits haben darüber hinaus auch unterschiedliche Schutzrichtungen.

Fraglich ist, ob ein ausdrücklicher Verweis in § 203 StGB auf das Datenschutzrecht, etwa § 11 BDSG, eine geeignete Lösung darstellt. Der Berufsgeheimnisschutz hat, anders als das Datenschutzrecht, nicht die Reglementierung des Umgangs mit jeglichen personenbezogenen Daten im Blick. § 203 StGB schützt vielmehr das besondere Vertrauensverhältnis zwischen dem Berufsgeheimnisträger und dem Betroffenen. In diesem Verhältnis werden Geheimnisse – zum Teil aus faktischem Zwang oder im Vertrauen auf die besondere Qualifikation und Integrität des Berufsgeheimnisträgers – „anvertraut". Der Schutz der Auftragsdatenverarbeitung zielt nicht auf ein solches Vertrauens- und Näheverhältnis, sondern entsprechend § 11 Abs. 2 Satz 1 BDSG auf die Sicherstellung der technischen und organisatorischen Datensicherheit sowie die Möglichkeit zur Weisung und Kontrolle gegenüber der auftragnehmenden Stelle ab. Zudem würde eine spezifisch auf die Auftragsdatenverarbeitung abzielende Lösung nicht die Fälle abdecken, in denen der IT-Dienst auf anderer gesetzlicher Grundlage (z.B. § 28 BDSG, Forschungsklauseln) beruht.

→ Erlaubnis in Berufsgesetzen

Durch die Normierung einer Offenbarungsbefugnis in den Berufsordnungen könnte eine folgenlose Offenbarung gegenüber IT-Dienstleistern, ähnlich wie schon in § 49b Abs. 4 BRAO für die Abtretung von Vergütungsforderungen, ermöglicht werden. Eine Offenbarung kann dann auch keine strafrechtlichen Folgen mehr haben, denn was in den Berufsordnungen ausdrücklich erlaubt ist, kann durch § 203 StGB nicht strafrechtlich sanktioniert sein.

Eine solche Regelung ausschließlich in den Berufsordnungen würde jedoch zu einer Zersplitterung der Offenbarungsbefugnisse führen und zumindest solche in § 203 StGB genannten Berufsgeheimnisträger von der Rechtsunsicherheit nicht befreien können, die sich auf keine Berufsordnung oder keine entsprechende Regelung in ihrer Berufsordnung stützen können.

→ Konkretisierung des Offenbarungsbegriffs

Eine gesetzliche Neuregelung könnte schließlich eine Konkretisierung des Offenbarungsbegriffs zum Ziel haben. Eine Regelung würde folglich am Tatbestandsmerkmal der „unbefugten Offenbarung fremder Geheimnisse" aus § 203 Abs. 1 StGB ansetzen.

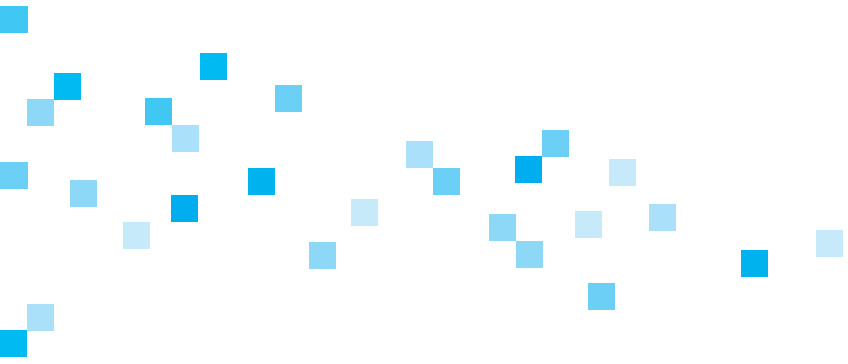
Hierbei könnte zum einen näher geregelt werden, ob und in welchen Fällen es zu einer strafbaren, da unbefugten Offenbarung kommt. Insbesondere könnte de lege ferenda klargestellt werden, ob und in welchen Fällen eine tatsächliche Kenntnisnahme des Dritten erfolgen muss und wann bereits die Ermöglichung der Kenntnisnahme für eine strafbare Offenbarung genügt. Zum anderen könnte der Offenbarungsbegriff dahingehend konkretisiert werden, dass die Weitergabe von Informationen an externe Dienstleister unter bestimmten, technisch oder rechtlich abstrakt bezeichneten Voraussetzungen noch keine Offenbarung im Sinne des § 203 Abs. 1 StGB darstellt.

Die Schwierigkeit für diesen Ansatz besteht darin, Tatbestand und Voraussetzungen einer privilegierten Weitergabe hinreichend konkret zu beschreiben und gleichwohl alle relevanten Fallgruppen zu erfassen.

Fazit

Derzeit besteht für Berufsgeheimnisträger bei Einschaltung externer IT-Dienstleister erhebliche Rechtsunsicherheit in Bezug auf eine Strafbarkeit nach § 203 StGB. Sowohl bei traditionellen Dienstleistungen wie IT-Wartung als auch bei neuen Formen wie Cloud Computing existiert für Berufsgeheimnisträger ein erhebliches Strafbarkeitsrisiko. Dies verhindert, dass das Potenzial dieser Dienste ausgeschöpft wird.

Zur Beseitigung des Strafbarkeitsrisikos und der bestehenden Rechtsunsicherheit ist eine Gesetzesänderung erforderlich. Insoweit bestehen unterschiedliche Lösungsansätze, die im Einzelnen diskutiert werden müssen. Insgesamt erscheint es dringend erforderlich, den Gesetzgebungsprozess unverzüglich in Gang zu setzen, um Berufsgeheimnisträgern die rechtssichere Nutzung von IT-Diensten zu ermöglichen.



Das Thesenpapier zur Schweigepflicht bei der Auslagerung von IT-Dienstleistungen

Das rechtspolitische Thesenpapier „Schweigepflicht bei der Auslagerung von IT-Dienstleistungen“ wurde durch Mitglieder der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ unter der Leitung von Prof. Dr. Georg Borges erarbeitet.

→ Mitwirkende/Autoren

Dr. Thorsten B. Behling, WTS Rechtsanwaltsgesellschaft mbH

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud

Mathias Cellarius, SAP SE

Dr. Astros Chatziastros, TMF e.V.

Dr. Johannes Drepper, TMF e.V.

Dr. Alexander Duisberg, Bird & Bird LLP

Günther Eble, Kommunale Informationsverarbeitung Baden-Franken

Alexander Glaus, Deutsche Bank AG

Björn Hajek, LL.M., Infineon Technologies AG

Dr. Marc Hilber, LL.M., Oppenhoff & Partner

Dr. Hubert Jäger, Uniscon universal identity control GmbH

Kristian Klodt, QSC AG

Rudi Kramer, DATEV eG

Thomas Kranig, Bayerisches Landesamt für Datenschutzaufsicht

Steffen Kroschwald, Universität Kassel

Jan Pohle, DLA Piper International LLP

Stephan Sädtler, Universität Passau

Gunther Schiefer, Karlsruher Institut für Technologie

Gabriel Schulz, Der Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Karin Vedder, Bayerisches Landesamt für Datenschutzaufsicht

Dr. Joseph Walenta, Deutsches Herzzentrum Berlin

Magda Wicker, Universität Kassel

Impressum

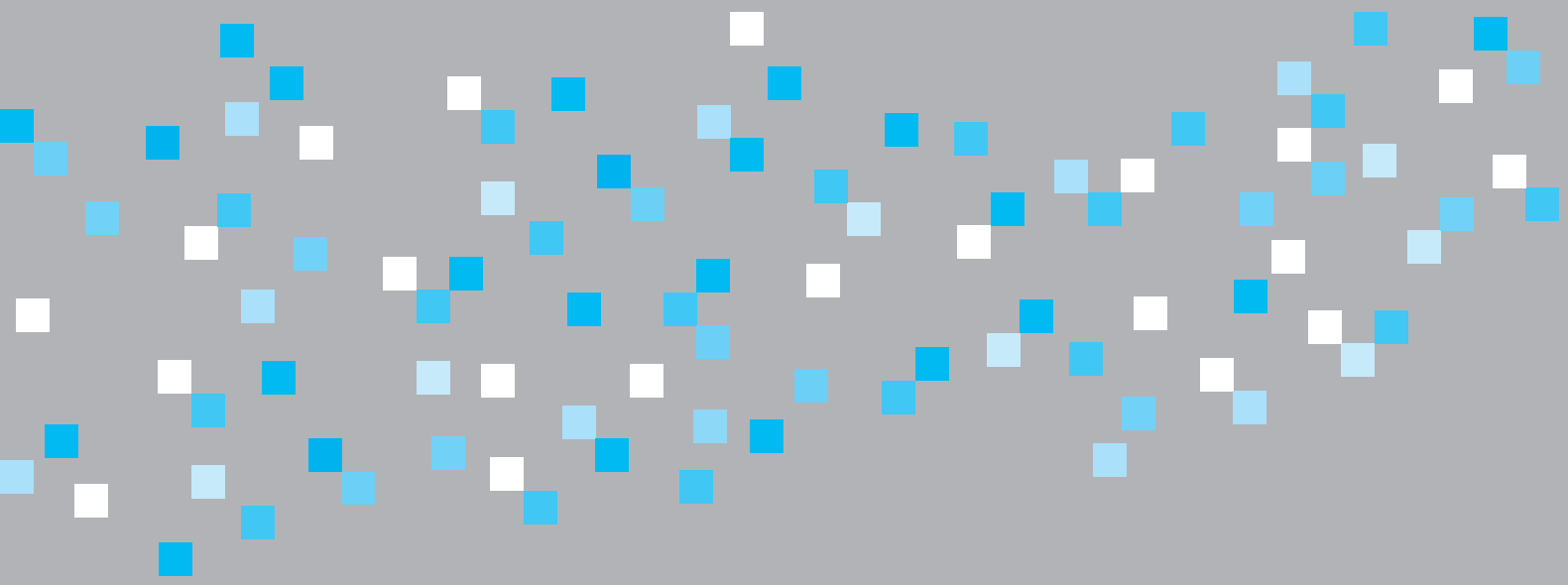
Herausgeber
Kompetenzzentrum Trusted Cloud
Arbeitsgruppe „Rechtsrahmen des Cloud Computing“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: Februar 2015



www.trusted-cloud.de