eBroschüre

Kazemi/Lenhard

Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

978-3-8240-5691-0

DeutscherAnwaltVerlag

eBroschüre

Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

Von

Rechtsanwalt
Dr. Robert Kazemi
Bonn

und

Dr. Thomas H. Lenhard
Rodalben

Zitiervorschlag:
Kazemi/Lenhard, Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei A Rn 1

Hinweis:

Die Formulierungsbeispiele in dieser eBroschüre wurden mit Sorgfalt und nach bestem Wissen erstellt. Sie stellen jedoch lediglich Arbeitshilfen und Anregungen für die Lösung typischer Fallgestaltungen dar. Die Eigenverantwortung für die Formulierung von Verträgen, Verfügungen und Schriftsätzen trägt der Benutzer. Autoren und Verlag übernehmen keinerlei Haftung für die Richtigkeit und Vollständigkeit der in der eBroschüre enthaltenen Ausführungen und Formulierungsbeispiele.

Anregungen und Kritik zu diesem Werk senden Sie bitte an: **kontakt@anwaltverlag.de**
Autoren und Verlag freuen sich auf Ihre Rückmeldung.

Copyright 2014 by Deutscher Anwaltverlag, Bonn
ISBN 978-3-8240-5691-0

DeutscherAnwaltVerlag

Inhalt

	Seite
Editorial	4
Interview mit Frau Dr. Auer-Reinsdorff zum Thema Datenschutz und Datensicherheit	6
A. Der Rechtsanwalt als Adressat des BDSG?	11
B. Datenschutz – Welche rechtlichen Rahmenbedingungen sind zu beachten	12
C. Pflicht zur Bestellung eines Datenschutzbeauftragten in der Anwaltskanzlei?	18
D. Keine Auskunftspflichten im Rahmen der Mandatsbearbeitung	24
E. Kommunikation und Datensicherheit	29
F. Voice-over-IP in der Anwaltskanzlei	36
G. Datenverlust trotz Datensicherung – Gefahren, die häufig unterschätzt werden	38
H. Warum Sie die Datenträger in Ihrer Kanzlei verschlüsseln sollten	41
I. Cloud-Computing und Weblösungen in der Anwaltskanzlei	43
J. Outsourcing in der Anwaltskanzlei – Ein berufs- und strafrechtliches Problem?	48
K. Aktenvernichtung und Archivierung	53
L. Datenschutz im Internet – Was ist auf der Kanzleiseite zu beachten	59
M. Beschäftigtendatenschutz – Grundlagen und ausgewählte Probleme	64
Glossar	75
Umfrageergebnisse	82

Editorial

Warum eine eBroschüre zum Datenschutz in der Kanzlei?

Als mich der Deutsche AnwaltVerlag fragte, ob ich die Mitarbeit an dem vorliegenden Werk übernehme, war ich zunächst kritisch. Datenschutz in der Anwaltskanzlei als Thema der Anwaltschaft? Viele werden hier im ersten Moment auf die anwaltlichen Berufspflichten verweisen, die den Datenschutz implizieren. Ist nicht gerade der Schutz des Mandantengeheimnisses eine der tragenden Säulen unseres Berufsstandes? Und macht nicht gerade dieser Umstand eine gezielte und genauere Betrachtung der Themen des Datenschutzrechts und der Datensicherheit in der Anwaltskanzlei obsolet? Einige wenige vertreten in der Tat die Nichtanwendbarkeit datenschutzrechtlicher Grundnormen des Bundesdatenschutzgesetzes (BDSG) in Bezug auf Rechtsanwälte und ihre Tätigkeit, andere wiederum wollen die datenschutzrechtlichen Bestimmungen des BDSG vollumfänglich auch auf Rechtsanwälte angewendet wissen. Die h.M. hingegen vertritt eine differenzierte Rechtsaufassung und will das BDSG nur dort verdrängt sehen, wo das anwaltliche Berufs- und Standesrecht konkretere Regelungen normiert hat. Welche Regelungen im Einzelnen Anwendung finden, ist – auch aus anwaltlicher Sicht – nur schwer zu beurteilen, wie aktuelle Vorgänge aus Bayern verdeutlichen. So berichtete die ***RAK München*** in ihrem Newsletter 5/2014[1] unter dem Titel **„Bay. Datenschutzaufsicht: Anlasslose Datenschutzprüfungen in Kanzleien“** davon, dass das Bayerische Landesamt für Datenschutzaufsicht (LDA) nach ihren Informationen derzeit "anlasslose Datenschutzprüfungen" nach § 38 BDSG in Anwaltskanzleien durchführe. In diesem Zusammenhang seien im Vorfeld zehn zufällig ausgewählte Prüfpunkte benannt worden, die Gegenstand der Prüfung sind. Die Kollegen der RAK München führen hier beispielhaft Fragen zu den folgenden Themenkomplexen auf:

- Datenschutzgerechte Datenträgervernichtung
- Einsatz einer Ende-Zu-Ende-Verschlüsselung bei E-Mail-Kommunikation
- Sicherer Abruf der E-Mails vom Mail-Server
- Sichere IT-Infrastruktur zwischen den Standorten
- Nutzung eines sicheren E-Mail-Dienstleisters
- Beanstandungsfreier Einsatz von Google-Analytics
- HTTPS-Verschlüsselung bei Einsatz besonderer Dienstleistungen über die Kanzlei-Website
- Einsatz von Leasing-Geräten (z.B. Drucker, Scanner, ...)
- Backup-Konzept der Datenträger
- Zutrittskontrolle

Vornehmlich, aber nicht ausschließlich also Fragen der (technischen) Datensicherheit, die den unvorbereiteten Kollegen sicherlich ins Grübeln bringen können. Ich will Ihnen natürlich nicht vorenthalten, dass ich es nicht bei einer Zitierung der Kammermitteilung belassen, sondern unmittelbar Kontakt zum LDA Bayern aufgenommen habe, um mehr zu erfahren. Die zuständige Sachgebietsleiterin berichtete davon, dass es sich hier nicht um ein „geplantes Vorgehen“ gegenüber Rechtsanwälten, sondern um routinemäßige Kontrollen handelte, die branchenübergreifend durchgeführt werden. Nach Aussage des LDA waren hiervon in Bayern bislang zwei Rechtsanwaltskanzleien betroffen. Ein Kollege entschied sich für die Zusammenarbeit mit dem LDA und erteilte Auskunft, er wurde auf vereinzelte Verbesserungsmöglichkeiten hingewiesen; das Verfahren war damit beendet. Der andere Kollege verwies auf die mangelnde Verpflichtung zur Auskunftserteilung und das anwaltliche Berufsrecht. Die hier aufgeworfenen Fragen werden aktuell nach Auskunft des LDA mit der BRAK erörtert, die ebenso die Auffassung vertritt, die Landesdatenschutzaufsicht sei für die Kontrolle der anwaltlichen Berufsausübung in

1 Abrufbar unter:
http://rak-muenchen.de/fileadmin/downloads/06-Mitgliederservice/04-Mitteilungsblatt%20Newsletter/02-Newsletter/2014/Newsletter05_2014.htm#Datenschutz.

datenschutzrechtlicher Hinsicht nicht zuständig. Diese Aufgabe komme allein den Rechtsanwaltskammern als Aufsichtsbehörden zu. Die Diskussion dauert an.

Die aktuellen Vorgänge aus Bayern belegen indes eines: Auch wir als Anwälte sollten uns mit Fragen des Datenschutzes und der Datensicherheit näher auseinandersetzen, anstatt hier die „Vogel-Strauß-Politik" zu betreiben, die wir unseren Mandanten stets auszureden versuchen. Denn ganz gleich, ob am Ende die Rechtsanwaltskammern oder die Landesdatenschutzbehörden die Einhaltung datenschutzrechtlicher Anforderungen in unseren Kanzleien überprüfen, sind diese Anforderungen existent. Daher sollten wir die Themen Datenschutz und Datensicherheit als Qualitätsmerkmal begreifen. Zusammen mit dem Sachverständigen für IT-Fragen, Dr. Thomas H. Lenhard, einem ausgewiesenen Experten in Fragen der Datensicherheit und langjährigem Datenschutzbeauftragten, will ich Ihnen mit dieser Broschüre hierzu eine Anleitung geben und Sie für Fragen des Datenschutzes und der Datensicherheit sensibilisieren. Denn anders, als man auf den ersten Blick meint, sind diese Themen im anwaltlichen Berufsalltag in zahlreichen Konstellationen zu beachten.

Diese eBroschüre versteht sich als Leitfaden für die tägliche Anwaltspraxis. Die einzelnen Beiträge sind dementsprechend nach Themenkomplexen gegliedert und in sich abgeschlossen. Lesen Sie also über das, was Sie gerade interessiert, ohne in der Broschüre hin und her blättern zu müssen. Etwaige einleitende Ausführungen können sich daher teilweise überschneiden, dies dient dem Konzept und liess sich nicht immer vermeiden. Über Rückfragen und Anmerkungen zu dieser eBroschüre freuen wir uns sehr.

Mit freundlichen kollegialen Grüßen

Dr. Robert Kazemi

Interview mit Frau Dr. Auer-Reinsdorff zum Thema Datenschutz und Datensicherheit

RAin Dr. Auer-Reinsdorff

Dr. Astrid Auer-Reinsdorff ist Fachanwältin für IT-Recht, Vizepräsidentin des Deutschen Anwaltvereins (DAV) und Vorsitzende der davit (Arbeitsgemeinschaft IT-Recht im DAV).

1. Welche datenschutzrechtlichen Vorschriften gelten für einen Rechtsanwalt in seinem Berufsalltag?

Bei der Datenverarbeitung in der Anwaltskanzlei ist zu unterscheiden zwischen den mandatsbezogenen Daten und Daten, die Kanzleiorganisation an sich betreffen. Kanzleiorganisatorische Daten sind die Daten der Beschäftigten der Kanzlei sowie der Bewerber um eine Anstellung, welche unter § 32 BDSG fallen, auch personenbezogene Daten von Lieferanten, Newsletter-Abonnenten und ähnliche Kontaktdaten ohne Mandatsbezug, welche von Mandantendaten trennbar gespeichert werden sollten und für die das Bundesdatenschutzgesetz (BDSG) einschränkungslos Anwendung findet. Daneben gehören zu den kanzleiinternen Daten die eigenen Finanzdaten, Vorlagen, Muster, Know-How, Login-Daten etc., welche zwar nicht dem Datenschutzrecht unterliegen, aber im Interesse der Kanzlei technisch und organisatorisch zu schützen sind.

Was die personenbezogenen Daten im Mandat angeht, unterliegen diese zunächst der anwaltlichen Verschwiegenheit (§ 203 StGB) und der Beschlagnahmefreiheit (§ 97 StPO). Wegen des § 1 Abs. 3 BDSG ist in der Literatur nach wie vor umstritten, ob das Bundesdatenschutzgesetz auf die Verarbeitung von personenbezogenen Daten im Mandat überhaupt keine Anwendung findet oder nur soweit, wie keine berufsrechtlichen Rahmenbedingungen beeinträchtigt würden.

Die Verschwiegenheitspflicht würde beeinträchtigt sein, wenn die zuständigen Landesdatenschutzbeauftragten bei uneingeschränkter Anwendbarkeit des Bundesdatenschutzgesetzes die Aufsicht über die Verarbeitung von personenbezogenen Daten im Mandat führen würden und Auskunftspflichten der Kanzlei diesen und/oder den Betroffenen gegenüber bestehen würden. Es betrifft die Auskunftspflichten über Art,

Umfang und Herkunft der gespeicherten und verarbeiteten Daten. Der Kern der anwaltlichen Arbeit ist es, Daten gerade nicht bei den Betroffenen selbst, also die personenbezogenen Daten der Gegner, Zeugen und sonstigen Beteiligten, sondern durch Information seitens des Mandanten zu erheben. Dies widerspricht dem datenschutzrechtlichen Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG). Im Interesse der Mandatsarbeit findet dieses Grundprinzip genauso wenig Anwendung wie die Verpflichtung zur Auskunftserteilung gegenüber dem Betroffenen nach § 34 BSDG, was auch zur Auskunft über die Herkunft der Daten verpflichten würde. Ferner könnten sich aus § 35 BDSG die Mandatsarbeit behindernde Löschungs- und Sperrungsansprüche der neben dem Mandanten Betroffenen ergeben.

Unabhängig davon, ob man von einer generellen Unanwendbarkeit des BDSG auf die mandatsbezogene Verarbeitung von personenbezogenen Daten ausgeht oder das BDSG mit den sich aus der Verschwiegenheit und den sonstigen Bedingungen der Berufsausübung ergebenden Einschränkungen für anwendbar ansieht, sind die technischen und organisatorischen Maßnahmen des Datenschutzes (§ 9 mit Anlage) sowie die Rahmenbedingungen für die Verarbeitung von personenbezogenen Daten im Auftrag (§ 11 BDSG) zum Schutz der Datenverarbeitung der Kanzlei sinnvoll.

Daneben sind die datenschutzrechtlichen Rahmenbedingungen des Telemediengesetzes (§§ 11 bis 15 a TMG) für den Webauftritt der Kanzlei, Einträge in Online-Branchenportalen, Bewertungsplattformen, Sozialen Diensten, Newsletter-Abonnements und die E-Mail-Kommunikation zu berücksichtigen.

2. Wenn Sie an grundsätzliche Sicherheitsvorkehrungen und Maßnahmen für Anwälte denken, welche könnten Sie empfehlen?

Analog den Anforderungen des § 9 BDSG mit Anlage sind die dort beschriebenen technischen und organisatorischen Maßnahmen sinnvoll. Besonderer Augenmerk sollte auf die Schulung der Mitarbeiter sowie deren Unterrichtung und ggf. Verpflichtung auf den Datenschutz analog § 5 BDSG sowie die Datensicherungen in Form von Back-ups und das Bereithalten von Verschlüsselungslösungen gelegt werden.

Da Anwaltskanzleien heute selbstverständlich einen Internetzugriff am Arbeitsplatz benötigen, ist es erforderlich, dass eine aktuelle Firewall-Lösung sowie eine laufend aktualisierte Antiviren-Software zum Einsatz kommen.

Außerdem sind den Nutzern der Systeme jeweils personenspezifische Benutzerkonten einzurichten und Berechtigungskonzepte zu entwerfen, die jedem Mitarbeiter die Rechte im System einräumen, welche für die tägliche Arbeit benötigt werden. Dies sollte aber nicht nach dem Prinzip „Alle haben auf alles Zugriff und entsprechende Bearbeitungs- und Löschungsrechte“ ablaufen.

Die Datensicherung der Kanzleidaten hat zuverlässig und regelmäßig zu erfolgen. Für den Ausfall der EDV-Systeme, Fehlfunktionen und drohende Datenverluste ist Vorsorge zu treffen.

Auch die zum Einsatz kommende Software ist dringend ausreichend lizenziert und jeweils aktualisiert einzusetzen. Für die mobilen Arbeitsgeräte ist zu prüfen, ob Daten verschlüsselt abgelegt werden, sowie die Nutzung öffentlicher WLAN-Zugänge ist kritisch zu prüfen und ggf. über einen Hotspot VPN abzusichern. Ebenso sind die Möglichkeiten des Zugriffs auf das Kanzleisystem von extern über VPN-Verbindungen abzubilden.

3. Was muss der Anwalt bei seiner elektronischen Kommunikation per E-Mail, WebAkte, DeMail usw. beachten (z.B. mit Mandanten und gegnerischen Anwälten)?

Über alle diese Kommunikationswege erfolgt die Kommunikation ohne Ende-zu-Ende-Verschlüsselung, d.h. die jeweiligen Provider und Dienstleister können bei Verstoß gegen ihre vertraglichen Verpflichtungen die Inhalte mitlesen. Bei einfacher E-Mail ist darüber hinaus auch der Transportweg ungeschützt, d.h. bei der Übermittlung könnte die Nachricht abgefangen werden und ist als Klartext unmittelbar auswert-

bar. Die elektronische Kommunikation erfordert generell ähnlich wie beim Verwenden einer Faxnummer einer genauen Adressatenkontrolle vor Versand. Das Risiko der Auswahl eines falschen Adressaten ist bei einfacher E-Mail aus einem Mailprogramm insbesondere wegen der Adressergänzungsfunktion und der Funktionalität „allen antworten" mit höheren Risiken der versehentlichen Übermittlung an den falschen Adressaten verbunden. Einer einfachen E-Mail fehlt zudem das Merkmal der Authentizität des Absenders und Empfängers.

DeMail hingegen bietet den Vorteil, dass der Inhaber des Accounts sich durch Identitätsnachweis bei der Einrichtung autorisiert. Über den Einsatz von DeMail lässt sich insbesondere das elektronische Einschreiben realisieren, was selbstverständlich voraussetzt, dass der Adressat auch ein DeMail-Postfach inne hat und dies als Zustellmöglichkeit eröffnet hat.

Davon zu unterscheiden ist der ePostbrief, welcher zur Identifizierung des Inhabers des Kontos derzeit kein DeMail-Gesetz konformes Verfahren einsetzt, nämlich postIdent. Der ePostbrief bietet aber den Vorteil, dass der Versender seine Adressaten erreichen kann, ohne vor Versand unterscheiden zu müssen, ob er an eine E-Mail-Adresse oder an eine Briefpostadresse versendet. Der Dienstleister würde bei fehlender E-Mail-Adresse die Nachricht ausdrucken, kuvertieren und auf dem Postweg zustellen. Ähnlich wie DeMail kann der Dienstleister bei der Umwandlung von Dateiformat in Briefpost vom Inhalt der Nachricht Kenntnis erlangen, auch wenn er eine besondere Lösung für Berufsgeheimnisträger anbietet, welche die Verschlüsselung des Inhalts standardmäßig abwickelt.

Die Web-Akte bietet gegenüber DeMail und ePostbrief den Vorteil, dass sowohl Anwalt als auch Mandant und jeder Benutzer, den die Anwaltskanzlei einrichtet, Dokumente hochladen kann und über den Mandatsverlauf die Dateien dauerhaft im Zugriff sind. Aber auch hierbei wären im Zweifel die Dateien zu verschlüsseln und/oder mit dem Mandanten im Voraus abzustimmen, dass er den Service nutzen möchte und in dem Ablegen seiner Mandatsakte in dem externen Ordner kein Offenbaren im Sinne des § 203 StGB sieht sowie in Kauf nimmt, dass die Daten dort im Zweifel der Beschlagnahmefreiheit nicht unterliegen könnten. Hier kann die Anwaltskanzlei erwägen, die Kosten der einzelnen mandatsbezogenen Web-Akte an den Mandanten als Auslage weiter zu geben und mit Mandatsende die einzelne Web-Akte zu löschen.

Eine weitere Möglichkeit der verschlüsselten Kommunikation, verbunden aber mit einer erheblichen Investition, ist ein Verschlüsselungs-Gateway, welches für die Kanzlei verschiedene Verschlüsselungsmethoden über einen Service verarbeiten kann, ohne dass die Kanzlei individuell die Nachrichten entschlüsseln müsste. Hier können Adressaten sich auf unterschiedliche Art und Weise authentifizieren, z.B. per qualifizierter elektronischer Signatur, PGP-Verschlüsselungszertifikat etc.

Bei nahezu allen Verschlüsselungsmöglichkeiten – auch mit dem Verschlüsselungszertifikat in Verbindung mit der qualifizierten elektronischen Signatur (QES) – darf der Anwender der zertifikatsausstellenden Stelle vertrauen, dass diese nicht vertrags- und rechtswidrig Mechanismen einsetzt, um die Verschlüsselung zu umgehen.

4. Welche Besonderheiten gelten bei der elektronischen Kommunikation mit Gerichten und Behörden?

Hier ist seit Jahren das Elektronische Gerichts- und Verwaltungspostfach (EGPV)[2] im Einsatz. Das EGVP hat den Vorteil, durch die Nutzung des OSCI-Verfahrens mit XML-Verschlüsselung die Inhalte derart zu übermitteln, dass der Dienstleister die Nachricht nicht mitlesen kann. Ohne dass es einer Aktion des Nutzers bedarf, tauscht das EGVP-Postfach des Senders mit dem Empfänger die Verschlüsselungsschlüssel nach dem Prinzip des doppelten Briefumschlags aus, d.h. das Postfach des Senders übermittelt

2 http://www.egvp.de.

sein öffentliches Verschlüsselungszertifikat an den Empfänger. Dieser verschlüsselt sein geheimes Zertifikat mit dem öffentlichen Zertifikat des Senders und versendet diese an das Senderpostfach. Das Senderpostfach entschlüsselt mit seinem geheimen zu seinem öffentlichen Schlüssel passenden Schlüssel und kann dann den geheimen Schlüssel des Empfängerpostfachs verwenden, um die Nachricht zu verschlüsseln, welche dann das Empfängerpostfach mit dem öffentlichen Schlüssel öffnen kann. Dokumente können einfach mit der qualifizierten elektronischen Signatur zuverlässig eingereicht werden. Durch die Funktion der Empfangsbestätigung kann der Sender kurzfristig die erfolgreiche Übermittlung überprüfen.

Das EGVP hat bislang den Nachteil, dass jedermann ohne jegliche Authentifizierung ein EGVP-Postfach einrichten kann. Nur die Gerichts- und Behördenliste (siehe Liste der Teilnehmer unter www.egvp.de) eröffnet die Kommunikation mit verifizierten Adressaten. Über SAFE (Secure Access to Federated e-Justice/e-Government) und das besondere elektronische Anwaltspostfach (beA) werden ab spätestens 1.1.2016 auch alle in Deutschland zugelassenen Rechtsanwälte identifiziert und bestätigt erreichbar sein, so dass die elektronische Zustellung von Anwalt zu Anwalt möglich werden wird.

5. Oft werden externe IT-Dienstleister beauftragt, die in Berührung mit sensiblen Daten kommen. Was gilt in einem solchen Fall zu beachten?

Mit den IT-Dienstleistern, welche die Kanzlei-EDV einrichten und administrieren, soll vor Arbeitsaufnahme eine Verschwiegenheitsvereinbarung abgeschlossen werden, welche zwar nur privatrechtlichen Bindungscharakter hat, aber den Dienstleister über die Besonderheiten bei der Betreuung der IT-Systeme in einer Anwaltskanzlei aufklärt. Entsprechend den Vorgaben des § 11 BDSG sollte eine Vereinbarung über die Verarbeitung von personenbezogenen Daten im Auftrag abgeschlossen werden (ADV – Auftragsdatenverarbeitungsvereinbarung). Bei den Wartungsarbeiten sollen die Dienstleister möglichst nicht unbeobachtet und unkontrolliert Zugriff auf die Systeme erhalten. Dies gilt auch für Fernwartungsmaßnahmen, sog. Remote-Zugriffe, bei denen der befugte Kanzleimitarbeiter vorzugsweise den Zugriff im Wartungs- oder Supportfall jeweils freischaltet. Ferner sollte die Verwaltung der Kanzleidaten derart organisiert sein, dass auf den einzelnen Arbeitsplatzrechnern möglichst keine Daten gespeichert werden, so dass im Reparaturfall der Dienstleister das Endgerät nicht mit dem gesamten Datenbestand außerhalb der Kanzlei verbringt.

Für die Nutzung von IT-Dienstleistungen wie moderne Cloud-Lösungen und Outsourcing-Lösungen, welche das IT-gestützte Arbeiten in allen Wirtschaftsbereichen sowie im Privaten erleichtern und oft preiswert und/oder mit höheren Sicherheitsniveaus für die datenverarbeitenden Anlagen Ressourcen effizient nutzen, ist in Bezug auf Mandantendaten anzuraten, Daten – bis auf Weiteres – verschlüsselt abzulegen. Hier sind die Entwicklungen im Berufsrecht zu beobachten, da seit dem DAV-Symposium zum IT-Outsourcing der Anwaltskanzlei am 29.3.2012[3] über zweifelsfreie und von der widerruflichen Zustimmung des Mandanten losgelöste einheitliche Rahmenbedingungen diskutiert wird. Für manche technische Gegebenheiten wird deren berufsrechtliche Unangreifbarkeit auch heute kaum in Zweifel gezogen, z.B. die Freischaltung einer Domain, was nur mittels eines Providers möglich ist, der theoretisch unter Verstoß gegen seine vertraglichen Verpflichtungen Zugriff auf die E-Mail-Kommunikation nehmen könnte. Die Verschlüsselung im Einzelfall ist aufwendig, weshalb eine Lösung zu bevorzugen ist, die ohne weiteres Zutun des Nutzers die Daten verschlüsselt wie z.B. doculife.

6. Wann muss ein Datenschutzbeauftragter bestellt werden?

Ein Datenschutzbeauftragter muss jedenfalls dann bestellt werden, wenn mehr als neun Personen, die nach Köpfen unabhängig von ihrer Funktion und der Art ihrer Beschäftigung als Teil- oder Vollzeitkräfte

3 http://anwaltsblatt.anwaltverein.de/rechtsprechung-details/items/Outsourcing_trotz_Anwaltsgeheimnis.html.

oder Auszubildende gezählt werden, mit der elektronischen Verarbeitung nicht mandatsbezogener Personendaten befasst sind. Auch wenn diese Personenanzahl mit der Verarbeitung mandatsbezogener Personendaten befasst ist, macht es Sinn, einen Datenschutzbeauftragten zu benennen, um diese Aufgabe verantwortlich zuzuweisen, auch wenn man der Auffassung folgt, das BDSG würde auf Mandatsdaten generell keine Anwendung finden.

7. Welche Tipps können Sie in Bezug auf die Benutzung von mobilen Geräten und Anwendungen im Berufsalltag geben?

Mobilen Geräten ist eine erhöhte Aufmerksamkeit zu widmen, um sie vor Verlust und Beschädigung zu schützen. Ferner sollte überlegt werden, Blickschutzfolien für das Arbeiten an öffentlichen Orten zu verwenden, damit umstehende Personen nicht mitlesen können. Der Zugriff auf die Daten ist mit dem Login-Passwort mit kurzer Zeitspanne zur Sperrung bei Nichtaktivität zu schützen. Ebenfalls ist zu überlegen, Verschlüsselungstools zu nutzen, um ggf. einzelne Ordner gesondert zu schützen, oder aber einen Speicherstick zu verwenden, auf dem die Mandatsinformationen verschlüsselt transportiert werden können.

Beim Einsatz von Verschlüsselungslösungen ist eine erhöhte Vorsorge zu treffen, dass der User das Verschlüsselungspasswort nicht vergisst, da es hierbei keine Passwortwiederherstellen-Funktionalität geben kann. Dies gilt z.B. auch für verschlüsselte Nachrichten-Apps wie eSIMS oder Hoccer.

Einfach zu handhaben und komfortabel für das Arbeiten unterwegs sind solche Speicherdienste wie Dropbox, die als Apps verfügbar sind, welche aber nicht ohne eine Verschlüsselungslösung zum Einsatz kommen sollten. docwallet bringt z.B. die Verschlüsselung in der Berufsgeheimnisträger-Variante bereits mit.

A. Der Rechtsanwalt als Adressat des BDSG?

Der Rechtsanwalt übt gemäß §§ 1, 2 Bundesrechtsanwaltsordnung (BRAO) einen freien und unabhängigen Beruf aus. Dabei unterliegt er verschiedenen strafbewehrten berufsrechtlichen Geheimhaltungspflichten, insbesondere denen aus § 43a Abs. 2 BRAO, § 50 BRAO sowie § 2 der Berufsordnung der Rechtsanwälte (BORA). Auf europäischer Ebene existieren ebenfalls Berufsregeln der Rechtsanwälte der Europäischen Union (sogenannte CCBE-Regeln), die unter Ziff. 2.3 ebenfalls Geheimhaltungspflichten des Rechtsanwaltes normieren. Wegen der Ausstrahlwirkung der vorgenannten anwaltlichen Berufspflichten auf das Datenschutzrecht wird vertreten, dass die Bestimmungen des BDSG gegenüber den berufsrechtlichen Bestimmungen subsidiär seien. Alle Daten, die unter das Anwaltsgeheimnis fallen, wären dementsprechend dem Anwendungsbereich des BDSG vollständig entzogen. Übrig blieben lediglich Daten ohne jeglichen Bezug zur eigentlichen anwaltlichen Tätigkeit, wie dies bei Daten des Büropersonales und beispielsweise bei Lieferantendaten der Fall sein mag.[4] Die herrschende Meinung[5] vertritt hingegen die Ansicht, dass die Anwendung des BDSG durch die Regelung des anwaltlichen Berufsrechts grundsätzlich nicht verdrängt, sondern lediglich ergänzt wird. Um mit den Worten *Sabine Leutheusser-Schnarrenbergers* zu sprechen: **1**

> *„Berufsrechtliche Verschwiegenheitspflicht und Datenschutzrecht sind, bildlich gesprochen, zwei Kreise mit unterschiedlichen Schutzrichtungen, die sich nur teilweise überschneiden: So reicht die Verschwiegenheitspflicht beispielsweise weiter als das Datenschutzrecht, weil sie nicht nur personenbezogene Daten, sondern alle Geheimnisse umfasst. Und das Datenschutzrecht reicht weiter, weil es nicht auf den Schutz des Mandanten beschränkt ist“.*[6]

Dasselbe gilt für Verwaltungsvorschriften, Anordnungen und Erlasse, die zur Auslegung der Vorschriften des BDSG herangezogen werden können. Die Subsidiarität tritt bezogen auf den Rechtsanwalt – nach herrschender Meinung – dementsprechend nur dann ein, wenn eine Tatbestandskongruenz vorliegt, d.h. wenn die spezielleren Regelungen des anwaltlichen Berufsrechtes inhaltlich einen Reglungsgegenstand des BDSG umfassen. Werden bestimmte Sachverhalte durch die spezifischen Regelungen hingegen nicht erfasst, so bleibt das BDSG nach herrschender Meinung insofern – lückenfüllend – anwendbar. **2**

Da die Anwaltschaft in heutiger Zeit fast vollständig automatisiert Daten verarbeitet, sind auch Rechtsanwälte damit grundsätzlich potenzielle Adressaten der datenschutzrechtlichen Normen des BDSG. Aus § 1 BDSG ist dementsprechend nur die partielle Nichtanwendbarkeit des BDSG auf solche Daten abzuleiten, die dem Berufsgeheimnis der Anwaltschaft unterliegen. Dies schließt die Anwendung des BDSG auf die anwaltliche Datenverarbeitung jedoch nicht aus. Es begrenzt aber die Anwendung bestimmter Vorschriften dahingehend, dass im Konfliktfall das Berufsgeheimnis stets vorgeht. Weder das Strafrecht noch das anwaltliche Berufsrecht stellen hingegen originäres Datenschutzrecht dar. Die hier normierten Verpflichtungen an den Rechtsanwalt strahlen allenfalls auf das Datenschutzrecht aus. **3**

4 So *Rüpke*, NJW 2008, 1121, 1122; *ders.*, ZRP, 2008, 87.

5 *Weichert*, NJW 2009, 550, 551; *ders.,* in: Schneider (Hrsg), FS für Heussen, 2009, S. 119; *Redeker*, NJW 2009, 554, 555 ff.; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 6 Rn 12.

6 *Leutheusser-Schnarrenberger*, AnwBl 2012, 477.

B. Datenschutz – Welche rechtlichen Rahmenbedingungen sind zu beachten

Das Datenschutzrecht war in den vergangenen 20 Jahren einer Vielzahl gesetzlicher Änderungen unterworfen. Vor allem die vergangenen fünf Jahre haben – auch bedingt durch eine Vielzahl von „Datenskandalen" – weitreichende Neuerungen hervorgebracht. Mit der Zahl und der Häufigkeit der Gesetzesänderungen hat sich auch die Rolle des Datenschutzrechts gewandelt. Von einem Randthema rücken Fragen des Datenschutzes immer weiter in den Fokus der anwaltlichen Beratungstätigkeit. Das Rechtsgebiet des Datenschutzes ist dabei für viele Anwälte und Anwältinnen nur schwer überschaubar, oft fehlt es an den notwendigen Grundlagen, um Probleme in diesem Bereich frühzeitig zu erkennen und die Mandanten entsprechend zu beraten. Gerade weil in Zeiten des Internets viele ganz unterschiedliche Unternehmungen mit verschiedensten Daten (Personaldaten, Nutzerdaten aus dem Internet, Kundendaten etc.) in Kontakt kommen, ist heute dennoch nahezu jeder Rechtsanwalt mit Fragen des Datenschutzrechtes befasst, ohne zugleich Spezialist auf diesem Gebiet zu sein. Dies gilt nicht zuletzt auch im Rahmen der eigenen Berufsausübung, bei der der Rechtsanwalt in verschiedenen Konstellationen mit dem Datenschutz in Kontakt kommt, sei es im Zusammenhang der Mandatsbearbeitung oder auch im Umgang mit Mitarbeitern/Mitarbeiterdaten der eigenen Kanzlei. Welche Regeln es hier zu beachten gilt, ist auf den ersten Blick nur schwer zu überblicken. Verschärft wird die Problematik zudem durch einen seit langer Zeit bestehenden (vermeintlichen) Konflikt des spezifischen anwaltlichen Berufsrecht zu den allgemeinen Bestimmungen des Datenschutzrechts, wie sie vornehmlich im BDSG und im Telemediengesetz (TMG) durch den Gesetzgeber normiert wurden. 1

Anwaltliches Berufsrecht ist kein (originäres) Datenschutzrecht

Der Rechtsanwalt übt gemäß §§ 1, 2 Bundesrechtsanwaltsordnung (BRAO) einen freien und unabhängigen Beruf aus. Dabei unterliegt er verschiedenen strafbewehrten berufsrechtlichen Geheimhaltungspflichten, insbesondere denen aus § 43a Abs. 2 BRAO, § 50 BRAO sowie § 2 der Berufsordnung der Rechtsanwälte (BORA). Auf europäischer Ebene existieren ebenfalls Berufsregeln der Rechtsanwälte der Europäischen Union (sogenannte CCBE-Regeln), die unter Ziff. 2.3 ebenfalls Geheimhaltungspflichten des Rechtsanwaltes normieren. 2

§ 43a BRAO

§ 43a BRAO verpflichtet den Rechtsanwalt zur Verschwiegenheit und bezieht diese Pflicht grundsätzlich auf alles, was ihm in Ausübung seines Berufes bekannt geworden ist. Nur solche Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen, sind von der Verschwiegenheitsverpflichtung des § 43a Abs. 2 BRAO nicht umfasst. 3

Demgegenüber schützt das BDSG den Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Sicherlich kann der Verstoß des Rechtsanwaltes gegen die ihm in § 43a Abs. 2 BRAO auferlegte Verschwiegenheitspflicht zugleich einen Eingriff in das Persönlichkeitsrecht des jeweiligen Mandanten bedeuten. Der Rechtsanwalt erhebt und verarbeitet im bestehenden Mandatsverhältnis zahlreiche personenbezogenen (Mandanten-) Daten, sodass sich die Frage stellt, ob auch der Rechtsanwalt im Rahmen seiner Berufsausübung Bestimmungen des BDSG unterliegt. Die Verschwiegenheitspflicht des § 43a Abs. 2 BRAO und der Umgang mit **personenbezogenen Daten des Mandanten** weisen zwar Gemeinsamkeiten auf, dennoch ist die Schutzrichtung beider Vorschriften eine andere. Mit dem Grundrecht auf informationelle Selbstbestimmung hat das zentrale Anliegen des § 43a Abs. 2 BRAO, die Verschwiegenheitspflicht, nur wenig gemein. Der Mandant ist im Rahmen einer bestehenden Mandatsbeziehung stets Herr der Verschwiegenheitspflicht des Anwaltes, und zwar nicht nur hinsichtlich seiner eigenen (personenbezogenen) Daten, sondern auch hinsichtlich der Daten Dritter, die der Anwalt preisgeben darf und muss, wenn der Mandant dies wünscht. 4

Der Schutz personenbezogener Daten im Rahmen des § 43a Abs. 2 BRAO ist lediglich Rechtsreflex der Vorschrift, die primär das bestehende Vertrauensverhältnis zwischen Anwalt und Mandant einem besonderen Schutz unterstellt.

So ist es nach § 43a Abs. 2 BRAO beispielsweise unzulässig, das Bestehen eines Mandatsverhältnisses überhaupt bekannt zu geben, soweit dieses nicht schon anderweitig bekannt ist. § 43a Abs. 2 BRAO verbietet grundsätzlich auch die Nennung von „Referenzmandaten" ohne Einwilligung des Mandanten; was in der Kanzlei gesprochen wird, soll in der Kanzlei bleiben. Schon die Veröffentlichung von Urteilen gegen oder zugunsten des Mandanten ohne dessen Einwilligung wäre im Rahmen des § 43a Abs. 2 BRAO sicherlich unzulässig. Gleiches gilt für die Weitergabe von Informationen des Mandanten an Dritte, weswegen die Vorschrift des § 43a BRAO über die Bestimmungen des BDSG hinausgeht. Sie ist – da § 28 Abs. 1 BDSG nur in beschränktem Maße Anwendung findet – in vielen Punkten wesentlich strenger. Während die Datenerhebung und -verarbeitung personenbezogener Daten im Rahmen bestehender rechtsgeschäftlicher oder rechtsgeschäftsähnlicher Schuldverhältnisse und unter Berücksichtigung der berechtigten Interessen der datenerhebenden Stelle sowie der schutzwürdigen Belange des Betroffenen auch ohne Einwilligung des Betroffenen zulässig sein kann, zeigen die vorgenannten Beispiele, dass es im Rahmen der Datenerhebung und -verarbeitung nach § 43a Abs. 2 BRAO grundsätzlich immer einer Einwilligung des Mandanten bedarf. Das zwischen Anwalt und Mandant bestehende und durch § 43a Abs. 2 BRAO geschützte Vertrauensverhältnis überlagert insoweit die ansonsten im Rahmen datenschutzrechtlicher Wertungen vorzunehmende Interessenabwägung und muss dazu führen, dass die schutzwürdigen (Geheimhaltungs-)Interessen des Mandanten die berufsbezogenen Interessen des Rechtsanwaltes, beispielsweise dahingehend, mit bestimmten Referenzmandaten Werbung zu treiben, stets überwiegen. 5

§ 50 BRAO

Auch § 50 BRAO trifft Bestimmungen, die im weitesten Sinne datenschutzrechtliche Aspekte betreffen. Nach § 50 Abs. 2 BRAO hat der Rechtsanwalt Handakten zu führen, die er auf die Dauer von fünf Jahren nach Beendigung des Mandatsauftrages aufzubewahren hat. Diese Verpflichtung erlischt nur dann schon vor Beendigung dieses Zeitraumes, wenn der Rechtsanwalt den Auftraggeber aufgefordert hat, die Handakten in Empfang zu nehmen und der Auftraggeber dieser Aufforderung binnen sechs Monaten, nachdem er sie erhalten hat, nicht nachgekommen ist (§ 50 Abs. 2 S. 2 BRAO). 6

§ 50 Abs. 3 BRAO normiert, dass der Rechtsanwalt seinem Auftraggeber (Mandant) die Herausgabe seiner Handakten verweigern kann, bis er wegen seiner Gebühren und Auslagen befriedigt ist. Zu den Handakten des Anwaltes zählen nicht der Briefwechsel zwischen dem Rechtsanwalt und seinem Auftraggeber und die Schriftstücke, die dieser bereits in Urschrift erhalten hat. Diese Informationen hat der Rechtsanwalt an seinen Mandanten auch unter Berücksichtigung der Verpflichtung des § 50 BRAO nicht herauszugeben und auch nicht im Sinne des § 50 Abs. 2 BRAO über den dort genannten Fünfjahreszeitraum aufzubewahren. 7

Sicherlich tut der Anwalt nicht schlecht daran, seine Handakten vollständig über einen gewissen Zeitraum aufzubewahren. Die daraus resultierenden umfassenden Archivflächen dürften jedem Rechtsanwalt, der seine Kanzlei über einen längeren Zeitraum führt, hinlänglich bekannt sein. Schon mit Blick auf etwaige Schadensersatzansprüche, die sich aus vermeintlichen Anwaltsfehlern begründen, empfiehlt es sich, die Aufbewahrung der Handakten auch über die Dauer von fünf Jahren hinweg zu bedenken. 8

Die Handakten des Rechtsanwaltes beinhalten eine Fülle von personenbezogenen Daten. Sie sind insoweit Datenspeicher im Sinne des BDSG. Die Anwaltsakten sind zudem systematisch gegliedert, weswegen insoweit Überschneidungen zum Grundsatz der Datensparsamkeit und zur Löschungsverpflichtung des § 35 BDSG bestehen können. Die Verpflichtung, seine Handakten über einen Zeitraum von mindes- 9

tens fünf Jahren aufzubewahren, steht der Löschungsverpflichtung des § 35 Abs. 2 Nr. 3 BDSG grundsätzlich entgegen, wonach Daten, die für eigene Zwecke verarbeitet werden, grundsätzlich zu löschen sind, sobald ihre Kenntnisse für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich sind.

Bezogen auf das anwaltliche Mandatsverhältnis als Dienstverpflichtung höherer Art, könnte dementsprechend argumentiert werden, dass der Anwalt verpflichtet sei, die im Rahmen der Mandatsführung erhobenen personenbezogenen Daten unmittelbar nach Beendigung des Mandats zu löschen. Dieser Argumentation steht § 50 Abs. 2 BRAO entgegen, der insoweit lex specialis zu der in § 35 Abs. 2 BDSG normierten Löschungsverpflichtung ist. § 50 Abs. 2 BRAO stellt insoweit eine in § 35 Abs. 3 Nr. 1 BDSG genannte gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfrist dar, die einer Löschung nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG entgegensteht. Nach § 35 Abs. 3 BDSG tritt in diesem Fall an die Stelle einer Löschung grundsätzlich eine Sperrungsverpflichtung des Rechtsanwaltes. Die Datensperrung muss dazu führen, dass die Daten, die in der Handakte vorhanden sind, nicht mehr verarbeitet oder genutzt werden können. Um dies sicherzustellen, sind gesperrte Daten zu kennzeichnen (§ 3 Abs. 4 Nr. 4 BDSG), was beispielsweise durch die Herausnahme der Akten aus dem laufenden Mandatsregister und Einfügung in die Archivlisten geschehen kann. Hinsichtlich der sodann im Archiv befindlichen Handakten hat der Rechtsanwalt gemäß § 35 Abs. 3 BDSG sicherzustellen, dass die dort gelagerten Daten vor dem unberechtigten Zugriff Dritter geschützt werden. **10**

§ 2 BORA

Auch § 2 BORA normiert eine Verschwiegenheitsverpflichtung des Anwaltes. Nach Absatz 1 ist der Rechtsanwalt „zur Verschwiegenheit berechtigt und verpflichtet". Dieses Recht und die Pflicht zur Verschwiegenheit beziehen sich auf alles, was dem Rechtsanwalt in Ausübung seines Berufs bekannt geworden ist, und bestehen auch nach Beendigung des Mandats fort. Die Pflicht zur Verschwiegenheit gilt nur dann nicht, soweit die Berufsordnung oder andere Rechtsvorschriften Ausnahmen zulassen oder die Durchsetzung oder Abwehr von Ansprüchen aus dem Mandatsverhältnis oder die Verteidigung des Rechtsanwaltes in eigener Sache die Offenbarung erfordert. Die Schutzrichtung des § 2 BORA gleicht insoweit der Schutzrichtung des § 43a BRAO. Anders als die Vorschrift des § 43a BRAO bezieht § 2 BORA die Mitarbeiter des Rechtsanwaltes in die dem Anwalt obliegende Verschwiegenheitspflichten mit ein. Auch § 2 BORA schützt damit das Vertrauensverhältnis zwischen Anwalt und Mandant und nicht primär die personenbezogenen Daten des Mandanten. Soweit über die Verschwiegenheitsverpflichtung dennoch der Schutz personenbezogener Mandantendaten sichergestellt wird, kann auch dies nur als bloßer Rechtsreflex der anwaltlichen Verschwiegenheitsverpflichtung angesehen werden. **11**

Ziff. 2.3. CCBE

Schließlich normiert Ziff. 2.3 CCBE (Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers = Berufsregeln der Rechtsanwälte der Europäischen Union),[7] dass es zum Wesen der Berufstätigkeit des Rechtsanwaltes gehört, **12**

> *„dass sein Mandant ihm Geheimnisse anvertraut und er sonstige vertrauliche Mitteilung erhält. Ist die Vertraulichkeit nicht gewährleistet, kann kein Vertrauen entstehen. Aus diesem Grund ist das Berufsgeheimnis gleichzeitig ein Grundrecht und eine Grundpflicht des Rechtsanwaltes von besonderer Bedeutung. Die Pflicht des Rechtsanwaltes zur Wahrung des Berufsgeheimnisses dient dem Interesse der Rechtspflege ebenso wie dem Interesse des Mandanten. Daher verdient sie besonderen Schutz durch den Staat."*

7 Abrufbar unter: http://www.brak.de/w/files/02_fuer_anwaelte/Berufsregeln_Mai%202006_090615.pdf.

Der Rechtsanwalt hat die Vertraulichkeit aller Informationen zu wahren, die ihm im Rahmen seiner beruflichen Tätigkeit bekannt werden, diese Pflicht zur Wahrung des Berufsgeheimnisses gilt nach Ziff. 2.3 CCBE grundsätzlich zeitlich unbegrenzt.

§ 203 StGB

Die vorbeschriebenen berufs- und standesrechtlichen Verschwiegenheitsverpflichtungen des Rechtsanwaltes werden strafrechtlich durch die Norm des § 203 StGB flankiert, der die unbefugte Offenbarung fremder Geheimnisse durch besonders benannte Geheimnisträger unter Strafandrohung stellt. In § 203 Abs. 1 Nr. 3 StGB wird der Rechtsanwalt als Adressat und möglicher Täter der vorbenannten Strafnorm bezeichnet. Dem in § 203 Abs. 1 Satz 1 StGB Genannten stehen gemäß § 203 Abs. 3 StGB ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (Rechtsreferendare). 13

§§ 53, 53a StPO

Korrespondierend mit der Verpflichtung des Rechtsanwaltes, ihm anvertraute Geheimnisse keinem Dritten zu offenbaren, finden sich die in der Strafprozessordnung normierten Zeugnisverweigerungsrechte der § 53 Abs. 1 Nr. 3 StPO (für den Rechtsanwalt) und des § 53a Abs. 1 StPO (für seine Gehilfen und die Personen, die zur Vorbereitung auf den Beruf an seiner berufsmäßigen Tätigkeit teilnehmen). 14

Auch die strafrechtlichen Bestimmungen schützen also wiederum das Vertrauensverhältnis zwischen Anwalt und Mandant. Es geht auch im Rahmen der strafrechtlichen Bewertungen nicht primär um den Datenschutz, d.h. den Schutz vor der Verwendung personenbezogener Daten im Lichte des Grundrechts auf informationelle Selbstbestimmung, sondern vorwiegend um den Schutz des zwischen Anwalt und Mandant bestehenden und von Verfassungs wegen garantierten Vertrauensverhältnisses.

Zwischenergebnis

Festzuhalten bleibt, dass weder das anwaltliche Berufsrecht noch das Strafrecht originäres Datenschutzrecht darstellen.[8] 15

Neben dem Berufsrecht gelten die Datenschutzgesetze

Dies ist der Grund, warum neben den Bestimmungen des anwaltlichen Berufsrechts auch die in den Datenschutzgesetzen normierten Verpflichtungen im anwaltlichen Berufsalltag zu beachten sind. Vornehmlich ist hier sicherlich das Bundesdatenschutzgesetz (BDSG) zu nennen, aber auch die spezialgesetzlichen Regelungen im Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) gilt es zu beachten. 16

Bundesdatenschutzgesetz (BDSG)

§ 1 Abs. 1 BDSG normiert den Zweck des Gesetzes dahingehend, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird." Hierzu regelt das BDSG die Tätigkeiten der Datenerhebung, der Datenverarbeitung und der Datennutzung und stellt dem Einzelnen wie auch den staatlichen Aufsichtsbehörden zur Kontrolle dieser Tätigkeiten umfassende Auskunfts- und Berichtigungs-, Löschungs- und Beschwerderechte zur Seite. Ins- 17

8 *Sabine Leutheusser-Schnarrenberger* formuliert dies im AnwBl 2012, 477 wie folgt: *„Berufsrechtliche Verschwiegenheitspflicht und Datenschutzrecht sind, bildlich gesprochen, zwei Kreise mit unterschiedlichen Schutzrichtungen, die sich nur teilweise überschneiden: So reicht die Verschwiegenheitspflicht beispielsweise weiter als das Datenschutzrecht, weil sie nicht nur personenbezogene Daten, sondern alle Geheimnisse umfasst. Und das Datenschutzrecht reicht weiter, weil es nicht auf den Schutz des Mandanten beschränkt ist."*

besondere letztere nehmen im Diskurs um die Anwendbarkeit des Bundesdatenschutzgesetzes im Rahmen der anwaltlichen Berufsausübung einen zentralen Stellenwert ein, können sie doch leicht mit den anwaltlichen Berufspflichten, insbesondere der anwaltlichen Verschwiegenheitspflicht kollidieren. Wegen der Ausstrahlwirkung der anwaltlichen Berufspflichten auf das Datenschutzrecht wird daher vertreten, dass die Bestimmungen des BDSG gegenüber § 43a Abs. 2 BRAO bzw. den in der BORA enthaltenen sonstigen Verschwiegenheitsverpflichtungen subsidiär seien. Alle Daten, die unter das Anwaltsgeheimnis fallen, wären dementsprechend dem Anwendungsbereich des BDSG vollständig entzogen. Übrig blieben lediglich Daten ohne jeglichen Bezug zur eigentlichen anwaltlichen Tätigkeit, wie dies bei Daten des Büropersonales und beispielsweise bei Lieferantendaten der Fall sein mag.[9]

Die herrschende Meinung[10] vertritt hingegen die Ansicht, dass die Anwendung des BDSG durch die Regelung des anwaltlichen Berufsrechts grundsätzlich nicht verdrängt, sondern lediglich ergänzt wird. Dasselbe gilt für Verwaltungsvorschriften, Anordnungen und Erlasse, die zur Auslegung der Vorschriften des BDSG herangezogen werden können. Die Subsidiarität tritt bezogen auf den Rechtsanwalt – nach herrschender Meinung – dementsprechend nur dann ein, wenn eine Tatbestandskongruenz vorliegt, d.h. wenn die spezielleren Regelungen des anwaltlichen Berufsrechtes inhaltlich einen Reglungsgegenstand des BDSG umfassen. Werden bestimmte Sachverhalte durch die spezifischen Regelungen hingegen nicht erfasst, so bleibt das BDSG nach herrschender Meinung insofern – lückenfüllend – anwendbar. **18**

Da die Anwaltschaft in heutiger Zeit fast vollständig automatisiert Daten verarbeitet, sind auch Rechtsanwälte damit grundsätzlich potenzielle Adressaten der datenschutzrechtlichen Normen des BDSG. Nur dort, wo es um solche Daten geht, die dem Berufsgeheimnis der Anwaltschaft unterliegen, bliebt das BDSG partiell unanwendbar. Dies schließt die Anwendung des BDSG auf die anwaltliche Datenverarbeitung jedoch nicht aus. Es begrenzt die Anwendung bestimmter Vorschriften lediglich dahingehend, dass im Konfliktfall das Berufsgeheimnis den Bestimmungen des BDSG vorzugehen hat. **19**

Telemediengesetz (TMG)

Am 1. März 2007 ist das "Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronisches-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG)"[11] in Kraft getreten. Mit ihm wurde das Telemediengesetz (TMG) eingeführt, welches die zuvor geltenden Regelungen des Teledienstegesetzes (TDG) und des Teledienstedatenschutzgesetzes (TDDSG) ersetzte. Das TMG gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TMG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgeschützte Dienste nach § 3 Nr. 25 TMG oder Rundfunk nach § 2 des RStV sind. Das TMG gilt darüber hinaus für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird, und umfasst damit sowohl die früheren Teledienste als auch die Dienste nach dem MDStV. Das TMG enthält in seinen §§ 11 bis 15 spezielle Regelungen zum Datenschutz in Telemediendiensten. Diese finden neben den Datenschutzvorschriften für Telekommunikationsdienste im TKG Anwendung und gehen für ihren Anwendungsbereich dem allgemeinen Datenschutzrecht im BDSG vor. **20**

Telekommunikationsgesetz (TKG)

Mit der Liberalisierung des Telekommunikationsmarktes bedurfte es zum Schutz von Kunden der nunmehr privatrechtlich organisierten Telekommunikationsdiensteanbieter umfangreicher Neuregelungen, **21**

9 So *Rüpke*, NJW 2008, 1121, 1122; *ders.*, ZRP, 2008, 87.

10 *Weichert*, NJW 2009, 550, 551; *ders.,* in: Schneider (Hrsg), FS für Heussen, 2009, S. 119; *Redeker*, NJW 2009, 554, 555 ff.; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 6 Rn 12.

11 BGBl 2007 I, S. 1719.

die eine Umsetzung des durch das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelten Rechts auf informationelle Selbstbestimmung sowie der unionsrechtlichen Vorgaben der Datenschutzrichtlinie sicherstellten. Der Gesetzgeber wollte zudem den Gefahren begegnen, die sich aus der Verwendung von Telekommunikationsdaten insbesondere für kommerzielle Zwecke ergeben. Das TKG sieht dementsprechend in Teil 7 (Fernmeldegeheimnis, Datenschutz, öffentliche Sicherheit) Vorschriften über den Datenschutz im Telekommunikationsbereich vor. Auch in diesem sektorspezifischen Datenschutz finden gemäß § 1 Abs. 3 BDSG die Bestimmungen des BDSG nur dann Anwendung, soweit die Spezialregelungen nicht Platz greifen.

Der siebte Teil des TKG gliedert sich in insgesamt drei Abschnitte. Der erste Abschnitt (§§ 88 bis 89 TKG) beinhaltet Regelungen zum Fernmeldegeheimnis. Im zweiten Abschnitt (§§ 91 bis 107 TKG) finden sich die speziellen datenschutzrechtlichen Vorschriften und im dritten Abschnitt (§§ 108 bis 115 TKG) die Vorschriften über die öffentliche Sicherheit. Die Übergänge sind fließend.[12] Wesentliche Vorschriften des dritten Abschnittes haben unmittelbare Auswirkungen auf den Datenschutz, z.B. die Diskussion über die Vorratsdatenspeicherung nach § 113a TKG, wie das in der breiten Öffentlichkeit beachtete Verfassungsgerichtsurteil[13] zur Vorratsdatenspeicherung zeigt. Neben der Vorratsdatenspeicherung sind die Vorschriften des TKG insbesondere auch dann von Bedeutung, wenn es um die Herausgabe von dynamischen IP-Adressen zwecks Verfolgung von Urheberrechtsverstößen geht,[14] die vor allem im Rahmen der sogenannten Massenabmahnungsfälle Bedeutung erlangen. Ebenfalls von zentraler Bedeutung ist § 98 TKG, der die Nutzung sogenannter Standortdaten für Dienste mit Zusatznutzen regelt. Auf die einzelnen Bestimmungen des TKG wird im Rahmen der Fallbetrachtungen näher eingegangen. **22**

12 *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, Einf. TKG Rn 5.

13 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256, 263, 586/08, BVerfGE 125, 260 = NJW 2010, 833; aus der zahlreichen Literatur dazu vgl. *Ohler*, JZ 2010, 626; *Wolff*, NVwZ 2010, 751; *Blankenburg*, MMR 2010, 587; *Westphal*, EuZW 2010, 494; vgl. auch EuGH, Urt. v. 10.2.2009 – Rs. C-301/06, Slg. 2009, I-593 = NJW 2009, 1801 zur Rechtsgrundlage der Vorratsdatenspeicherung im europäischen Recht.

14 *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, Einf. TKG Rn 5.

C. Pflicht zur Bestellung eines Datenschutzbeauftragten in der Anwaltskanzlei?

Nach § 4f BDSG besteht für nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und hierzu mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Unter automatisierter Verarbeitung versteht das BDSG die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (§ 3 Abs. 2 BDSG). Unter einer Datenverarbeitungsanlage (Abk.: DVA) ist ein elektronisches System zu verstehen, welches Daten annimmt, speichert, verarbeitet und abgibt (beispielsweise PC, aber auch große Rechenzentren). Bereits heute ist der Einsatz von EDV im Rahmen der Mandatsbearbeitung in der Rechtsanwaltskanzlei eher die Regel denn die Ausnahme; so nutzen allein ca. 14.000 Rechtsanwaltskanzleien im Bundesgebiet die Kanzleisoftware des Branchenprimus RA-Micro.[15] Studien zum Einsatz von Informationstechnik in der Anwaltskanzlei in den Jahren 2010 bis 2013 gehen von einer aktuellen Nutzungsquote in Höhe von ca. 86 % aus.[16] Spätestens mit Inkrafttreten des durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten neu geschaffenen § 130d ZPO und seiner Entsprechensregelungen in den besonderen Prozessregeln der Fachgerichtsbarkeiten zum 1.1.2022, die den Rechtsanwalt **verpflichten,** vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen als elektronisches Dokument zu übermitteln, wird sich die Nutzungsquote auf 100 % erhöhen. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen hat in der Rechtsanwaltschaft damit eine enorme Bedeutung. Es liegt also nahe, von einer Anwendbarkeit des § 4f BDSG in der Rechtsanwaltskanzlei auszugehen. So einfach die Feststellung auf den ersten Blick erscheinen mag, so kompliziert stellt sich die tatsächliche Rechtslage bei näherem Hinsehen dar. Sind Rechtsanwälte verpflichtet, einen Datenschutzbeauftragten zu bestellen, und wenn ja, wie weit reicht diese Verpflichtung und welche Aufgaben kommen dem Datenschutzbeauftragten im Falle der Bestellpflicht zu? 1

Die BRAK gegen den Rest der Welt? – Keine Verpflichtung zu Bestellung eines Datenschutzbeauftragen im Rahmen der mandatsbezogenen Datenverarbeitung

In einer – soweit ersichtlich – nach wie vor Geltung beanspruchenden Stellungnahme der BRAK aus September 2004[17] und einer Ergänzung selbiger im März 2005[18] wird die These vertreten, der Rechtsanwalt sei bezüglich seiner mandatsbezogenen Informationsverarbeitung **nicht verpflichtet**, einen Beauftragten für Datenschutz zu bestellen. Nur soweit regelmäßig mindestens 10 Personen mit der Personaldatenverarbeitung beschäftigt seien, sei ein „auf diesen Verarbeitungsbereich beschränkter Datenschutzbeauftragter" zu bestellen. Selbst Großkanzleien werden kaum über eine derartig personenstarke Personalabteilung verfügen, so dass die Bestellung eines Datenschutzbeauftragten in der Rechtsanwaltskanzlei nach dieser Ansicht faktisch keine Rolle spielen dürfte. 2

Die BRAK begründet ihre Rechtsauffassung im Wesentlichen mit einem Anwendungsvorrang der Bestimmungen des anwaltlichen Berufs(ausübungs)rechts und dem Verweis auf die Norm des § 1 Abs. 3 BDSG, wonach andere Rechtsvorschriften des Bundes, die die Verarbeitung personenbezogener Daten einschließlich deren Veröffentlichung regeln, den Vorschriften des BDSG vorgehen. Die BRAK verkennt dabei nicht, dass weder die BRAO noch die BORA spezifische Regelungen zur Kontrolle der Da- 3

15 Zahlen der RA MICRO.

16 Studie nicht repräsentativ, abrufbar unter http://www.treysse.com/2013/10/18/einsatz-von-informationstechnik-in-der-anwaltskanzlei-2013/.

17 BRAK Stellungnahme Nr. 31/2004, abrufbar unter: http://www.brak.de/w/files/stellungnahmen/StnBDSinKanzleien-2004.pdf.

18 http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2005/maerz/stellungnahme-der-brak-2005-10.pdf.

tenverarbeitung im Mandatsverhältnis enthalten oder gar Regelungen zum Themenkomplex des Datenschutzbeauftragten in der Rechtsanwaltskanzlei vorhalten. Auch sonstige, die anwaltliche Berufsausübung betreffende Regelungswerke, insbesondere die straf- und strafprozessrechtlichen Regelungen in § 203 StGB und §§ 53, 53a StPO, verhalten sich zu dieser Frage nicht. Mit Blick auf das hohe Schutzgut der anwaltlichen Verschwiegenheit und das – auch von Verfassungs wegen – geschützte Recht auf eine (weitgehend) staatlicher Kontrolle entzogene anwaltliche Beratung, sei eine Verpflichtung zur Bestellung eines – den staatlichen Datenschutzaufsichtsbehörden zur Auskunft verpflichteten – betrieblichen Datenschutzbeauftragten gleichwohl nicht durchsetzbar. Die Anwendung datenschutzrechtlicher Normen, insbesondere derer, die die Bestellung eines Datenschutzbeauftragten fordern, bedinge insoweit eine „Aufweichung oder Durchbrechung der anwaltlichen Verschwiegenheitspflicht" und führte dazu, dass „Mandanten sich ihren anwaltlichen Vertretern nicht mehr uneingeschränkt anvertrauen könnten."

Da der Rechtsanwalt bei Bestellung eines Datenschutzbeauftragten leicht in die Situation geraten könne, seinen fachlich hochspezifischen Informationsumgang von angestellten Junganwälten, Rechtsanwaltsfachangestellten oder sonstigen Gehilfen kontrollieren zu lassen, ergäbe sich eine „unvertretbare Gefährdung der Unabhängigkeit des eigenverantwortlichen Rechtsanwalts". Insgesamt wäre die Tätigkeit eines Datenschutzbeauftragten in der Rechtsanwaltskanzlei damit durch die quasi-neutrale Rolle – zwischen Datenverarbeiter und Betroffenen – gekennzeichnet, wie sie ihm das BDSG zuweist (§ 4f Abs. 3, 4 und 5 S. 2). Danach könnte die paradoxe Situation eintreten, dass ein Datenschutzbeauftragter sich gegenüber dem Rechtsanwalt für das Recht auf informationelle Selbstbestimmung des Prozessgegners einzusetzen hätte, und zwar auch aufgrund von Kenntnissen, die ihm nur aufgrund interner EDV-Aktenkontrolle zugänglich geworden sind. 4

Schließlich sei auch die im BDSG vorgesehene Möglichkeit, dass sich der Datenschutzbeauftragte in Zweifelsfällen an die Aufsichtsbehörde wenden kann oder muss, mit dem Berufsgeheimnis nicht zu vereinbaren. 5

Gesetzgeber und Literatur sind weitgehend anderer Auffassung

Die Auffassung der BRAK, die auch in zahlreichen aktuellen Stellungnahmen zur Reform des europäischen Datenschutzrechts vertreten wird,[19] ist – auch in der Rechtsanwaltschaft – nicht nur auf Zustimmung gestoßen. Nachdem der DAV ursprünglich die Auffassung der BRAK teilte, ist hier ein zumindest partielles Abrücken von der Rechtsauffassung festzustellen. Frau Kollegin *Auer-Reinsdorff* formuliert hier vorsichtig, dass ein Datenschutzbeauftragter jedenfalls dann bestellt werden müsse, wenn mehr als neun Personen, die nach Köpfen unabhängig von ihrer Funktion und der Art ihrer Beschäftigung als Teil- oder Vollzeitkräfte oder Auszubildende gezählt werden, mit der elektronischen Verarbeitung personenbezogener Daten nicht mandatsbezogener Daten befasst sind. Die Frage, ob dies auch für die mandatsbezogenen Daten gilt, bleibt offen. In der Datenschutz-Checkliste für die Anwaltskanzlei des DAV[20] heißt es hierzu jedoch, dass sich auch bei „reiner mandatsbezogener Datenverarbeitung" die Ernennung eines Datenschutzbeauftragten empfehle. Dabei könne die Anwaltskanzlei einen internen Angestellten – nicht die Inhaber der Kanzlei oder den IT-Beauftragten – oder aber einen externen Dritten beauftragen. 6

Helmut Redeker[21] formuliert noch deutlicher und führt aus, dass selbstverständlich auch die Anwaltschaft verpflichtet ist, nach § 4f BDSG einen betriebliche Datenschutzbeauftragten zu bestellen, der auch die anwaltliche Datenverarbeitung im Hinblick auf die dem Berufsgeheimnis unterliegenden Daten zu beauf- 7

19 Stellungnahmen der BRAK Nr. 30/2012, 53/2012 und 25/2013.

20 Abrufbar unter: http://www.anwaltverein.de/downloads/praxis/mustervertrag/ChecklisteDatenschutz.pdf.

21 *Redeker*, NJW 2009, 554, 556.

sichtigen habe. Für die Argumentation der BRAK verbliebe anlässlich der klaren gesetzgeberischen Zielsetzungen des BDSG ersichtlich kein Raum.[22]

Neben der Mehrzahl der Aufsichtsbehörden[23] stellen sich weitere namhafte Institutionen[24] auf den Standpunkt, dass auch der Rechtsanwalt bei Vorliegen der sonstigen Voraussetzungen auch dann einen Datenschutzbeauftragten zu bestellen habe, soweit es um die Bearbeitung mandatsbezogener Daten gehe. 8

Datenschutzbeauftragter ab 10 Personen erforderlich, aber auch sinnvoll

Auch wir teilen die Auffassung der BRAK nicht. Sie mag berufspolitisch nachvollziehbar sein. Zahlreiche Argumente, die gegen eine Bestellung in Bezug auf die mandatsbezogene Datenverarbeitung vorgebracht werden, sind indes wenig stichhaltig und durch aktuelle gesetzgeberische Korrekturen überholt. 9

So erstreckt § 203 Abs. 2a StGB die Verschwiegenheitspflicht auch auf den Beauftragten für den Datenschutz. Auch dieser darf Geheimnisse, die ihm in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden sind und von denen er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt, nicht einfach Dritten offenbaren. Damit aber wird der Beauftragte für den Datenschutz dem Rechtsanwalt als Berufsgeheimnisträger gleichgestellt und die Gefahr der „unbefugten" Offenbarung mandatsbezogener Informationen strafrechtlich sanktioniert. Entsprechend der zum Drittgeheimnis entwickelten Grundsätze[25] steht die Befugnis zur Erteilung eines Einverständnisses mit der Weitergabe allein dem Rechtsanwalt als dem ursprünglichen Geheimnisträger selbst zu, § 4f Abs. 4a BDSG. Der Gefahr der „Verletzung des Mandatsgeheimnisses" wird so wirksam begegnet. Gem. § 4f Abs. 4 BDSG ist der Beauftragte für den Datenschutz zudem zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen selbst befreit wird. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke zudem einem Beschlagnahmeverbot (§ 4f Abs. 4a S. 2 BDSG). Obgleich sich der Datenschutzbeauftragte im Rahmen seiner Aufgabenerfüllung „in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden" und deren Beratung in Anspruch nehmen kann, sind Verletzungen der anwaltlichen Verschwiegenheit damit tatsächlich nicht zu befürchten. 10

Auch ein Eingriff in die anwaltliche Berufsausübung geht mit der Verpflichtung zur Bestellung eines Datenschutzbeauftragten nicht einher. Zwar können dem Datenschutzbeauftragtem im Rahmen seiner Berufsausübung keine Weisungen erteilt werden, umgekehrt ist er selbst aber auch gegenüber dem Rechtsanwalt als verantwortliche Stelle nicht weisungsbefugt. Er wirkt – seiner Aufgabenzuweisung folgend – lediglich auf die Einhaltung von Datenschutzvorschriften hin. Hierunter ist nach gängiger Praxis nichts anderes zu verstehen, als dass er ihm auffällige datenschutzrelevante Sachverhalte erfasst, vermerkt, und 11

22 Ähnlich auch *Weitze*, DStR 2004, 2218 ff. für die Steuerberater; siehe auch Zuck, Vortragsfolien „Datenschutz in der Rechtsanwaltskanzlei", abrufbar unter: http://www.davit.de/uploads/media/praes-dr-zuck-ak-4.pdf; siehe auch *Weichert*, in: Kilian/Heussen, Computerrechts-Handbuch, 26. Ergänzungslieferung 2008, Teil 13, Rn 58; *Weichert*, NJW 2009, 550, 551; ders., in: Schneider (Hrsg), FS für Heussen, 2009, S. 119; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 6 Rn 12.

23 So bspw. ULD SH unter: https://www.datenschutzzentrum.de/wirtschaft/stellungnahme_brak.htm; Landesbeauftragter für Datenschutz und Informationsfreiheit NRW unter: https://www.ldi.nrw.de; Der Landesbeauftragte für den Datenschutz Baden-Württemberg, abrufbar unter: http://www.baden-wuerttemberg.datenschutz.de/verarbeitung-personenbezogener-daten-durch-rechtsanwalte/; siehe hierzu auch den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich vom 8.11.2007, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2007/20071108_Anwendbarkeit_des_Bundesdatenschutzgesetzes_auf_Rechtsanw__lte/Anwendbarkeit_des_Bundesdatenschutzgesetzes_auf_Rechtsanwaelte1.pdf.

24 So der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., abrufbar unter: https://www.bvdnet.de/system-ordner/tt-news/detailansicht/article/datenschutz-in-der-anwaltskanzlei-verbot-der-bestellung-eines-datenschutzbeauftragten.html; Gesellschaft für Datenschutz und Datensicherheit e.V, RDV 2004, S. 284.

25 Ausführlich hierzu: *Cierniak/Pohlit*, in: MüKo zum StGB, 2. Auflage 2012, § 203 Rn 77 ff.

– soweit es ihm eingeräumt wird – Änderungsvorschläge unterbreitet. Ob sich der Rechtsanwalt an den Empfehlungen des Datenschutzbeauftragten orientiert oder nicht, obliegt jedoch weiterhin allein diesem selbst. Er bleibt die allein verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG. Der Datenschutzbeauftragte berät und wahrt durch den einer Beratung immanenten Empfehlungscharakter seine Unabhängigkeit, aber auch die des Anwalts. Hierbei hat der Datenschutzbeauftragte, die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen und die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit dem Datenschutzrecht und der Datensicherheit vertraut zu machen. Hierin ist kein Verstoß gegen zwingendes anwaltliches Berufsrecht, sondern sicherlich eine sinnvolle Unterstützung des Rechtsanwaltes zu sehen, mit der eher eine Stärkung des von Unabhängigkeit und Verschwiegenheit geprägten Berufsbildes des Rechtsanwaltes verbunden ist.

Externe Bestellung eines Datenschutzbeauftragten zulässig

Mit dem DAV ist zudem davon auszugehen, dass auch der Rechtsanwalt nicht verpflichtet ist, sich im Rahmen der Bestellung eines Datenschutzbeauftragten auf bei ihm angestellte und ggf. nicht hinreichend qualifizierte Mitarbeiter zu beschränken. Auch der Rechtsanwalt kann sich vielmehr externer Datenschutzbeauftragter bedienen. Hierfür spricht bereits § 203 Abs. 2a StGB, der allgemein vom Beauftragten für den Datenschutz spricht und hier gerade nicht zwischen angestelltem („internen") und freiberuflich („externen") Datenschutzbeauftragten differenziert. Eine „Eingliederung" in die betriebliche Organisation des Rechtsanwaltes ist damit – anders als dies beispielsweise bei anderen externen Dienstleistern der Fall sein mag[26] – gerade nicht erforderlich. Auch die im BDSG normierten Aussageverweigerungsrechte, Beschlagnahme- und Verwertungsverbote gelten ebenso für den internen, wie für den externen Datenschutzbeauftragten. 12

Eine externe Bestellung kann dabei erhebliche Vorteile haben. So darf zum Datenschutzbeauftragten nämlich nur bestellt werden, wer die notwendige Fachkunde und Zuverlässigkeit besitzt. Der Düsseldorfer Kreis[27] stellt hier hohe Mindestanforderungen. 13

Unabhängig von der jeweiligen Branche und Größe des Unternehmens muss jeder Datenschutzbeauftragte über erhebliches Wissen im Datenschutzrecht verfügen. Dies umfasst unter anderem Grundkenntnisse zu den verfassungsrechtlich garantierten Persönlichkeitsrechten der von Datenverarbeitungen Betroffenen und der Mitarbeiter der Rechtsanwaltskanzlei. Zudem erfordert die Bestellung zum Datenschutzbeauftragten umfassende Kenntnisse der für die Kanzlei einschlägigen Regelungen des BDSG und der Spezialgesetze (BRAO, StGB). Schließlich hat der Datenschutzbeauftrage auch vertiefte Kenntnisse zur Datensicherheit, insbesondere technischer Natur, vorzuweisen. Hierzu ist der Rechtsanwalt verpflichtet (§ 4f Abs. 3 Satz 7 BDSG, § 4f Abs. 2 BDSG), dem betrieblichen Datenschutzbeauftragten die Erlangung und Erhaltung seiner Fachkunde erforderliche Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Die hiermit einhergehende finanzielle Belastung ist nicht unerheblich. Es muss auch dem Rechtsanwalt daher unbenommen bleiben, sich hier externer Dienstleister zu bedienen. 14

Der DAV[28] empfiehlt in diesem Zusammenhang sogar **jeder Kanzlei,** sich einer Datenschutzschulung durch externe Berater zu unterziehen. Diese sollte auch umfassen, wie sich die Mitarbeiter bei der Anfrage einer Aufsichtsstelle (Datenschutzbeauftragter des Landes, zuständige Rechtsanwaltskammer) und bei Auskunfts- und Löschungsbegehren von Betroffenen zu verhalten haben. 15

26 Siehe hierzu den Beitrag „Outsourcing" in der Rechtsanwaltskanzlei – Ein Berufs- und strafrechtliches Problem?
27 Das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich.
28 http://www.anwaltverein.de/downloads/praxis/mustervertrag/ChecklisteDatenschutz.pdf.

Anforderungen an den und Aufgaben des Datenschutzbeauftragten

16 Unabhängig davon, ob sich der Rechtsanwalt für die Bestellung eines internen oder eines externen Datenschutzbeauftragten entscheidet, ist die Zuverlässigkeit des Beauftragten sicherzustellen. Diese erfordert neben der Fachkunde, dass kein Interessenkonflikt bei der Wahrnehmung der Funktion des Datenschutzbeauftragten besteht. Ein solcher besteht vor allem bei allen Personen, die ein eigenes Interesse am Unternehmen (etwa wegen Beteiligung an seinem Vermögen wie z.B. Teilhaber oder Gesellschafter) oder Leitungsfunktion haben. Partner einer Rechtsanwaltskanzlei sind damit keine geeigneten Datenschutzbeauftragten.

17 Die Aufgabe und Tätigkeit eines Datenschutzbeauftragten wird in den §§ 4f und 4g BDSG geregelt. Der Beauftragte für Datenschutz wirkt nach der gesetzgeberischen Intention auf die Einhaltung des BDSG und anderer Datenschutz-Gesetze hin. Die zentrale Aufgabe ist dabei die Unterstützung bei der ordnungsgemäßen Datenverarbeitung.

18 In dieser Funktion soll der Datenschutzbeauftragte auf die Einhaltung der Datenschutzbestimmungen hinwirken, indem er betriebsinterne Datenschutzvorgänge prüft und beurteilt, ob die zur Sicherung des Rechtes auf informationelle Selbstbestimmung getroffenen Maßnahmen ausreichen oder Verbesserungsmöglichkeiten bestehen. Dabei hat er neben der Zulässigkeit der Datenverarbeitung, auch die getroffenen Schutzmechanismen, insbesondere die EDV und das Netzwerk zu bewerten, was gleichsam ein gewisses technisches Verständnis erfordert. Die Prüfung und Überwachung hat in regelmäßigen Abständen nach eigenem Ermessen zu erfolgen. Sobald neue Verfahren in einem Betrieb eingeführt werden, ist der Datenschutzbeauftragte hierüber vorab zu informieren und in die Entscheidungsfindung einzubeziehen. Ein wesentliches Augenmerk liegt dabei darauf, dass ausschließlich Befugte eine nur auf den Zweck beschränkte Verarbeitung vornehmen können und dass der Eigentümer der Daten sein Selbstbestimmungsrecht auf Auskunft, Korrektur, Sperrung und Löschung wahrnehmen kann. Schließlich obliegt dem betrieblichen Datenschutzbeauftragten auch die Schulung der Mitarbeiter, um diese für die Belange des Datenschutzes zu sensibilisieren. Im Rahmen dieser Schulungstätigkeit hat der Datenschutzbeauftragte vor allem über mögliche Änderungen im Bereich der Datenschutzgesetzgebung zu informieren, soweit diese vom Unternehmen zu beachten sind. Den Datenschutzbeauftragten trifft damit gleichsam eine Verpflichtung, sich durch geeignete Fortbildungen und das Studium aktueller Gesetzgebungsvorhaben auf dem Laufenden zu halten.

19 Da der Datenschutzbeauftragte in seinem Funktionsbereich nicht immer populäre Entscheidungen trifft, sieht das Gesetz seine Weisungsfreiheit und Unabhängigkeit von Vorgesetzten in seinen Funktionsbereichen vor. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden und ist direkt der Geschäftsleitung unterstellt. Seit der Novellierung des BDSG im Jahre 2009 ist der Datenschutzbeauftragte zudem mit einem verbesserten Kündigungsschutz ausgestattet (§ 4f Abs. 3 BDSG) und kann, solange er seine Funktion innehat, lediglich außerordentlich gekündigt werden. Dieser Kündigungsschutz bleibt auch nach einer Abberufung als betrieblicher Datenschutzbeauftragter für ein weiteres Jahr nach der Beendigung der Bestellung bestehen.

20 Die Bestellung eines internen Datenschutzbeauftragten hat in der Regel für einen gewissen Zeitraum zu erfolgen, um sicherzustellen, dass er seine Tätigkeit im angemessenen Umfang ausführen kann. Je nach Bundesland werden dabei Zeiträume zwischen 3 und 5 Jahren als angemessen angesehen.

Wen trifft die Verpflichtung zur Bestellung eines Datenschutzbeauftragten?

21 Hier gilt § 4f S. 2 und 3 BDSG, der den nicht-öffentlichen Stellen, in denen mehr als neuen Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten auferlegt. Eine automatisierte Verarbeitung liegt vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von

Datenverarbeitungsanlagen erfolgt (§ 3 Abs. 2 BDSG). Eine Datenverarbeitungsanlage ist eine Einrichtung, die Daten nach vorgegebenen Programmen und Verfahren verarbeitet. In der Regel sind damit Computer im weitesten Sinne gemeint, auf denen personenbezogene Daten gespeichert und/oder bearbeitet werden.22Die Pflicht gilt, sobald **mind. 10 Personen regelmäßig** mit der automatisierten Verarbeitung beschäftigt sind. Hierunter fallen nicht nur Vollzeitkräfte, sondern auch freie Mitarbeiter, Auszubildende, Leiharbeiter, Praktikanten und Volontäre. **Nur kurzeitige Beschäftigte sind nicht zu berücksichtigen** (bspw. Urlaubsvertretungen). Die Zahl der "in der Regel" beschäftigten darf dabei nicht durch einfaches Abzählen an einem bestimmten Stichtag ermittelt werden; vielmehr erfordert die Feststellung der maßgeblichen Beschäftigtenzahl neben einem Rückblick auf die vergangene Lage des Betriebes insbesondere eine Einschätzung seiner zukünftigen Entwicklung. Notwendig ist also, dass der Mitarbeiter während des größten Teils des Jahres tätig ist bzw. voraussichtlich tätig sein wird, so dass eine nur vorübergehende Mehr- oder Minderbeschäftigung in aller Regel unbeachtlich ist.23Sobald innerhalb einer Rechtsanwaltskanzlei damit ständig mehr als 10 Personen, einschließlich des anwaltlichen Hilfspersonals, Zugriff auf die elektronische Patientendatenverwaltung haben, hat die Kanzlei einen betrieblichen Datenschutzbeauftragten zu bestellen. Wer als Arbeitgeber (Rechtsanwalt) selbst ein unternehmerisches Risiko trägt, wird nicht mitgezählt, so dass der oder die Kanzleiinhaber im Rahmen der 10-Personen-Grenze nach h.M. nicht zu berücksichtigen sind. In den Fällen, in denen keine elektronische Akte geführt wird, greift die Verpflichtung zur Bestellung zudem erst, wenn mindestens 20 Personen innerhalb der Rechtsanwaltskanzlei beschäftigt werden (§ 4f Abs. 1 S. 3 BDSG).

D. Keine Auskunftspflichten im Rahmen der Mandatsbearbeitung

Wegen der Ausstrahlwirkung der anwaltlichen Berufspflichten auf das Datenschutzrecht und mit Blick auf die Vorschrift des § 1 Abs. 3 BDSG, wird vertreten, dass die Bestimmungen des BDSG gegenüber § 43a Abs. 2 BRAO bzw. den in der BORA enthaltenen sonstigen Verschwiegenheitsverpflichtungen subsidiär seien. Alle Daten, die unter das Anwaltsgeheimnis fallen, wären dementsprechend dem Anwendungsbereich des BDSG vollständig entzogen. Übrig blieben lediglich Daten ohne jeglichen Bezug zur eigentlichen anwaltlichen Tätigkeit, wie dies bei Daten des Büropersonales und beispielsweise bei Lieferantendaten der Fall sein mag.[29] 1

Die herrschende Meinung[30] vertritt hingegen die Ansicht, dass die Anwendung des BDSG durch die Regelung des anwaltlichen Berufsrechts grundsätzlich nicht verdrängt, sondern lediglich ergänzt wird. Dasselbe gilt für Verwaltungsvorschriften, Anordnungen und Erlasse, die zur Auslegung der Vorschriften des BDSG herangezogen werden können. Die Subsidiarität tritt bezogen auf den Rechtsanwalt – nach herrschender Meinung – dementsprechend nur dann ein, wenn eine Tatbestandskongruenz vorliegt, d.h. wenn die spezielleren Regelungen des anwaltlichen Berufsrechtes inhaltlich einen Reglungsgegenstand des BDSG umfassen. Werden bestimmte Sachverhalte durch die spezifischen Regelungen hingegen nicht erfasst, so bleibt das BDSG nach herrschender Meinung insofern – lückenfüllend – anwendbar. 2

Da die Anwaltschaft in heutiger Zeit fast vollständig automatisiert Daten verarbeitet, sind auch Rechtsanwälte damit grundsätzlich potenzielle Adressaten der datenschutzrechtlichen Normen des BDSG. Aus § 1 BDSG ist dementsprechend nur die partielle Nichtanwendbarkeit des BDSG auf solche Daten abzuleiten, die dem Berufsgeheimnis der Anwaltschaft unterliegen. Dies schließt die Anwendung des BDSG auf die anwaltliche Datenverarbeitung jedoch nicht aus. Es begrenzt aber die Anwendung bestimmter Vorschriften dahingehend, dass im Konfliktfall das Berufsgeheimnis stets vorgeht. 3

Auskunfts- und Benachrichtigungspflichten gegenüber dem Mandanten?

Gemäß § 34 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten, die Empfänger, an die Daten weitergegeben werden, und den Zweck der Datenspeicherung zu erteilen. Nach § 33 Abs. 1 BDSG ist der Betroffene für den Fall, dass erstmals personenbezogene Daten für eigene Zwecke ohne seine Kenntnis gespeichert werden, von der Speicherung zu benachrichtigen (§ 33 Abs. 1 BDSG). Die Benachrichtigungspflicht besteht nicht, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung seiner personenbezogenen Daten erlangt oder die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen. 4

Auch die vorgenannten Auskunfts- und Benachrichtigungspflichten gegenüber dem Mandanten verstoßen nicht gegen die Geheimhaltungspflichten des anwaltlichen Berufsrechts. §§ 33, 34 BDSG sind mithin im Mandatsverhältnis grundsätzlich anwendbar. Da die Speicherung der personenbezogenen Mandantendaten einer gesetzlichen Aufbewahrungspflicht folgt (§ 50 BRAO), muss der Mandant über die erstmalige Erhebung der Daten jedoch nicht gesondert informiert werden (§ 33 Abs. 2 BDSG). Hinzu kommt, dass Mandanten bei der Begründung von Mandatsverhältnissen in aller Regel freiwillig eine Vielzahl personenbezogener Daten über sich preisgeben und eine Datenerhebung ohne Kenntnis des Betroffenen grundsätzlich nicht stattfindet. Dies mag anders sein, wenn der Rechtsanwalt in Vorbereitung eines potenziellen Mandats beispielsweise Recherchen über seinen künftigen Mandaten einholt. In diesem Fall wären die zu diesem Zwecke erhobenen personenbezogen Daten des potenziellen Mandanten, sollte es 5

29 So *Rüpke*, NJW 2008, 1121, 1122; *ders.*, ZRP, 2008, 87.

30 *Weichert*, NJW 2009, 550, 551; *ders.,* in: Schneider (Hrsg), FS für Heussen, 2009, S. 119; *Redeker*, NJW 2009, 554, 555 ff.; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 6 Rn 12.

nicht zu einer Mandatserteilung kommen, durch den Rechtsanwalt wieder zu löschen. Eine darüber hinausgehende Verpflichtung, den (potenziellen) Mandanten bereits im Rahmen der erstmaligen Datenerhebung über die Speicherung der Daten zu informieren, erscheint hingegen aus hiesiger Sicht nicht zwingend erforderlich.

Personenbezogene Daten der gegnerischen Partei oder sonstiger Dritter

Im Rahmen der Mandatsführung werden regelmäßig – ohne Kenntnis des Betroffenen – Daten erhoben, beispielsweise über den Forderungsgegner oder sonstige Dritte. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten jedoch nur dann zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Grundsätzlich müsste daher eine Einwilligung in die Datenerhebung eingeholt werden. Ebenso könnten auch §§ 33, 34, 35 BDSG Anwendung finden. Dies hätte zur Folge, dass der Rechtsanwalt in dem Moment, in dem er (für einen Mandanten) personenbezogene Daten eines Schuldners, Prozessgegners oder sonstigen Dritten erhebt und speichert, grundsätzlich zur Mitteilung dieses Vorganges an den Betroffenen verpflichtet sein könnte. Gemäß § 34 Abs. 4 BDSG besteht für die verantwortliche Stelle jedoch keine Pflicht zur Auskunftserteilung, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 BDSG nicht zu benachrichtigen ist. Nach § 33 Abs. 2 Satz 1 Nr. 3 BDSG besteht insbesondere dann keine Benachrichtigungspflicht, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen. Diese Norm zielt ausdrücklich auf gesetzliche Geheimhaltungspflichten, z.B. die des Anwalts hinsichtlich seiner beruflichen Tätigkeit ab. So kann es im Rahmen der Mandatsführung sinnvoll erscheinen, den Gegner nicht schon dadurch „vorzuwarnen", dass man ihm mitteilt, man habe im Auftrag eines Mandanten über ihn Daten gespeichert. Zudem – dies ist allgemeine Meinung – ist der Mandant „Herr" der im Rahmen der Mandatsbeziehung gewonnenen Daten. Er muss grundsätzlich selbst entscheiden können, wann ein Prozessgegner von der Einschaltung eines Rechtsanwaltes erfährt. Auskunfts- und Benachrichtigungspflichten nach §§ 33, 34 BDSG sind in Bezug auf Daten der Gegenseite oder sonstiger Dritter daher zu verneinen. 6

In Bezug auf Drittdaten gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG, wonach eine einwilligungslose Datenerhebung immer dann zulässig ist, wenn es zur Wahrung berechtigter Interessen der verantwortlichen Stelle (hier des Rechtsanwaltes) erforderlich ist und schutzwürdige Interessen nicht überwiegen. Es ist nicht schutzwürdig, dem Anwalt Daten über Dritte, die zur Rechtsvertretung des Mandanten nötig sind, vorzuenthalten. Ausschließlicher Zweck der Datenspeicherung in einer Anwaltsakte ist die Rechtsvertretung eines Mandanten, nicht die Auskunftserteilung an Dritte oder sonstige Nutzung. Beschränkt sich die anwaltliche Datenverarbeitung auf die Abwicklung des Mandats, so ist dies datenschutzrechtlich durch die Mandatserteilung gerechtfertigt, auch wenn der Anwalt sich noch so parteiisch verhält und hierbei das Persönlichkeitsrecht eines Betroffenen verletzt. Die Erhebung personenbezogener Daten der Gegenseite oder sonstiger Dritter dient der Durchführung des anwaltlichen Mandatsverhältnisses. Dieses genießt den vorbeschriebenen Vertrauensschutz, weswegen auch ein Einwilligungserfordernis in die Datenerhebung durch den betroffenen Dritten nicht ausgemacht werden kann. 7

Entsprechendes gilt für Löschungs- und Sperrungsansprüche nach § 35 Abs. 2 bis 4 BDSG. Auch deren Anwendung wird durch die speziellen Vorschriften des anwaltlichen Berufsrechts verdrängt. Die Speicherung von Informationen in der Anwaltsakte ist zulässig, egal welcher Unsinn und welche Persönlichkeitsbeeinträchtigung darin enthalten ist, wenn und insoweit die Erforderlichkeit zur Wahrnehmung des Mandats plausibel begründbar ist. Solange dies der Fall ist, bestehen Löschungsansprüche des Gegners grundsätzlich nicht. 8

Löschungsansprüche können allenfalls nach § 35 Abs. 2 Nr. 3 BDSG bestehen, wenn die gespeicherten Unterlagen nicht mehr im Mandatsverhältnis und auch nicht mehr aus Beweis- und Dokumentationsgründen benötigt werden. Wann dies der Fall ist, muss durch den Anwalt im Rahmen seiner Mandatsführung im Einzelfall entschieden werden können. Klagbare Löschungsansprüche der Gegenseite gegenüber dem Rechtsanwalt bestehen daher grundsätzlich nicht. 9

Keine Auskunftspflichten gegenüber Datenschutzkontrollinstanzen

Nach § 38 BDSG wird die Ausführung des BDSG durch die Aufsichtsbehörden der Länder kontrolliert. Die der Kontrolle unterliegenden privaten Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde gemäß § 38 Abs. 3 BDSG auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft solcher Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der ZPO bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. 10

Vor allem die Datenschutzbeauftragten der Länder[31] sind der Ansicht, die Auskunftspflicht des § 38 BDSG treffe auch den Rechtsanwalt. Dies ergebe sich aus einer Zusammenschau des § 38 Abs. 4 Satz 3 BDSG i.V.m. § 24 Abs. 6 BDSG und § 2 Nr. 2 BDSG. Den Datenschutzkontrollinstanzen stünden daher umfassende Auskunfts- und Besichtigungsansprüche zu. 11

Unseres Erachtens greift diese Auffassung jedoch zu kurz. In diesem Zusammenhang greift wieder die Vorschrift des § 1 Abs. 3 Satz 2 BDSG zum Schutz der beruflichen Geheimhaltungspflichten des Rechtsanwaltes ein. Diese verbietet es, Daten, die Berufsgeheimnissen unterliegen, gegenüber den Datenschutzkontrollinstanzen aufzudecken. Sie verbietet den Datenschutzkontrollinstanzen auch, diese Daten etwa durch andere Kontrollmaßnahmen zu erhalten. Ohne einen solchen Schutz bliebe das Berufsgeheimnis nicht unberührt. Eine Auskunftsverpflichtung des Rechtsanwaltes gegenüber den Datenschutzbehörden besteht daher nicht. Bei Auskunftspflichten verdrängt § 1 Abs. 3 Satz 2 BDSG vielmehr die in § 38 Abs. 3 BDSG grundsätzlich enthaltene Auskunftsverpflichtung. Über die der anwaltlichen Schweigepflicht unterliegenden Daten dürfen Rechtsanwälte und ihre Mitarbeiter den Datenschutzkontrollinstanzen keine Auskunft erteilen. Sie können sich insoweit auf das ihnen nach dem anwaltlichen Berufsrecht zustehende anwaltliche Verschwiegenheitsrecht zurückziehen.[32] 12

Auch die in § 38 Abs. 4 BDSG vorgesehenen sonstigen Betretungs-, Prüfungs- und Einsichtsrechte der Datenschutzkontrollinstanzen bestehen gegenüber Rechtsanwälten nicht. Auch insoweit geht die anwaltliche Verschwiegenheitsverpflichtung den Befugnissen der Datenschutzkontrollbehörden nach § 38 Abs. 4 BDSG vor. Nur so kann das Vertrauensverhältnis zwischen Anwalt und Mandant wirksam geschützt werden. 13

Sonderproblem: „Onlinebestellungen" von Kanzleimaterialien

Im Steuerrecht besteht nach § 147 AO eine eigene Aufbewahrungspflicht für steuerrelevante Belege. Diese gilt für alle Buchführungs- und Aufzeichnungspflichtigen im Sinne der §§ 140, 141 AO, also auch für Rechtsanwälte als Freiberufler. Ein steuerrelevanter Beleg liegt – einfach gesagt – immer dann vor, wenn die Belege, Buchungen oder Berechnungen die Steuerlast mindern können. 14

31 Hierzu: *Weichert*, NJW 2009, 550, 553; KG Berlin, Beschl. v. 20.8.2010 – 1 Ws (B) 51/07–2 Ss 23/07, DStR 2010, 2375 zum Auskunftsersuchen des Berliner Beauftragen für Datenschutz und Informationsfreiheit.

32 So auch KG Berlin, Beschl. v. 20.8.2010 – 1 Ws (B) 51/07–2 Ss 23/07, DStR 2010, 2375: „Ein Rechtsanwalt ist nicht verpflichtet, einem Datenschutzbeauftragten Auskunft darüber zu erteilen, woher er Kenntnisse über bestimmte Informationen und personenbezogene Daten erlangt hat. Auch wenn die datenschutzrechtlichen Vorschriften grundsätzlich eine Auskunftspflicht vorsehen, entfällt diese Verpflichtung aufgrund der anwaltlichen Verschwiegenheitspflicht.".

Geschäftsprozesse werden zunehmend durch E-Mail-Kommunikation abgewickelt. E-Mail-Dokumente sind nach den Grundsätzen des Steuerrechtes zu archivieren, soweit sie steuerrelevante Belege enthalten. Nach § 147 Abs. 6 AO ist die Finanzbehörde berechtigt, im Rahmen einer Außenprüfung Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Der Steuerpflichtige muss die steuerlich relevante E-Mail-Kommunikation elektronisch archivieren und sicherstellen, dass die Dokumente während der Aufbewahrungsfrist maschinell ausgelesen werden können. E-Mail-Kommunikation mit steuerlich relevantem Inhalt muss damit während der gesamten gesetzlichen Aufbewahrungsfrist elektronisch archiviert werden.[33] Auf diese elektronisch vorzuhaltenden steuerrelevanten Belege hat die Finanzverwaltung im Rahmen von Betriebsprüfungen weitgehende Zugriffsrechte, die sich auch auf die Datenverarbeitungssysteme erstrecken, die die steuerrelevanten Belege enthalten (§ 147 Abs. 6 Satz 1 AO). Bewahrt der Steuerpflichtige Belege elektronisch auf, so hat die Finanzverwaltung ein umfassendes Datenzugriffsrecht. Dies beinhaltet als erstes das Recht auf Lesbarmachung am Bildschirm und nicht etwa nur das Recht auf Ausdruck von digital gespeicherten Belegen. Die Finanzverwaltung und nicht der Steuerpflichtige soll entscheiden dürfen, welche Belege und Daten vorgelegt und überprüft werden. **15**

Die vorgenannten Grundsätze können dann an Relevanz gewinnen, wenn – wie in vielen Rechtsanwaltskanzleien üblich – Kanzleimaterial durch die Sekretariate nicht nur per Telefax, sondern auch online bestellt wird. Gelangen Fakturierungen und sonstige steuerrelevante Rechnungen im Rahmen des Onlinebestellvorganges in digitaler Form (per E-Mail) in die Rechtsanwaltskanzlei, kann sich eine Konfliktlage zwischen der anwaltlichen Verschwiegenheitsverpflichtung und dem Einsichtsrecht der Finanzbehörden „am Bildschirm" ergeben. Dies kann insbesondere dann der Fall sein, wenn Bestellungen nicht über ein konkretes, nur für die Abwicklung von Materialbestellungen eingerichtetes Postfach, sondern vielmehr über das zentrale E-Mail-Postfach der Kanzlei oder des Sekretariates erfolgen. In diesen Postfächern befindet sich in aller Regel auch Kommunikation mit dem Mandanten, die unstreitig der Verschwiegenheitsverpflichtung unterliegt. **16**

Nach nicht rechtskräftiger Auffassung des FG Nürnberg[34] ist die elektronische Betriebsprüfung auch bei einem Berufsgeheimnisträger grundsätzlich zulässig. Das Finanzgericht kommt zu dem Ergebnis, dass die Finanzverwaltung die elektronische Betriebsprüfung auch bei Berufsgeheimnisträgern durchführen dürfe (hier Steuerberater). Diese könnten sich gegenüber der Finanzverwaltung nicht darauf berufen, aus den vorzulegenden Daten könnten geschützte Mandantendaten ersichtlich sein. Nach Auffassung des FG Nürnberg ist es vielmehr Aufgabe des Berufsgeheimnisträgers, seine Datenbestände so zu organisieren, dass bei einer zulässigen Einsichtnahme in die steuerlich relevanten Datenbestände keine geschützten Bereiche tangiert werden. So sei der Datenzugriff nicht deshalb ermessenswidrig, weil bei dem Steuerpflichtigen eine Trennung zwischen ungeschützten und geschützten Daten nicht möglich sei. Nach den Grundsätzen ordnungsgemäßer Buchhaltung sei ein effizientes internes Kontrollsystem vorgeschrieben, nach dem sensible Informationen des Unternehmens gegen unberechtigte Kenntnisnahme zu schützen und unberechtigte Veränderung durch wirksame Zugriffs- bzw. Zugangskontrollen zu unterbinden sind. Auch das BDSG verlange die Trennung der Daten nach den Verwendungszwecken und deren zweckgebundene Verarbeitung. Entsprechend diesen Vorgaben verfügten heute nahezu alle im Einsatz befindlichen Betriebssysteme und datenverarbeitungsgeschützten Buchführungssysteme über Möglichkeiten, den Zugriff auf die prüfungsrelevanten Bereiche im Sinne des § 147 Abs. 1 AO zu beschränken. Sollte ein Datenverarbeitungssystem eine Trennung der Daten nicht zulassen, könne dies nicht zur rechtlichen Unzulässigkeit des Datenzugriffes führen. Anderenfalls könnte derjenige, der **17**

33 FG Düsseldorf, Urt. v. 5.2.2007 – 16 V 3454/06 A(AO), EFG 2007, 892; hierzu auch AK 2013, 57.

34 FG Nürnberg, Urt. v. 30.7.2009 – 6 K 1286/2008, DStR 2010, 1355; die Revision zu diesem Verfahren ist unter dem Az.: VIII R 44/09 vor dem BFH anhängig, bislang aber noch nicht entschieden.

eine nicht den allgemeinen Anforderungen entsprechende Software benutzt eine praktisch wirksame Außenprüfung verhindern. Dem Berufsgeheimnisträger ist nach Auffassung des FG Nürnberg jedenfalls durchaus möglich, bei der Erfassung der Geschäftsvorfälle und der Erstellung der Belege, die Trennung der verschwiegenheitspflichtigen Angaben von den steuer- und buchführungsrelevanten Daten herbeizuführen. Wenn er diesbezüglich „seine Hausaufgaben" nicht gemacht habe, könne er hiermit eine zulässige Prüfungshandlung nicht blockieren.

18 Das vorgenannte Urteil beleuchtet das Spannungsverhältnis zwischen Betriebsprüfungen bei Berufsgeheimnisträgern und deren Pflicht zur Verschwiegenheit. Nach § 193 Abs. 1 Alt. 2 AO ist eine Außenprüfung zwar auch bei Berufsgeheimnisträgern möglich, dieser Grundsatz kollidiert aber mit der beruflichen Verschwiegenheitspflicht, bei Anwälten gemäß § 53a BRAO, § 2 BORA sowie den Auskunftsverweigerungsrechten nach § 102 Abs. 1 AO. Die daraus entstehende Grundsatzfrage, ob bei einem Berufsgeheimnisträger überhaupt eine Betriebsprüfung angeordnet werden kann oder ob seine Praxis nicht vielmehr „prüfungsfreie Zone" bzw. „finanzamtsfreier Raum" ist, hat der BFH bereits verneint.[35]

Mit Urt. v. 28.10.2009[36] ging der BFH sogar einen großen Schritt weiter und gab einen Rahmen vor, welche (Papier-)Unterlagen ein Berufsgeheimnisträger bei einer ihn betreffenden Betriebsprüfung wegen seiner Verschwiegenheitspflicht zurückbehalten muss. Danach darf der Berufsgeheimnisträger nur nicht mandatsbezogene Unterlagen und diejenigen Unterlagen vorlegen, bei denen die Mandanten auf eine Geheimhaltung verzichtet haben. Alle anderen Unterlagen müsse der Berufsgeheimnisträger schwärzen bzw. vollständig zurückbehalten.

19 Die Entscheidung des FG Nürnberg,[37] gegen welche die Revision anhängig ist, geht nun noch einen Schritt weiter und befasst sich mit der Frage, inwieweit die Finanzverwaltung im Rahmen einer Außenprüfung bei einem Berufsgeheimnisträger auf Unterlagen, die mit Hilfe eines Datenverarbeitungssystems erstellt worden sind, zugreifen darf. Die Ausführungen des FG Nürnberg hätten – für den Fall, dass der BFH die Rechtsprechung bestätigt – dabei weitreichende Konsequenzen.

20 Um Schwierigkeiten, die sich aus dem vorbeschriebenen Spannungsverhältnis ergeben, zu vermeiden, empfiehlt sich daher, Zugriffsbeschränkungen auf die steuerlich relevanten Dokumente sicherzustellen, z.B. durch eindeutige Indexkriterien wie Buchungsdatum und Zugriffsbeschränkungen. Zudem ist zu beachten, dass sichergestellt werden muss, dass z.B. bei Personaldokumenten, die der Betriebsprüfer auch nicht versehentlich zu Gesicht bekommen darf, eine besondere Schutzvorkehrung eingerichtet wird.

21 Speziell in Bezug auf Bestellungen von Kanzleimaterial und die daraus resultierenden digitalen Rechnungsbelege, die die Finanzverwaltung grundsätzlich so einsehen kann, wie sie in die Kanzlei gelangt sind, empfiehlt es sich in jedem Fall, eine Trennung der Bestellvorgänge von der Mandantenpost vorzunehmen. Hier scheint aus unserer Sicht die Einrichtung eines eigenen E-Mail-Postfaches für Bestellungen (beispielsweise: bestellungen@kanzlei-mustermann.de) sinnvoll und notwendig.

35 BFH, Urt. v. 8.4.2008 – VIII R 61/06, siehe dazu *Mutschler*, DStR 2008, 2087.
36 BFH, Urt. v. 8.4.2008 – VIII R 61/06, siehe dazu *Mutschler*, DStR 2008, 2087.
37 FG Nürnberg, Urt. v. 30.7.2009 – 6 K 1286/2008, DStR 2010, 1355.

E. Kommunikation und Datensicherheit

Die Anforderungen an die Datensicherheit sind i.d.R. etwas höher im Bereich Ihrer Kanzlei als im privaten Bereich. Daher sollte hier auch keine Technik zum Einsatz kommen, die für den Heim- und Hausbereich konzipiert wurde. 1

WLAN in der Kanzlei

Insbesondere sollte dies dort beachtet werden, wo sicherheitsrelevante Technik eingesetzt wird, wie im Bereich von Internet-Routern oder WLAN-Routern (WLAN = Wireless Local Area Network). Als Anwalt sind Sie Profi und professioneller Anwender Ihrer Kommunikations- und Informationstechnologie in Ihrer Kanzlei. Dementsprechend sollten Sie auch die Technik einsetzen, die für den professionellen Einsatz konzipiert wurde. Im Gegensatz zu kabelgebundenen Netzwerken deckt ein WLAN-Netzwerk einen gesamten Bereich signaltechnisch ab. Es muss also hier keine physische Verbindung zum Netzwerk bestehen, um einen Hackerangriff darauf zu starten. In manchen Publikationen wird daher empfohlen die Signalstärke zu vermindern. Vor dem Hintergrund häufig auftretender Verbindungsprobleme bei der regulären Nutzung von WLAN erscheint dieser Vorschlag aber keinesfalls zielführend. Denn selbst wenn ein Signal nicht ausreicht, um mit einem im Notebook eingebauten WLAN-Adapter eine stabile Verbindung aufzubauen, so verfügen Hacker doch üblicherweise über Hardwarekomponenten, die diesem Umstand Rechnung tragen. Die bessere Lösung ist hier die Verwendung eines für den professionellen Einsatz geeigneten WLAN-Routers, der über entsprechende Sicherheitsmechanismen verfügt. Für solche Geräte werden regelmäßig vom Hersteller Software-Updates zur Verfügung gestellt. Diese sollten, sobald sie zur Verfügung stehen, zeitnah eingespielt werden. Was nun die Verschlüsselungsverfahren angeht, so sollte in keinem Fall mehr auf die Verschlüsselungsverfahren WEP (Wired Equivalent Privacy) oder WPA (Wi-Fi Protected Access) zurück gegriffen werden. Soweit Sie noch diese Protokolle verwenden, sollten Sie das unbedingt ändern, denn ein Hackerangriff auf Router, die mit einem dieser Systeme arbeiten, wird üblicherweise in einem Zeitraum von 15 Minuten bis maximal 10 Stunden zum Erfolg führen. WLAN sollte ausschließlich die neueste dafür vorgesehene Verschlüsselung nutzen. Derzeit entspricht WPA2 dem Stand der Technik. Dabei ist allerdings darauf zu achten, dass die eingesetzte Hardware professionellen Anforderungen genügt, die Netz-ID ausgeblendet ist und sich nicht jeder Rechner am Router bekannt machen darf. D.h. ein Rechner, der mit dem Router kommunizieren will, sollte dort manuell eingetragen werden. Ebenfalls sollte die Filterung nach MAC-Adressen erfolgen und eine Stateful-Inspection-Firewall integriert sein oder separat eingesetzt werden. 2

WLAN bietet zahlreiche Angriffsmöglichkeiten. Grundsätzlich sollte daher überlegt werden, ob es wirklich erforderlich ist, WLAN in der Kanzlei einzusetzen oder ob das Notebook nicht auch an ein Netzwerkkabel angestöpselt werden könnte.[38] In keinem Fall sollten Sie für Ihre Mandanten eine Art Hotspot betreiben und schon gar nicht einen solchen im selben Netz integriert haben, in dem sich auch die Rechner und Server der Kanzlei befinden. Soweit ein WLAN benötigt wird, um z.B. mit dem Smartphone eine Internet-Verbindung zu nutzen, sollte ebenfalls geprüft werden, ob das nicht als separates Netzwerk im Router definiert werden kann, so dass hier keine Verbindungsmöglichkeit vom Smartphone zum internen Netz der Kanzlei besteht.[39] 3

Sonstiger Systemschutz

Virenscanner und Firewalls bieten einen relativen Schutz Ihrer Systeme. Die Anwender sind jedoch immer gefordert, auch verantwortungsvoll mit Technik und personenbezogenen Daten umzugehen, so haben z.B. private USB-Datenträger an einem beruflich genutzten System nichts zu suchen. Was den meis- 4

38 Zur Haftung für einen unzureichend gesicherten WLAN-Anschluss: BGH v. 12.5.2010 – I ZR 121/08.
39 Hierzu auch AK 2013, 37.

ten Lesern eigentlich als selbstverständlich erscheint, ist allerdings eine der größten Gefährdungen. So sind aus der Praxis durchaus Fälle bekannt, in denen sich Mitarbeiter über die technische Sperrung von USB-Datenträgern beschwert haben, weil sie ihren Kolleginnen und Kollegen die neuesten Urlaubsbilder nicht präsentieren konnten. Wird nun ein verseuchter USB-Datenträger an ein Gerät angeschlossen, so wird zumindest ein Teil der Sicherheitstechnik in der Kanzlei ausgehebelt.

Auf diese Art, ebenso wie durch das unbedarfte Anklicken von Internetinhalten oder das unreflektierte Öffnen von Email-Anhängen unbekannter Versender werden häufig Systeme trotz vorhandener Sicherheitsmaßnahmen verseucht. Das Personal sollte daher regelmäßig geschult und für die Gefahren im Zusammenhang mit der IT sensibilisiert werden. Einige Schadprogramme werden gefunden, wenn ein vollständiger Systemscan durch ein aktuelles Antivirenprogramm durchgeführt wird. Andere Schädlinge wie z.B. Bot-Viren sind so konzipiert, dass sie sich auf eine sehr subtile Art und Weise in Ihre Systeme einnisten können. Sind Ihre Rechner erst einmal durch einen solchen Bot-Virus infiziert, so werden diese i.d.R. durch Kriminelle für deren niedrige Zwecke missbraucht. Das kann so aussehen, dass Ihr Rechner für die Verbreitung illegaler Dateien und Inhalte oder für Angriffe auf Unternehmensnetzwerke missbraucht wird. In einigen Fällen ist bei einer solchen Infektion aufgefallen, dass die Systeme langsamer reagierten als das gewöhnlich der Fall war. Bei der anschließenden Suche mittels spezieller zur Beseitigung von Bot-Viren konzipierter Software wurden diese dann identifiziert und beseitigt. Sie sollten daher bei Auffälligkeiten und in regelmäßigen Abständen einen speziellen Scan nach Bot-Viren auf Ihren Systemen durchführen. 5

E-Mail-Kommunikation

Gewöhnliche E-Mail ist per se ein unsicheres Kommunikationsmedium. Selbst wenn Sie zu einem externen Provider eine SSL- oder TLS-Verschlüsselung nutzen, was seit dem Jahreswechsel von vielen Email-Providern gefordert wurde, so ist zwar die Kommunikation zwischen Ihrem Rechner und dem Email-Server gesichert – wenn nicht gerade wieder ein Programmierfehler die vermeintliche Absicherung ad absurdum führt – jedoch besteht diese Verbindung dann auch nur für einen kleinen Teil der gesamten Transportstrecke. Bei der Übermittlung im Internet, insbesondere zu Ihrem Postfach auf dem Server eines Providers muss davon ausgegangen werden, dass die E-Mail vollständig unverschlüsselt transportiert wird. Das heißt, dass Daten über öffentliche Netze in einem grundsätzlich für jeden lesbaren Zustand transportiert werden. Wer jetzt glaubt, dass E-Mails nur von Superhackern und Geheimdiensten mitgelesen werden können, dem sei gesagt, dass im Internet ausreichende technische Werkzeuge und Anleitungen zur Verfügung stehen, womit jeder, der es schafft einen Rechner einzuschalten auch in der Lage ist, sich fremde Daten zu verschaffen. Das derartige Unterfangen illegal sind, verhindert nicht, dass es sie gibt. 6

Vorsicht ist allgemein auch bei der Anwendung der E-Mail-Programme walten zu lassen. So sollte bei der Übermittlung an mehrere Empfänger – beispielsweise eines Newsletters oder allgemeinen Mandanteninformationen – stets die sog. Blind-Copy (Bcc) das Mittel der Wahl sein. Anderenfalls droht datenschutzrechtliches Ungemach, wie ein Fall aus Bayern verdeutlicht. Dort hatte die Mitarbeiterin eines Unternehmens einen E-Mail-Verteiler verwendet, der aus E-Mail-Adressen bestand, die vorwiegend die Vor- und Nachnamen von Personen zeigten. Sämtliche Adressaten wurden im „An"- bzw. im „CC"-Feld kontaktiert und waren daher für alle Empfänger sichtbar. Wegen des Verstoßes gegen den Datenschutz verhängte die Behörde ein Bußgeld gegen die betroffen Mitarbeiterin und das Unternehmen. 7

E-Mail ist also grundsätzlich in der altbekannten Version untauglich für die anwaltliche Kommunikation mit Mandanten, Kollegen und Gerichten, soweit darin personenbezogene Daten übermittelt werden. Einen Ausweg bietet hier die Verschlüsselung. Sollte es also notwendig werden, Dokumente mit brisanten Inhalten, personenbezogenen Daten oder besonderen Arten personenbezogener Daten per Mail zu ver- 8

senden, so ist darauf zu achten, dass eine nach dem Stand der Technik als sicher angesehene Verschlüsselung zu Einsatz kommt. In diesem Fall ist das mit einem relativ großen Aufwand für die Kanzlei verbunden, da Sie das Verschlüsselungsverfahren auswählen, installieren und auf dem aktuellen Stand halten müssen. Ansonsten ist der oft gewählte Vergleich der E-Mail mit der Postkarte zutreffend – es fehlt selbst an der »Minimalsicherung« eines verschlossenen Umschlags wie bei der postalischen Kommunikation. Vergegenwärtigt man sich des Weiteren die Funktionsweise des Internets und der E-Mail-Übermittlung, wird deutlich, dass weitaus mehr Manipulations- und Zugriffsmöglichkeiten bestehen. Auf elektronische Daten kann auf vielfältigere, spurlosere und leichtere Art zugegriffen werden als auf Inhalte der Papier-Post. Aufgrund der technischen Funktionsweise der Datenübermittlung im Internet kann auf E-Mails einfach, automatisiert und großflächig zugegriffen werden, zumal nicht einmal sicher gestellt werden kann, dass die Datenpakete auch über Server geleitet werden, die außerhalb des Geltungsbereichs von TKG und StGB liegen. Soweit der Telekommunikationsanbieter daher keine zusätzlichen Sicherungsmechanismen zur Verfügung stellt, bedingt der Einsatz der einfachen E-Mail im Bereich besonders schutzwürdiger Daten ohne eine Ende-zu-Ende-Verschlüsselung eine erhöhte Gefahr. Hierüber ist der Mandant – sollte auf eine solche Möglichkeit verzichtet werden – in jedem Fall zu informieren und seine Einwilligung in die Form der „einfachen" und unverschlüsselten E-Mail-Kommunikation einzuholen. Für den Rechtsanwalt hat dies den positiven Effekt, neben der Bekräftigung des Eindrucks des vertrauenswürdigen Umgangs mit den Informationen seines Mandanten auch eine Strafbarkeit gem. § 203 StGB ausschließen zu können.[40]

De-Mail als Alternative?

Eine Alternative dazu bietet die De-Mail. Das Verfahren, dessen Entwicklung von der Bundesregierung beauftragt und vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert wurde, bietet den rechtssicheren Versand von E-Mails und Dokumenten. Soweit Sie auf dieses Verfahren zurückgreifen, ist im Falle eines Vorkommnisses im Zusammenhang mit dem Datenschutz sichergestellt, dass Sie, hinsichtlich der Versendung von E-Mail und Dokumenten, die für den Umgang mit personenbezogenen Daten notwendige Sorgfalt beachtet haben. 9

Natürlich stellt sich vor dem Hintergrund vieler Enthüllungen und zahlreicher Vorstöße durch die Innenminister während der letzten Jahre, mit der Datensammelwut US-amerikanischer Behörden gleich zu ziehen, die Frage, ob ein Staat, der ein Verfahren entwickeln lässt, das dann auch noch von staatlicher Stelle zertifiziert wird, sich nicht die Möglichkeit schafft, trotz vermeintlicher Sicherheit alles mitzulesen. Für Kriminelle im Internet dürfte es jedoch ungleich schwieriger werden, sich bei Verwendung von De-Mails Informationen zu beschaffen. 10

Allerdings ruft das Identifizierungsverfahren, worauf mindestens einer der De-Mail-Provider besteht, bei interessierten Personen mitunter ein gewisses Maß an Unbehagen hervor. Dass bei Bestellung einer De-Mail eine PIN-Nummer an eine angegebene Mobilfunknummer gesendet wird, wäre noch zu vertreten. Dass das als besonders sicher geltende Verfahren auch die eindeutige Identifikation des Nutzers erforderlich macht, ist auch noch nachvollziehbar. Nicht nachvollziehbar ist jedoch der Umstand, dass ein De-Mail-Provider hier nicht auf das bewährte Postident-Verfahren oder ein vergleichbares Verfahren zurückgreift. Stattdessen bekommt man persönlichen Besuch von einem sogenannten De-Mail-Mitarbeiter. Ob ein solcher zur besonderen Verschwiegenheit verpflichtet ist, im Vorfeld vom Verfassungsschutz überprüft wurde oder ob es sich um den Mitarbeiter irgendwelcher Personalvermittler oder Subunternehmer handeln könnte, konnte im Rahmen der Recherche zum vorliegenden Artikel nicht ermittelt werden. Eine Nachfrage bei der Deutschen Telekom AG hat hingegen ergeben, dass dort ein dem Postident vergleichbares Verfahren angeboten wird, bei dem man sich in einem Telekom-Shop oder in einem Hermes 11

40 Weitergehende Tipps zum allgemeinen Umgang mit E-Mails finden sich auch bei *von Wilmsdorff*, AK 2014, 60 ff.

PaketShop identifizieren kann. Auf Wunsch des Nutzers kann auch ein Telekom-Mitarbeiter in die Kanzlei kommen, so dass hier 3 Alternativen der Identifizierung angeboten werden. Alles in allem bietet De-Mail mit der Rechtssicherheit im Bezug auf Datenschutz und Zustellung wesentliche Vorteile bei gleichzeitig einfacher Nutzung und wird daher zum sicheren und schnellen Datenaustausch empfohlen.

E-POSTBRIEF als Alternative

12 Seit 2010 bietet auch die Deutsche Post AG eine neue Versendungsform an, den sog. E-POSTBRIEF. Der E-POSTBRIEF bietet, wie die De-Mail, die Möglichkeit zur Übermittlung von Briefen in elektronischer Form. Zur Teilnahme am Verfahren, ob als Absender oder Empfänger, ist eine individuelle Registrierung erforderlich. Anders als die De-Mail, beschränkt sich der E-POSTBRIEF jedoch nicht allein auf die elektronische Übermittlung. Es gibt zwei Versandwege: Zum einem den vollelektronischen Versandweg, bei dem der vom Absender verfasste elektronische Brief unmittelbar an den Empfänger versendet wird. Der elektronisch übermittelte E-POSTBRIEF wird außerdem mit einer qualifizierten digitalen Signatur ausgestattet, nachdem über das Postident-Verfahren die Identitäten von Absender und Empfänger verifiziert wurden. Bei dem anderen Versandweg ist nur der Absender, nicht aber der Empfänger registrierter Teilnehmer des E-POSTBRIEF-Verfahrens. Bei diesem sog. Hybridbrief wird der vom Absender elektronisch erstellte Brief durch die Deutsche Post AG ausgedruckt, kuvertiert und dem Empfänger auf dem normalen Postweg zugestellt. Es findet also ein Medienbruch statt.

13 Wie bei der De-Mail verzichtet der E-POSTBRIEF bei der vollelektronischen Übermittlung auf eine Ende-zu-Ende-Verschlüsselung. Der Versand erfolgt mit einer sog. Transportverschlüsselung sowie einer providerseitigen Verschlüsselung der Nachricht. Technisch schließt diese Art der Verschlüsselung die Kenntnisnahme durch unberechtigte Dritte zwar (weitgehend) aus; Mitarbeiter der verarbeitenden Rechenzentren haben indes auch bei dieser Art der Verschlüsselung Zugriff auf die Daten. Dies beruht darauf, dass die Nachricht nicht wie bei einer sog. Ende-zu-Ende- Verschlüsselung bereits auf dem Endgerät des Nutzers, sondern erst durch die Deutsche Post verschlüsselt wird, wodurch zumindest deren Mitarbeitern eine Kenntnisnahme theoretisch möglich ist, so dass die Vertraulichkeit des Kommunikationsvorganges nicht vollständig gewahrt wird. Eine Verschlüsselung findet „nur“ zwischen dem Absender und dem E-Postserver und zwischen dem E-Post-Server und dem Empfänger statt. Die Post AG begründet dies damit, dass die E-POSTBRIEFE beim Eingang in das E-POSTBRIEF-System von einem Malware-Scanner geprüft würden. Bei einem positiven Befund wird die Annahme durch das System verweigert und dies dem Nutzer mitgeteilt. Eine Prüfung auf Malware erfolgt ebenfalls vor Übermittlung einer Nachricht an den Empfänger. Bei einem positiven Befund werden Absender und Empfänger informiert. Der Zugriff auf die Nachricht bzw. den Anhang, für die der positive Malware-Befund vorliegt, bedürfen einer expliziten Bestätigung durch den Nutzer. Lehnt er dies ab, werden weder der E-POSTBRIEF noch die Attachments zugestellt. Bei jedem Öffnen eines Attachments einer Nachricht wird auch dieses auf Malware geprüft. Aus anwaltlicher Sicht fragt sich hier zu Recht, warum eine solche Malwareprüfung überhaupt erforderlich ist und warum diese einer – aus Vertraulichkeitsgesichtspunkten sicherlich wünschenswerten – Ende-zu-Ende-Verschlüsselung im Wege steht. Die im System angelegte Möglichkeit der Entschlüsselung der E-Mail-Inhalte durch den Diensteanbieter lässt hier Raum für Manipulationen, die im Rahmen einer „sicheren“ elektronischen Kommunikation gerade verhindert werden sollen. Man könnte sagen, besser zum Teil verschlüsselt als gar nicht verschlüsselt; doch wenn man sich schon die Mühe macht, für eine sichere Kommunikation zu sorgen, so sollte diese auch wirklich sicher und nicht nur teilweise sicher sein. Es bleibt daher zu hoffen, dass die Post hier nachbessert und Rechtsanwälten die Option auf eine Ende-zu-Ende-Verschlüsselung einräumt. Bis dies der Fall ist, ist der Absender des E-POSTBRIEFES – wie bei der De-Mail – bei Daten mit erhöhtem Schutzbedarf gehalten, zusätzliche, eigene Maßnahmen, wie z.B. das Anfügen der zu übermittelnden Daten in einem verschlüsselten Anhang, zu ergreifen.

In diesem Fall entfällt freilich die Möglichkeit der Nutzung des sog. Hybridbriefes,[41] von der aus Sicht des Rechtsanwaltes ohnehin eher abgeraten wird. Der durch den Ausdruck des elektronisch übersandten Schriftstücks zum Zwecke der klassischen Zustellung zwingende Medienwechsel bedingt eine theoretische Kenntnisnahmemöglichkeit durch Mitarbeiter des Verarbeitungszentrums. Die E-POST weist zwar darauf hin, dass das Ausdrucken, Kuvertieren und Frankieren im Regelfall voll automatisiert erfolgt, gleichwohl ist dies nicht immer der Fall. Hier finden sich dann aber keine entsprechenden Straftatbestände, die bereits die Kenntnisnahme durch Mitarbeiter des Verarbeitungszentrums unter Strafe stellen. Über § 202 Abs. 1 Nr. 1 StGB wird nur mit Strafe bedroht, wer einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, das nicht zu seiner Kenntnis bestimmt ist, öffnet – dies ist beim Ausdruck des elektronischen E-POSTBRIEFS zwecks Kuvertieren und Zustellen (noch) nicht der Fall; über § 206 Abs. 1 StGB wird erst die Weitergabe von Tatsachen, die dem Post- oder Fernmeldegeheimnis unterliegen, unter Strafandrohung gestellt. Auch wenn der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) in seinem 23. Tätigkeitsbericht[42] ausführt, dass „die vertrauliche Behandlung der übermittelten Daten bei Hybridbrief dadurch gewährleistet werden soll, dass die mit dem Ausdruck der Briefe betrauten Mitarbeiter/innen sich strafbar machen, falls sie das Post- und Fernmeldegeheimnis (Art. 10 GG) verletzen würden“ und eine Vor-Ort-Prüfung des Rechenzentrums der Post „keine datenschutzrechtlichen Probleme zutage“ gebracht habe, geht mit dem Medienbruch eine Offenbarung der sensiblen Inhalte anwaltlicher Kommunikation einher, die jedenfalls unter Imagegesichtspunkten keinesfalls wünschenswert ist. So berichtet auch der BfDI von Eingaben zum E-POSTBRIEF, die sich konkret mit dem Ausdruck des E-POSTBRIEFS durch die Deutsche Post AG, wenn eine Zustellung nur auf dem „normalen Postweg“, also als Hybridbrief, möglich ist, befassen. Hier bestanden u.a. Bedenken, ob das Postgeheimnis gewahrt wird. Derartigen Nachfragen sollte sich der Rechtsanwalt gegenüber seinem Mandanten nicht aussetzen und daher besser auf die Nutzung des sog. Hybridbriefes verzichten. Vor dem Hintergrund, dass dieser (derzeit) zudem auf eine Seitenzahl von maximal 99 Seiten beschränkt ist, eignet er sich für längere Schriftstücke ohnehin nicht. **14**

Mit Blick auf die Verbesserung des Datenschutz- und Sicherheitsniveaus elektronischer Post kann die Nutzung des vollelektronischen E-POSTBRIEFES jedoch eine sinnvolle Lösung darstellen.[43] Dies belegt nicht zuletzt auch die Zertifizierung des vollelektronischen Verfahrens mit dem Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.[44] **15**

Elektronischer Rechtsverkehr und Signaturkarte

Bereits im Zuge der EGVP-Einführung hatten viele Kanzleien bereits Signaturkarten angeschafft. Einige Kanzleien hatten dies jedoch unterlassen, da das Verfahren von der Beantragung bis zum produktiven Einsatz recht zeitaufwendig und mitunter technisch aufwendig war. Nunmehr wird die elektronische Kommunikation mit Gerichten zur Pflicht. **16**

Hinsichtlich des Verfahrens der Signaturkarte kann davon ausgegangen werden, dass es sich um ein ausgereiftes und als allgemein zuverlässig angesehenes Verfahren handelt, das dem Stand der Technik entspricht.

Es bestehen daher seitens des Datenschutzes keinerlei Bedenken, damit zu arbeiten. Allerdings gibt es auch hier etwas zu beachten, insbesondere die Frage, wie die Signaturkarte und die zugehörige PIN auf- **17**

41 Siehe hierzu die Leistungsbeschreibung des E-POSTBRIEFES unter http://www.epost.de/content/dam/dp/dokumente/leistungsbeschreibung.pdf.

42 http://www.thm.de/zaftda/tb-bfdi/doc_download/566–23-tb-bfdi-bund-2009–10–17–5200-vom-12–04–2011.

43 So auch: *Schmidt/Brüning/Schliesky*, Der E-POSTBRIEF in der öffentlichen Verwaltung, abrufbar unter: http://www.lvstein.uni-kiel.de/t3/fileadmin/user_upload/MSV_11_FINAL.pdf.

44 Das Zertifizierungsgutachten kann in Kurzform unter https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g120301 heruntergeladen und eingesehen werden.

bewahrt werden. Es ist sicherlich keine gute Lösung, wenn dieses Allgemeingut in der Kanzlei ist. Das Bundesamt für Sicherheit in der Informationstechnik hat diesbezüglich drei Grundregeln veröffentlicht[45]:

1. *Die Signaturkarte inkl. PIN (falls vorhanden) muss von dem Anwender unbedingt vor fremdem Zugriff geschützt werden;*
2. *Der Signier-PC muss unbedingt vor unautorisiertem Zugriff geschützt werden;*
3. *Falls verfügbar nutzen Sie einen Kartenleser mit integriertem PinPad.*

Auch wenn der elektronische Rechtsverkehr erst ab 2016 verpflichtend ist, so sollten Kanzleien sich bereits jetzt darum kümmern. Vier Wochen vor dem Stichtag sich des Themas anzunehmen, wird voraussichtlich nicht ausreichend sein, denn zum einen muss die Signaturkarte zunächst beschafft/beantragt werden. Dann braucht es ein Kartenlesegerät, das auch für den Einsatz mit der Signaturkarte geeignet ist. Um das Lesegerät und die Karte nutzen zu können, braucht es darüber hinaus auch eine Software. Und schließlich soll das Verfahren auch ggf. in Ihre Kanzleisoftware eingebunden werden, was je nach eingesetzter Software nicht ganz trivial ist. Mit anderen Worten braucht es eine entsprechende Vorlaufzeit, mit der Signaturkarte zu arbeiten. Es wird daher empfohlen, soweit Sie nicht schon mit der Signaturkarte arbeiten, sich jetzt bereits darum zu kümmern, Signaturkarte und Kartenlesegerät zu beschaffen und ggf. jetzt bereits zu integrieren. Diejenigen, die zu lange warten, stehen nachher vielleicht vor dem Problem, dass der Software-Anbieter die Anfragen, die kurz vor dem Stichtag eingehen, aus Kapazitätsgründen gar nicht mehr rechtzeitig abarbeiten kann oder dass im Bereich der benötigten Geräte kurzfristig Engpässe auftreten. Davon abgesehen, wird der elektronische Rechtsverkehr die Kommunikation mit den Gerichten beschleunigen, so dass es eigentlich erstrebenswert erscheint, die Vorteile so früh wie möglich nutzen zu können. **18**

Eine Entscheidung des OLG Düsseldorf[46] betreffend die Nutzung des EGVP sorgte kürzlich zudem für Verwirrung. Gegenständlich war die Zurückweisung einer auf elektronischem Weg via EGVP an das OLG Düsseldorf übermittelten Berufungsbegründung sowie eines anschließenden Wiedereinsetzungsantrags. Zwar unterhält das OLG erkennbar ein EGVP, jedoch darf wegen dessen Existenz nicht obligatorisch von einer Nutzbarkeit ausgegangen werden. Im vorliegenden Fall handelte es sich um eine Berufungszivilsache, für die der elektronische Rechtsverkehr beim Oberlandesgericht noch nicht eröffnet ist. Welche Gerichte hieran teilnehmen, entscheiden die jeweiligen Landesregierungen in ihren Rechtsverordnungen (§ 130a Abs. 2 ZPO). Das Gericht wies in den Urteilsgründen darauf hin, dass die auf der Internetpräsenz www.egvp.de online einsehbare Rubrik „Teilnehmer" nachprüfbar macht, an welche Gerichte rechtswirksam via EGVP übertragen werden kann. Durch eine einfache Recherche sei zu ermitteln gewesen, dass bislang weder die Landesregierung Nordrhein-Westfalen noch das durch sie ermächtigte Justizministerium für zivile Berufungsverfahren die elektronische Übermittlung ermöglicht haben. Selbst wenn ein Gericht ein EGVP unterhält, ist daher stets zu kontrollieren, ob es in der Rechtsverordnung und der Teilnehmerliste auf www.egvp.de aufgenommen ist. **19**

Regel 1: Setzen Sie in Ihrer Kanzlei in sicherheitsrelevanten Bereichen (Router, WLAN-Router) keine Billiggeräte für den Heimgebrauch ein. **20**

Regel 2: Überlegen Sie, ob Sie Ihre Kanzlei und sich dem erhöhten Risiko aussetzen wollen, das durch die Verwendung von WLAN (Wireless Local Area Network) gegeben ist, oder ob eine Arbeit ausschließlich mit kabelgestützten Verbindungen in der Kanzlei möglich ist.

Regel 3: Verwenden Sie keinesfalls die technisch veralteten Verschlüsselungsverfahren WEP oder WPA in einem WLAN (Wireless Local Area Network).

45 Fragen und Antworten zur elektronischen Signatur, Bundesamt für Sicherheit in der Informationstechnik, 2014, https://www.bsi.bund.de/DE/Themen/weitereThemen/ElektronischeSignatur/FAQ/faq_node.html.

46 OLG Düsseldorf, Urt. v. 24.7.2013 – VI-U (Kart) 48/12.

Regel 4: Verwenden Sie im Hardwarebereich nur leistungsfähige Stateful-Inspection-Firewalls, die lernfähig sind und über die Logik verfügen, nur angeforderte Antworten aus dem Internet zu akzeptieren, und gleichzeitig wissen, in welchem Netzwerk sich welche Netzwerkadresse befindet.

Regel 5: Lassen Sie kein dynamisches Einhängen von Rechnern in das WLAN zu. Blenden Sie die SID des WLAN aus und verwenden Sie einen Router, der nach mehreren fehlerhaften Authentifizierungsversuchen (z.B. 3 bis 5 Fehlversuche) vom Angreifer für eine vordefinierte Zeitspanne (z.B. 5 bis 15 Minuten) keine Verbindungsanfragen mehr annimmt.

Regel 6: Bieten Sie keinesfalls Ihren Mandanten und Besuchern ein unverschlüsseltes und offenes WLAN als Service an!

Regel 7: Schulen und sensibilisieren Sie regelmäßig das Personal hinsichtlich der Gefahren der IT-Nutzung.

Regel 8: Jeder Rechner muss mit einem Virenscanner ausgestattet sein, der (mehrfach) täglich aktualisiert werden soll. Regelmäßig und bei Auffälligkeiten sollen die Systeme zusätzlich nach Bot-Viren durchsucht werden.

Regel 9: Versenden Sie keine unverschlüsselten Dokumente per E-Mail. Verschlüsseln Sie Dokumente mit einem nach dem Stand der Technik sicheren Verfahren oder nutzen Sie De-Mail.

F. Voice-over-IP in der Anwaltskanzlei

1 Voice-over-IP (VoIP) ist auf dem Vormarsch. Gleichwohl, rät das DSL-Magazin[47], sollte man sich beim Einsatz von VoIP das Postkartenprinzip zu eigen machen. Das bedeutet, dass man nichts über einen entsprechenden Telefonanschluss bespricht, was man nicht auch unkritisch auf eine Postkarte schreiben könnte. Diese Einschätzung würde den Wert des Kommunikationsmediums für den Einsatz in der Kanzlei deutlich einschränken, z.B. wenn es um das Gespräch zwischen Anwalt und Mandant geht. Sollte daher von der Nutzung von VoIP-Diensten generell Abstand genommen werden?

2 Ein Fall aus Rheinland-Pfalz könnte zum Anlass genommen werden, diese Frage unbesehen zu verneinen: Hacker hatten sich unbemerkt Zugriff auf das Firmen-Telefonnetz eines Unternehmers verschafft und außerhalb seiner Geschäftszeiten teure Auslandstelefonate geführt. Der Schaden belief sich auf rund 11.000 EUR. Ist es wirklich so leicht, sich Zugriff auf ein VoIP-Netz zu verschaffen oder hatte der Unternehmer hier nicht richtig vorgesorgt. Hierzu ist es zunächst wichtig, die hinter VoIP stehende Technik zu verstehen und sich zu vergegenwärtigen, dass hier keine „klassische" Telefonie betrieben, sondern das Datenverbindungen zur Gesprächsübertragung verwandt werden.

3 Während die klassische Telefonie dank einer geschlossenen Punkt-zu-Punkt-Verbindung schon von Haus aus ein hohes Maß an Sicherheit garantiert, schickt VoIP digitalisierte Sprachpakete über das Internet. VoIP ist dabei nicht gleich VoIP: Wie die Beauftragte für den Datenschutz und die Informationsfreiheit in einer aktuellen Broschüre[48] hervorhebt, existiert hier kein einheitlicher Standard, sondern werden verschiedene technische Varianten „mit fließenden Übergängen" eingesetzt, die sich zum Teil erheblich unterscheiden. Das wohl meist verbreitete Protokoll stellt das sog. Session Initiation Protocol (SIP) dar, daneben kommen Next Generation Network (NGN) als direkter Nachfolger des Telefonnetzes oder auch das H.323-Protokoll zum Einsatz. Die Beauftragte für den Datenschutz und die Informationsfreiheit hält insbesondere SIP und H.323 „von Natur aus [für] geschwätzig und per se nicht für die vertrauliche Kommunikation geeignet", muss diese Sicherheit bei Voice-over-IP erst hergestellt werden. Denn die Verbindungs- und Gesprächsdaten IP-basierter Telefonate gelangen nicht etwa auf geschützten Leitungsbahnen, sondern über das offene IP-Netz vom Sender zum Empfänger. Trifft man hier keine Sicherheitsvorkehrungen, ist die VoIP-Kommunikation ebenso anfällig für Angriffe Dritter wie ungeschützte Webseiten und E-Mail-Verbindungen.

4 Für diese Problematik scheinen allerdings bislang nur wenige VoIP-Anwender sensibilisiert, was angesichts der breiten öffentlichen Diskussion zum Thema Datenschutz kaum noch nachvollziehbar ist. Wie unbedacht oft agiert wird, zeigt exemplarisch der Umgang mit SIP (Session Initiation Protocol), dem heute meistverbreiteten Protokoll für den Aufbau von Voice-over-IP-Verbindungen. In seiner Standardversion sieht dieses Protokoll keine Verschlüsselung der Verbindungsdaten vor. Es kann jedoch durch Einbettung des Verschlüsselungsprotokolls SSL (Secure Sockets Layer), heute offiziell als TLS (Transport Layer Security) bezeichnet, zu SIPS (Session Initiation Protocol Secure) erweitert werden. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt im Rahmen seines Kataloges zum IT-Grundschutz diesbezüglich den Einsatz von Protokollerweiterungen wie „Secure Real – Time Transport Protocol" (SRTP) und „Secure Real – Time Streaming Protocol" (SRTSP) oder die Anwendung spezieller Signalisierungssoftware. Die Mehrzahl der Anwender verzichtet allerdings bisher auf diese Option und nutzt SIP ohne ergänzende Verschlüsselung. Dies gilt es in der Rechtsanwaltskanzlei zu vermeiden. Sonst lassen sich mit einfachen Mitteln auf dem Weg der Telefonpakete Daten sammeln. Softwaresysteme sind dabei in der Lage zu erkennen, welche Pakete zu welchen Telefonverbindungen gehören und setzen diese so zusammen, dass eine verwertbare Aufzeichnung eines Gesprächs entsteht. Auf diese

47 http://www.dsl-magazin.de/voip/sicherheit.

48 http://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/InternetTelefonie.pdf?__blob=publicationFile.

Art und Weise, sind mit einfachen Mitteln Tausende oder sogar Millionen von Telefonaten abhörbar. Innerhalb der Sprachpakete kann dann nach bestimmten Ausdrücken gesucht werden, so dass Telefonate z.B. anhand der Ausdrücke „Liechtenstein“ und „Schwarzgeld“, „Kontodaten“ und „Transaktion“ oder weiterer Begriffe wie „Erpressung“ oder „Unfallflucht“ identifiziert werden können. Professionelle Hacker nutzen hierfür so genannte Sniffer-Programme, die sich legal aus dem Internet herunterladen lassen. Diese Programme sind kostenfrei verfügbar und zumindest für Profis so einfach zu bedienen, dass das Abhören und Mitschneiden kein großes Problem mehr darstellt. Wer solche Tools nutzt, kann sich Zugriff auf Endgeräte und Voicemail-Boxen verschaffen und erhält zudem umfangreiche Informationen über die Identität der Gesprächsteilnehmer, den aktuellen Gesprächsstatus sowie den Zeitpunkt und die Dauer der jeweiligen Telefonate.

Wer sich für den Einsatz von VoIP in der Rechtsanwaltskanzlei entscheidet, sollte daher nicht im Do-it-Yourself-Wege vorgehen, sondern sich von spezialisierten Unternehmen beraten und von diesen eine ausreichende Datensicherheitsstruktur integrieren lassen.[49] Verschlüsselungs- und Authentifizierungsverfahren sind in diesem Kontext die wohl zentralen Begriffe. Aufgrund der Variabilität des Einsatzes von VoIP, sei es betreffend die eingesetzten Protokolle oder den gewählten Lösungsansatz, können konkrete Handlungsempfehlungen leider nicht ausgesprochen werden. Wichtig erscheinen jedoch in jedem Fall die Separierung des Telefon-Netzwerks vom restlichen Datenverkehr sowie die Etablierung einer starken, zertifikatsbasierten Netzzugangskontrolle sowie die Etablierung individueller und starker Passwörter und das Deaktivieren nicht benötigter Dienste.[50] Bei jeder VoIP-Einrichtung sollte zudem die Abschirmung des Telefonie-Servers durch Firewall, Virenscanner und Passwörter Standard sein. Will man die Hürden für potenzielle Angreifer so hoch wie möglich setzen, ist es auch entscheidend, nicht nur den Verbindungsaufbau, sondern auch die Audiodaten des Gesprächs mit Hilfe eines entsprechenden Verschlüsselungsprotokolls zu codieren. 5

Die Internet-Telefonie braucht des Weiteren einen VoIP-Router. Bei Stromausfall kann dann i.d.R. nicht mehr telefoniert werden. Kurze Stromausfälle führen zum Abbruch eines Telefonats, während das herkömmliche Telefonsystem (analog oder ISDN) über eine eigene externe Stromversorgung verfügt. Auch hier sollten entsprechende Vorkehrungen getroffen werden. Schließlich sind in den vergangenen Monaten vermehrt Netzausfälle bei VoIP-Anbietern aufgetreten. So berichten beispielsweise auch Telekom-Kunden mit IP-Telefonie-Anschluss von fortwährenden z.T. stundenlangen Netzausfällen, einige berichten sogar über tagelange Ausfälle.[51] 6

VoIP ist gleichwohl eine Technologie, die beim Einsatz entsprechender Sicherheitsmaßnahmen nicht nur eine ernsthafte Alternative zur klassischen Telefonie darstellt, sondern aufgrund der Synergiepotenziale die bisherigen Technologien in vielen Bereichen langfristig sukzessive ablösen kann. Gleichzeitig sollte jedoch jedem Rechtsanwalt klar sein, dass die unbedarfte Einführung von VoIP erhebliche Bedrohungspotenziale mit sich bringen kann. Im Vergleich von Standard-Installationen klassischer Telefonie-Lösungen ist der ungesicherte Einsatz von VoIP-Technologie mit deutlich größeren Risiken verbunden. Geeignete Sicherheitsmaßnahmen sind heute technisch und organisatorisch realisierbar. Bei der Auswahl eines Systems sollten daher die realisierten Sicherheitsmaßnahmen im Fokus stehen und nicht nur reine Funktionalitätsgesichtspunkte in die Entscheidung einbezogen werden. Die Kosten für die erforderlichen Sicherheitsmaßnahmen müssen daher bereits frühzeitig in die Planungen mit einbezogen werden. Am Ende sollte die Entscheidung für oder gegen den Einsatz von VoIP-Systemen immer zugunsten der IT-Sicherheit und damit des Mandatsgeheimnisses ausfallen. 7

49 Eine entsprechende Liste von Anbietern hält beispielsweise die Initiative Mittelstand unter: http://www.tk-voip-bestenliste.de bereit.

50 So *Freund*, DuD 2014, 523, 524.

51 http://m.heise.de/newsticker/meldung/Kommentar-zu-Netzausfaellen-Super-GAU-fuer-Voice-over-IP-2305606.html?from-classic=1.

G. Datenverlust trotz Datensicherung – Gefahren, die häufig unterschätzt werden

Wie in Bezug auf Cloud Computing noch an späterer Stelle angesprochen wird, ist es notwendig, von elektronisch gespeicherten Daten regelmäßig Datensicherungen zu erstellen. Diesem Erfordernis wird, wie die Praxis zeigt, nicht in jeder Anwaltskanzlei Rechnung getragen. Kommt es dann zu einem Festplattendefekt, sind mitunter die Daten der eingesetzten Anwaltssoftware oder auch E-Mail- und Adressdatenbanken verloren. Während in den letzten Jahren in derartigen Schadensfällen häufig noch Daten aus defekten Festplatten von spezialisierten Datenrettungsunternehmen wieder hergestellt werden konnten, macht die neueste Technik, insbesondere der Einsatz von SSD-Festplatten derartige Datenrettungen in den meisten Fällen unmöglich. Jeder Anwalt, der bislang noch nicht über ein Datensicherungskonzept verfügt oder die Sicherung der Daten als Prozess in die Abläufe der Kanzlei eingebunden hat, sollte sich daher fragen, was es für die Kanzlei bedeutet, wenn von einem Moment auf den anderen sämtliche elektronische Daten (elektronische Akte, Korrespondenzen, Daten des EGVP-Verfahrens, Buchhaltungsdaten) der Kanzlei unwiederbringlich zerstört sind. 1

An dieser Stelle sind sich wahrscheinlich alle Leser einig, dass Datensicherungen elementar zur Sicherung des Fortbestands einer Kanzlei beitragen. Davon abgesehen, befasst sich Datenschutz nicht nur damit, unberechtigte Zugriffe auf Daten zu verhindern. Wesentlicher Teil des Datenschutzes ist es auch, ungewollte Änderungen oder Löschungen sowie den Verlust von (personenbezogenen) Daten zu verhindern. Demnach ist Datensicherung eine der elementarsten Aufgaben, wenn elektronische Datenverarbeitung zum Einsatz kommt. An dieser Stelle nun, wird der eine oder andere Leser denken: „Kein Problem – meine Mitarbeiter wechseln ja jeden Tag die Sicherungsbänder“. 2

Genau hier liegt häufig das Problem. Das tägliche Wechseln von Bändern wiegt uns zuweilen in Sicherheit. Zuweilen werden hier Bänder verwendet, bei denen sich durch den häufigen Gebrauch über die Jahre bereits die Beschichtungen abgelöst haben. Die Bänder können dann längst keine Daten mehr aufnehmen oder sichern, werden aber immer noch jeden Tag gewechselt. Das „große Hallo“ kommt dann, wenn ein Gerät oder eine Festplatte defekt ist und die Datensicherung vom Vortag eingespielt werden soll. An diesem Punkt fällt dann häufig auf, dass die Datensicherung entweder auf den Bändern oder Medien nicht vorhanden ist oder aber nicht funktioniert. Trotz täglichen Aufwands und gewissenhaften Wechseln der Sicherungsmedien ist die betroffene Kanzlei dann am selben Punkt angelangt, an dem sie wäre, hätte man nie eine Datensicherung erstellt. Es ist daher unverzichtbar, auch regelmäßig zu überprüfen, ob das, was gesichert wurde, auch verwertbar ist. Das kann z.B. dadurch erfolgen, dass in ein Testverzeichnis alle 14 Tage oder 4 Wochen ein paar Dateien zurück gesichert werden. Niemals sollten bei einem solchen Rücksicherungstest allerdings die Daten in die produktiven Verzeichnisse eingespielt werden und dort andere Daten überschreiben! Des Weiteren ist darauf zu achten, dass der Rücksicherungstest nicht immer von ein und demselben Sicherungsmedium ausgeführt wird, das vielleicht das einzige ist, das noch funktionsfähig ist. Soweit Sicherungsbänder verwendet werden, sollte bei der ersten Verwendung ein Datum festgelegt werden, zu dem ein Band ersetzt werden muss. Das kann von Medientyp zu Medientyp unterschiedlich sein und hängt auch davon ab, wie häufig ein Band oder Datenträger überschrieben oder genutzt wird. Eine solches Verfallsdatum könnte z.B. nach einem oder nach zwei Jahren festgelegt werden. Nicht nur das Alter kann Speicher- und Sicherungsmedien unbrauchbar werden lassen. Die Lagerung kann hier ebenfalls einen wesentlichen Teil dazu beitragen, dass Sicherungen bei Bedarf nicht mehr funktionsfähig sind. Die klassischen Sicherungsmedien nutzen elektromagnetische Eigenschaften eines Trägermaterials, um Daten zu speichern. Entsprechend können diese Speichermedien durch starke Magnetfelder massiv in ihrer Funktion/Brauchbarkeit beeinträchtigt werden. Darüber hinaus sind diese Speichermedien i.d.R. nur begrenzt resistent gegen hohe Temperaturen. Sie sollten also in keinem Fall der Wärmeeinwirkung einer Heizung oder der direkten Sonneneinstrahlung ausgesetzt werden. Ein weiterer Fehler in Bezug auf die Datensicherung be- 3

steht häufig darin, dass die Datensicherung zwar auf einer eigenen Festplatte erstellt wird, diese jedoch im Server eingebaut ist, der dadurch gesichert werden soll. Im Falle eines Blitzschlags, Feuers oder Wasserschadens, bedeutet das den Totalverlust der Daten. Ebenso wenig, wie eine Datensicherung auf dem gesicherten Server liegen soll, soll sie im selben Serverschrank oder Serverraum gelagert werden, in dem die Sicherung erfolgt. Brennt der Server oder Serverraum, würde sich die Datensicherung hier ebenfalls in Rauch auflösen. Das Zurückspielen einer Datensicherung ist i.d.R. die Ultima Ratio, wenn schwerwiegende Fehler im System auftauchen oder das System ganz oder teilweise zerstört wurde. Entsprechend sicher sollten Datensicherungen aufbewahrt werden. Entweder werden diese in einem Brandschutztresor eingelagert oder man lagert sie in einem anderen Gebäude oder in einem Bankschließfach ein.

Das setzt natürlich einen Transport der Datensicherungen voraus und es besteht die Möglichkeit, dass diese verloren gehen oder entwendet werden. Für diesen Fall ist es sinnvoll, Datensicherungen mit einem Passwort zu versehen und diese zu verschlüsseln. Entsprechendes bieten die meisten aktuellen Programme zur Datensicherung an. 4

Wie sollte nun in der Kanzlei eine Datensicherung erfolgen?

Natürlich ist es abhängig von Art und Umfang der Daten, die gesichert werden, wie die Datensicherung in der Kanzlei strukturiert ist. Wird ein Rechner nur als Schreibmaschine verwendet und sind alle Schriftstücke/Akten in gedruckter Form verfügbar, so werden die Anforderungen an die Datensicherung sicherlich nicht so komplex und umfangreich sein. Auch die Datenmenge wird sich in diesem Fall in einer überschaubaren Größenordnung bewegen. Es wäre hier ausreichend, täglich die Änderungen und neuerstellten Dateien auf einen externen Datenträger zu kopieren. Hier sollten allerdings mindestens zwei externe Datenträger zum Einsatz kommen, die abwechselnd verwendet und dann jeweils außerhalb sicher eingelagert werden. Darüber hinaus kann dann z.B. wöchentlich noch eine CD mit dem gesamten Datenbestand erstellt werden, die ebenso wie die Installationsmedien sicher verwahrt wird. 5

Bei einer Großkanzlei, bei der die Abläufe ganz wesentlich vom sicheren Betrieb der IT-Anlagen abhängen und eine datenbankgestützte Kanzleisoftware eingesetzt wird, sind die Anforderungen an die Datensicherung i.d.R. erheblich größer. Hier spielt insbesondere die Frage eine tragende Rolle, welche maximale Standzeit der IT-Anlagen im Havariefall kompensierbar ist. Es ist hier durchaus sinnvoll, mehrere Strategien und Methoden der Datensicherung zu kombinieren. So kann z.B. eine Image-Sicherung erfolgen, die es erlaubt, einen kompletten Server auf anderer Hardware innerhalb von zwei bis drei Stunden wiederherzustellen. Derartige Imagesicherungen können, über den Tag hin, mehrere Wiederherstellungspunkte definieren, auf deren Stand dann ein Ersatzgerät zeitnah zur Verfügung gestellt werden kann. Auch wenn diese Systeme z.T. über die Fähigkeiten verfügen, auch installierte Datenbanken wiederherstellbar mitzusichern, sollte eine Datenbank immer auch separat gesichert werden. Des Weiteren empfiehlt sich auch eine Sicherung auf Dateiebene, so dass relativ schnell von der einzelnen Datei über die Datenbank bis zum kompletten Server alles wiederhergestellt werden kann und die Datensicherungen z.T. auch inhaltlich redundant sind. Wird das Backup ordentlich geplant, so ist es durchaus realistisch, die Serversysteme einer Großkanzlei innerhalb eines Zeitraums von 8 bis 12 Stunden, selbst wenn die Kanzlei bis auf die Grundmauern niedergebrannt ist, wieder verfügbar zu haben. 6

Alles in allem reicht es also nicht, jeden Tag Bänder zu wechseln und zu hoffen, dass man die Datensicherung nie braucht. Die Datensicherung ist ein elementares Erfordernis, das im Havariefall den Fortbestand der Kanzlei sichern kann. Die folgenden Regeln sollen eine kleine Hilfestellung geben, damit Ihre Datensicherung Ihren Zweck erfüllt. 7

Regel 1: Datensicherungskonzept erstellen und dafür Sorge tragen, dass danach verfahren wird.
Regel 2: Regelmäßig soll ein Rücksicherungstest in ein Testverzeichnis durchgeführt werden, um sicherzustellen, dass Sicherung und Rückspeicherung funktionieren.

Regel 3: Soweit Sicherungsbänder verwendet werden, sollen diese mit einem Datum versehen sein, wann sie zu ersetzen sind.

Regel 4: Schützen Sie Sicherungsbänder/Speichermedien vor starken Magnetfeldern und vor Hitzeeinwirkung.

Regel 5: Datensicherungen sollen räumlich getrennt von den gesicherten Anlagen aufbewahrt werden. Günstigerweise erfolgt die Lagerung in einem Brandschutztresor und/oder in einem anderen Gebäude.

Regel 6: Datensicherungen sollen passwortgeschützt (Bandsicherung) und verschlüsselt gespeichert werden.

Regel 7: Der Backup-Plan sollte Teil eines Notfallkonzepts sein, in dem (kurz, aber nachvollziehbar) beschrieben ist, wie im Katastrophenfall die Kanzlei weiterarbeiten kann.

H. Warum Sie die Datenträger in Ihrer Kanzlei verschlüsseln sollten

War dieses Kapitel ursprünglich dem Thema Verschlüsselung von Notebook-Festplatten gewidmet, so zeigte ein aktueller Fall, dass bestimmte Umstände nicht nur im Zusammenhang mit einem Notebook auftreten können. 1

Wie das Swiss IT-Magazine bereits in seiner Ausgabe 2005/19[52] schrieb, lag damals eine Statistik der Londoner Polizei für das Jahr 2001 vor, aus der hervorging, dass innerhalb eines Jahres dort 2.900 Notebooks und 1.300 PDAs in Taxis vergessen wurden. Damals gehörten mobile Geräte längst nicht in dem Maße zum täglichen Leben, wie das heute der Fall ist. Verlust und Diebstahl mobiler Geräte ist heute an der Tagesordnung. Was aber, wenn Ihnen ein Notebook verloren geht, auf dem Sie elektronische Akten und Unterlagen gespeichert haben? 2

Soweit Sie mit mobilen Geräten arbeiten und diese auch außerhalb der Kanzlei bei sich führen, ist die Gefahr des Verlustes allgegenwärtig. Also sind präventive Maßnahmen unerlässlich, um zu vermeiden, dass Personen, die Ihr Gerät an sich bringen, Zugriff auf die personenbezogenen Daten Ihrer Mandanten erhalten. 3

Ein probates Mittel, das einfach zu realisieren ist, ist die Festplattenverschlüsselung. Grundsätzlich sollte Ihr Notebook auch immer passwortgeschützt sein. Der Passwortschutz allein reicht aber beim Abhandenkommen des Geräts nicht aus, um den Zugriff auf Daten zu verhindern.[53] Um in diesem Fall auf Ihre Daten zuzugreifen, genügt es dann nämlich, die Festplatte auszubauen, in ein USB-Festplattenrahmen einzubauen und an einen anderen Rechner anzuschließen. Der Passwortschutz wurde dann ausgehebelt und der Zugriff auf Dateiebene ist möglich. Daher sollten die Festplatten eines Notebooks immer verschlüsselt sein. In diesem Fall würde dann der Versuch eines Dritten, auf die Dateien zuzugreifen, nur kryptische Zeichenfolgen liefern. Mittlerweile werden auch Einbaugeräte für Notebooks angeboten, mit denen diese mit GPS-Unterstützung wiedergefunden werden können. Das hat jedoch keine Auswirkungen auf die Notwendigkeit der Festplattenverschlüsselung. Alternativ könnten einzelne Verzeichnisse und Dateien verschlüsselt werden. Wichtig dabei ist, dass beim Abhandenkommen des Geräts keine Mandantendaten (auch keine Mitarbeiterdaten) in falsche Hände gelangen. 4

Die PDAs (Personal Digital Assistent), also die elektronischen Adressbücher und Terminplaner des Jahres 2001 (s.o.) sind zum Großteil heute den Smartphones gewichen, die neben den Funktionalitäten von Telefon, Internet und diversen Programmen auch den Funktionsumfang ihrer Urahnen bieten. Durch die kompakte Bauweise sind Smartphones aller Voraussicht nach noch deutlich mehr gefährdet, was Verlust und Diebstahl angeht, als das bei Notebooks der Fall ist. Hier wird empfohlen, grundsätzlich das Gerät so einzurichten, dass ein potentieller Dieb/Finder in angeschaltetem Zustand nicht sofort Zugriff auf Funktionen und Daten hat. Darüber hinaus sollte unbedingt eine Schutzsoftware installiert sein, die es ermöglicht, bei Verlust sämtliche darauf befindliche Daten zu löschen. 5

Häufig wird allerdings die Gefährdung für die stationär eingesetzten Rechner unterschätzt. Gerade in Innenstädten und Bereichen, in denen ein hohes Maß an Beschaffungskriminalität gegeben ist, sollten Sie Überlegungen anstellen, ob Ihre Kanzlei ausreichend gegen Einbruch und Diebstahl abgesichert ist. Ansonsten wäre es empfehlenswert, sämtliche Datenträger zu verschlüsseln. Schließlich und endlich bleiben noch weitere Datenträger wie USB-Sticks, DVD, USB-Festplatten und andere. Auch hier sollten Sie Daten verschlüsseln oder USB-Sticks einsetzen, die über eine sichere Verschlüsselung verfügen. Je kleiner die Komponenten sind, desto eher können sie abhandenkommen. Gut zu wissen, dass in einem solchen Fall keine unberechtigten Personen auf Ihre Daten bzw. die Daten Ihrer Mandanten zugreifen können. 6

52 Sicherheit durch Datenverschlüsselung; Swiss IT-Magazine, Ausgabe 2005/19, Online-Version unter: http://www.itmagazine.ch/Artikel/28892/Sicherheit_durch_Datenverschluesselung.html.

53 *Lenhard, Th.*, Datenschutz für Heilpraktiker, in: Der Heilpraktiker – Fachzeitschrift für Natur- und Erfahrungsheilkunde, Ausgabe 09/2014.

Regel 1: Verschlüsseln Sie Daten oder Festplatten aller mobilen Geräte, die Sie außerhalb der Kanzlei verwenden. **7**

Regel 2: Soweit Einbruch und Diebstahl von Geräten in Ihrer Kanzlei nicht ausgeschlossen werden kann, sollten die Datenträger aller Rechner verschlüsselt werden.

Regel 3: Soweit Sie USB-Sticks verwenden, sollten diese über eine sichere Verschlüsselung verfügen. Alle anderen externen Datenträger sollten ebenfalls verschlüsselt sein.

I. Cloud-Computing und Weblösungen in der Anwaltskanzlei

Vereinzelt werden bereits von Anwaltskanzleien Cloud-Lösungen eingesetzt. Aus diesem Grund soll hier zunächst die Frage behandelt werden, was Cloud-Computing überhaupt ist und wie es – grob skizziert – funktioniert. Im nächsten Schritt werden dann die Fragen beantwortet, wie sicher Cloud-Computing ist und unter welchen Gegebenheiten es für eine Anwaltskanzlei einsetzbar ist. 1

Böse Zungen behaupten, dass der Begriff eigentlich weniger auf das englische Wort für Wolke hinweist als auf die Situation, dass hier unter Umständen Daten „geklaut" werden. Gleich vorweg: Der englische Begriff bezeichnet tatsächlich eine (Daten-) Wolke. Allerdings ist die deutsche Variante der Interpretation auch nicht von der Hand zu weisen, denn in jüngster Vergangenheit gab es zahlreiche, zum Teil recht schwerwiegende Vorfälle im Zusammenhang mit Cloud-Computing. 2

Wie funktioniert nun eine solche Cloud?

Eine Cloud ist eine Infrastruktur, die i.d.R. für den Nutzer oder Kunden des Anbieters über das Internet zu erreichen ist. Zwar kann Cloud-Computing viele Facetten der Informationstechnologie abbilden, jedoch beschränkt sich die vorliegende Betrachtungsweise zunächst auf die Speicherung von Dateien durch den Nutzer. Auf umfangreichere Lösungen des Cloud-Computing wird am Ende des Kapitels eingegangen. Der Anwender/Nutzer, das wären dann ggf. Sie, muss sich je nach Struktur der verwendeten Lösung an dem Cloud-System anmelden und kann Dateien dort ablegen und Verzeichnisse erstellen oder er hat die Cloud als Laufwerk auf seinem Rechner verknüpft und kann dort direkt seine Daten/Dateien speichern. Der Vorteil dieser Speicherung liegt erst einmal auf der Hand. Alle, die in der Kanzlei auf entsprechende Dateien zugreifen müssen, haben den Zugriff zur Cloud. Das wäre mit einem Dateiserver in der Kanzlei natürlich auch möglich. Zusätzlich zum internen Zugriff kann aber auch – hoffentlich nur bei entsprechender Authentifizierung – über das Internet auf die Dateien/Unterlagen zugegriffen werden. Dieser Zugriff auf die Daten in der Cloud, der im Allgemeinen sogar mittels eines Smartphones möglich ist, ist also standortunabhängig und kann ebenso aus dem nächstgelegenen Amtsgericht wie vom anderen Ende der Welt erfolgen. Damit liegt der große Vorteil der Nutzung einer Cloud klar vor Augen. Betrachten wir jedoch den Prozess, was passiert, wenn ein anwaltliches Schreiben, in dem i.d.R. personenbezogene Daten eines Mandanten auftauchen, welche nicht für die Öffentlichkeit bestimmt sind, in der Cloud gespeichert wird, so wird deutlich, dass die Entscheidung für Cloud-Computing sehr weitreichende Folgen haben kann. Cloud-Computing bedeutet, dass üblicherweise eine große Anzahl von Anwendern ihre Daten auf der Infrastruktur eines Anbieters speichern. Dabei schreiben die Nutzer ihre Daten auf die gleichen Laufwerke und nutzen die gleichen Datenbanken für die Zugriffskontrolle. Grundsätzlich sieht der Nutzer nur eine bzw. seine logische Sichtweise. Angezeigt werden seine Verzeichnisse und seine Dateien. Tatsächlich wird hier aber unter Umständen eine Trennung vorgegaukelt, die so nicht gegeben ist. Wenn der Anbieter z.B. damit wirbt, dass die Festplatten verschlüsselt sind, dann mag dass im Falle des Austauschs eines defekten Datenträgers ein gewisses Maß an Sicherheit geben, dass die Daten von Dritten nicht ohne größeren Aufwand gelesen werden können. Auch wenn eine Verschlüsselung beschränkten Schutz bietet, falls ein Server entwendet wird, sind dann aber alle Daten der Nutzer gleich verschlüsselt. Das bedeutet, dass die Mitarbeiter des Cloud-Anbieters in einem solchen Fall – soweit nicht zusätzlich jede einzelne Datei verschlüsselt ist – auf alle Dokumente Zugriff nehmen können, die von Ihrer Kanzlei dort gespeichert wurden. Das ist sicherlich so nicht gewollt. Ebenso wie es zu vermeiden gilt, dass Akten der Kanzlei im Internet für jedermann einsehbar sind. Hier wird der eine oder andere Leser vielleicht Zweifel haben, ob diese größte anzunehmende Katastrophe für eine Kanzlei denn realistisch sei. Nachdem bereits eine vierstellige Zahl an Psychiatrie-Akten offen im Internet verfügbar war, sollte Entsprechendes für den Bereich der Anwaltskanzleien nicht leichtfertig für unmöglich erklärt werden. Daher ist die erste Regel, die Sie bei Nutzung einer Cloud beachten sollten, diejenige, dass Dateien und Dokumente bereits in der Kanzlei verschlüsselt werden, bevor sie in der Cloud gespeichert werden. 3

Die Vorteile der Cloud können Sie trotzdem nutzen, soweit Sie auf Ihren mobilen Geräten den entsprechend Schlüssel bzw. die Verschlüsselungssoftware installiert haben, die für den lesbaren Zugriff auf Ihre Dokumente erforderlich ist. Mittlerweile ist zu diesen Zwecken Software verfügbar, bei deren Einsatz der Nutzer nicht einmal merkt, dass jede Datei auf dem Verzeichnis, auf dem er arbeitet, verschlüsselt ist und nur in verschlüsselter Form auch dort abgelegt werden kann.

Außerhalb der EU bzw. des EWR kann davon ausgegangen werden, dass in vielen Regionen der Welt so etwas wie Datenschutz nicht existent ist. Wie uns durch Edward Snowden und die jüngsten Ausspähskandale hinlänglich bekannt sein dürfte, zählen zu diesen „datenschutzrechtlichen Entwicklungsländern" auch die Vereinigten Staaten von Amerika. Nach dem derzeitigen Stand verfügbarer Informationen erscheint also eine Speicherung von Daten in den USA grundsätzlich als nicht ausreichend sicher. Davon abgesehen, ist eine entsprechende Speicherung von Mandantendaten (personenbezogene Daten) in den USA ohne Vorliegen einer Rechtsgrundlage, welche dieses explizit erlauben würde, unzulässig. 4

Der größte Vorteil des Cloud-Computing, nämlich die weltweite Erreichbarkeit einer Cloud ist zugleich auch ihre größte Schwäche. Eine große Menge personenbezogener Daten weckt Begehrlichkeiten. Daten, die über das Internet weltweit erreichbar sind, können entsprechend auch weltweiten Angriffen und Ausspähversuchen ausgesetzt sein. Auch wenn die Daten nur in Ihrer Kanzlei ver- und entschlüsselt werden können, sollten Sie dennoch ausschließlich verschlüsselte Kommunikationsverbindungen zur Cloud verwenden. 5

Ein Vorfall bei einem großen Cloud-Anbieter im Jahr 2012 hat einen bei den Nutzern vielverbreiteten Irrglauben aufgedeckt. Viele Cloud-Nutzer sind nämlich der Auffassung, dass die Cloud nicht nur hinsichtlich von Fremdzugriffen sicher wäre, sondern auch hinsichtlich der Verfügbarkeit der Daten. Bei dem v.g. Anbieter kam es hinsichtlich eines Teils der dort gespeicherten Daten zu einem Totalverlust. Die Reaktion darauf seitens des Anbieters war ein lapidarer Verweis auf seine Geschäftsbedingungen und hier insbesondere auf einen Passus, dass jeder für die Datensicherung (Backup) seiner Daten selbst verantwortlich ist. Cloud-Benutzung kann also hinsichtlich der Datensicherheit (hier: Vermeidung von Datenverlust) mitunter ein erhöhtes Risiko mit sich bringen, soweit das Vorhandensein ausreichender Datensicherungen nicht sichergestellt ist. Soweit Server gesichert werden, welche in der Kanzlei betrieben werden, ist es sinnvoll und notwendig, entsprechende Sicherungen außerhalb der Kanzlei einzulagern, damit bei einem Feuer- oder Wasserschaden nicht gleichzeitig die Server und ihre Datensicherungen zerstört werden. Soweit die Daten der Kanzlei außerhalb auf einer Cloud gespeichert werden, ist es vertretbar die Datensicherungen dieser Daten in der Kanzlei aufzubewahren. Schließlich sollten hier auch erweiterte Cloud-Lösungen kurz angesprochen werden, da derartige Systeme mittlerweile speziell für Kanzleien angeboten werden oder zumindest von diesen unterstützend eingesetzt werden können. Hierbei handelt es sich um webbasierte Dienste, die nicht nur als Datenspeicher fungieren, sondern browserbasierte Softwarelösungen zur Verfügung stellen. Das Spektrum reicht dabei von Plattformen, welche die Abwicklung von Schadensfällen erleichtern, bis zur vollständigen Kanzleisoftware. Die Vorteile der schnellen und unkomplizierten Kommunikation sowie der Kostenersparnis liegen auf der Hand. Dennoch ist bei der Nutzung derartiger Lösungen auch einiges zu beachten. 6

Notwendigkeit ADV-Vertrag

Nach herrschender Ansicht verlieren Daten ihren Personenbezug auch nicht durch Verschlüsselung (sog. absolute Personenbezogenheit), sodass hierdurch die Anforderungen des Datenschutzrechts nicht einfach ausgehebelt werden können. Eine inhaltliche Verarbeitung der Daten in verschlüsselter Form ist zudem kaum möglich, sodass sich der Nutzen einer „verschlüsselten Cloud" ohnehin nur auf die externe Speicherung beschränkt. In jedem Fall ist mit der Übermittlung von Mandantendaten in die Cloud damit 7

ein datenschutzrelevanter Vorgang verbunden. Das Verhältnis zum Cloud-Anbieter ist als Auftragsdatenverarbeitung im Sinne des § 11 BDSG zu qualifizieren.[54]

8 Eine von den Datenschutzbeauftragten des Bundes und der Länder herausgegebene „Orientierungshilfe – Cloud Computing" weist ausdrücklich darauf hin, dass nach § 11 Abs. 2 Satz 4 BDSG der Cloud-Anwender, also der Nutzer einer Cloud-Lösung vor Beginn der Datenverarbeitung und sodann regelmäßig sich vom den beim Cloud-Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat.[55] Das aktive Handeln des Auftraggebers ist hierbei Voraussetzung. Das heißt, dass er Informationen anfordern muss oder die technischen und organisatorischen Maßnahmen durch eigene Inaugenscheinnahme bei beim Auftragsdatenverarbeiter prüfen muss. Es ist mitunter ausreichend, wenn der Auftragsdatenverarbeiter regelmäßig von einer unabhängigen sachverständigen Stelle auf die Einhaltung der datenschutzrechtlichen Bestimmungen und die Datenschutzkonformität hinsichtlich organisatorischer und technischer Maßnahmen geprüft wird oder aktuelle Zertifizierungen vertrauenswürdiger Zertifizierungsstellen wie z.B. dem Bundesamt für Sicherheit in der Informationstechnik, dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein oder der EuroPriSe GmbH vorweisen kann. Mit Hinweisen auf irgendwelche wohlklingenden US-Normen oder außereuropäische Zertifikate ist hier niemandem geholfen.[56] Auch mündliche Zusagen, dass man sich gerade im Zertifizierungsprozess befinden würde, sind nutzlos. Soweit entsprechende Zertifizierungen nicht nachgewiesen werden können, gestaltet sich die Prüfung organisatorischer und technischer Maßnahmen mitunter schwierig. So stellen sich dann Fragen wie z.B., ob die eingesetzte Verschlüsselung dem Stand der Technik entspricht. Das BSI-Grundschutzhandbuch beschreibt z.B. unter der Kategorie M 2.164 (Auswahl eines geeigneten kryptographischen Verfahrens), dass der Schlüssel eines symmetrischen kryptographischen Verfahrens eine Mindestlänge von 100 Bit haben soll.[57] Eine am 10.2.2014 vom BSI herausgegebene technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen"[58] legt jedoch fest, dass fortan für neue Anwendungen nur noch Blockchiffren (Schlüssel) verwendet werden sollen, deren Länge mindestens 128 Bit beträgt. Dieser Umstand steht exemplarisch für die Weiterentwicklung technischer Standards bzw. des Stands der Technik. Ein 128 Bit langer Schlüssel würde demnach bei Einsatz symmetrischer Verschlüsselungsverfahren aktuell gerade noch dem Stand der Technik entsprechen. Wie das Beispiel zeigt, ist ein hohes Maß an Spezialwissen erforderlich, um entsprechende Fragestellungen bewerten zu können. Bei Nichtvorliegen von adäquaten Zertifizierungen oder qualifizierten Audit-Ergebnissen können unzählige Fallstricke zum Problem werden. Wesentlich dabei ist, dass der Auftraggeber der Datenverarbeitung, das sind eventuell Sie, in der Verantwortung steht, dass die Daten ordnungsgemäß verarbeitet werden. Diese Verantwortung können Sie nicht auf einen Auftragsdatenverarbeiter delegieren. Hier ist eine Kanzlei dann schnell durch die Komplexität des für viele Juristen fremden Themengebiets überfordert, so dass empfohlen wird, vor Einsatz von erweiterten Cloud-Lösungen einen unabhängigen Datenschutzexperten zu konsultieren.

9 Durch den Einsatz erweiterter Weblösungen kann eine Kanzlei signifikante Einsparungen erzielen. Für den Einsatz solcher Systeme ist es jedoch elementar, dass nicht nur die Chancen und Vorteile betrachtet werden, sondern der Nutzer sich auch mit den damit verbundenen Pflichten auseinandersetzt. Ganz besonders sollte eine Frage betrachtet werden: Habe ich eine tägliche Datensicherung oder kann ich noch

54 *Wagner/Blaufuß*, BB 2012, 1751, 1752.

55 Orientierungshilfe – Cloud Computing, Herausgegeben von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2011.

56 *Kazemi/Lenhard*, Cloud-Computing – Entwicklung für den Datenschutz in Kliniken, in: KHIT-Magazin, Ausgabe 02/2013.

57 BSI-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Kategorie M 2.164, http://www.bsi.bund.de, 2013.

58 BSI – Technische Richtlinie: Kryptographische Verfahren:
Empfehlungen und Schlüssellängen, Bundesamt für Sicherheit in der Informationstechnik, 2014.

arbeiten, wenn der Webservice nicht erreichbar ist (z.B. DSL-Störung), und was bedeutet ein Datenverlust beim Anbieter des Dienstes für meine Kanzlei?

Cloud-Nutzung bringt also nicht nur Vorteile, sondern auch Pflichten mit sich. Im Zusammenhang mit Cloud-Computing sollte also eher weniger Glauben wohlklingenden Werbetexten geschenkt werden. Auch sollte man sich keinesfalls auf Auskünfte von Anbietern verlassen, dass man keinen Vertrag zur Auftragsdatenverarbeitung (§ 11 BDSG) bräuchte, denn verantwortlich für die ordnungsgemäße Verarbeitung personenbezogener Daten sind Sie, sofern Sie eine Web- oder Cloud-Lösung nutzen. In seiner Werbung wird üblicherweise jeder Anbieter für sich in Anspruch nehmen, der Beste und Sicherste zu sein. Dabei scheuen manche Anbieter – da unterscheiden sich die Cloud-Anbieter nicht von Rechenzentrumsbetreibern oder Software-Unternehmen – die Zertifizierung ihrer Dienste ebenso wie der Teufel das Weihwasser scheut. Allerdings deckt die Branche hier die gesamte technische Palette ab, angefangen von unverantwortlichen Lösungen bis zu Varianten, die nach dem Stand der Technik als sicher gelten können. Generell wird also nicht von Cloud-Computing abgeraten. Es sollte aber genauestens geprüft werden, ob eine Lösung die hier beschriebenen Kriterien erfüllen kann. **10**

Natürlich gibt es auch die Alternative, eine für professionelle Einsätze geeignete VPN-fähige (VPN = Virtual Private Network) Firewall in der Kanzlei zu installieren und weitere sicherheitsrelevante Implementierungen vorzunehmen, damit man weltweit auf seinen eigenen Server zugreifen kann. Darüber hinaus wäre ein Online-Archiv eine weitere mögliche Alternative für die Dateispeicherung, da man hier über seine eigene (in sich geschlossene) Datenbank verfügt und i.d.R. gespeicherte Daten sowie Kommunikationskanäle hochverschlüsselt sind. **11**

„doculife Law" als Cloud-Alternative

Wer nicht auf die Cloud verzichten möchte, sollte bei der Auswahl seines Cloud-Anbieters auf fachliche Beratung zurückgreifen, um die technischen Risiken des jeweiligen Services im Vorfeld genau einschätzen zu können. In diesem Zusammenhang ist das Projekt „doculife Law" von Telekom und T-Systems hervorzuheben, das in Kooperation mit der davit (Arbeitsgemeinschaft IT-Recht im DAV) angeboten und entwickelt wurde. Die Cloudlösung „doculife Law" bietet neben einer revisionssicheren Datenspeicherung zusätzlich ein sicheres Dokumentenmanagement aus der Cloud. Einen entsprechenden Kooperationsvertrag haben die Telekom-Tochter und die davit im Jahr 2013 unterzeichnet. Über die Cloud-Lösung können Dokumente erstellt, bearbeitet und archiviert sowie beliebig viele digitale Akten angelegt werden.[59] Auf Wunsch werden die an die Cloud übertragenen Daten Ende-zu-Ende und mindestens gemäß AES 256 verschlüsselt. **12**

Finger weg von der iCloud im anwaltlichen Berufsalltag

Dringend abzuraten ist jedoch von der Nutzung der sog. Apple iCloud.[60] Diese scheint auf den ersten Blick praktisch und für den Apple-Fan unter den Rechtsanwälten genau die richtige Lösung zu sein. Mit Blick auf die strengen Vorgaben zum Geheimnisschutz in § 203 StGB und dem anwaltlichen Berufsrecht (§ 43a Abs. 2 S. 1 und 2 i.V.m. § 2 BORA), lohnt sich aber ein Blick in die Nutzungs-AGB dieses Services.[61] Hier wird schnell deutlich, dass sich zumindest Apple die jederzeitige Einsichtnahme in den Inhalt der in die Cloud hochgeladenen Daten vorbehält. So heißt es hier u.a.: **13**

59 Näheres hierzu unter: http://www.davit.de/fileadmin/pdf/doculife_Law_www.pdf.

60 Ausführlich hierzu: *Schelzke*, HRRS 2013, 86 ff., abrufbar unter: http://www.hrr-strafrecht.de/hrr/archiv/13-03/index.php?sz=7.

61 Abrufbar unter: http://www.apple.com/legal/internet-services/icloud/de/terms.html.

„Apple behält sich jedoch das Recht vor, jederzeit zu prüfen, ob Inhalte angemessen sind und mit dieser Vereinbarung übereinstimmen, und Apple ist berechtigt, Inhalte jederzeit ohne vorherige Ankündigung nach eigenem Ermessen herauszufiltern, zu verschieben, abzulehnen, zu modifizieren und/oder zu entfernen, wenn diese Inhalte diese Vereinbarung verletzen oder in sonstiger Weise anstößig sind."

Weiter heißt es:

„Sie erklären sich damit einverstanden, dass Apple, ohne Ihnen gegenüber zu haften, auf Ihre Accountinformationen und ***Ihre Inhalte zugreifen****, diese* ***nutzen, aufbewahren und/oder an Strafverfolgungsbehörden, andere Behörden und/oder sonstige Dritten weitergeben darf****, wenn* ***Apple der Meinung ist, dass dies vernünftigerweise erforderlich oder angemessen ist****, wenn dies gesetzlich vorgeschrieben ist oder wenn Apple einen hinreichenden Grund zu der Annahme hat, dass ein solcher Zugriff, eine solche Nutzung, Offenlegung oder Aufbewahrung angemessenerweise notwendig ist."*

Es liegt auf der Hand, dass eine solche Befugnis in keinem Fall mit den besonderen Geheimnispflichten des anwaltlichen Berufsalltages zu vereinbaren ist. Wer darüber hinaus auch noch meint, die Daten seien in der iCloud wenigsten technisch sicher aufgehoben, sollte auch hier in die AGB schauen, die ausdrücklich darauf hinweisen, dass Apple gerade nicht garantiert, dass die Inhalte, *„die Sie über den Dienst speichern oder auf die Sie mit Hilfe des Dienstes zugreifen, nicht versehentlich* ***beschädigt oder verfälscht werden, verloren gehen oder gelöscht werden.****"* Schließlich sollte man sich vergegenwärtigen, dass die Server der Firma Apple in den USA stehen, folglich werden auch die Daten dort gespeichert. Die Datenintegrität und Datensicherheit sind damit nicht gewährleistet. Aus diesem Grunde hat die iCloud im anwaltlichen Berufsalltag nichts zu suchen. **14**

Soweit Sie sich für die Nutzung von Cloud-Computing entscheiden, sollten Sie folgende Regeln[62] beachten: **15**

Regel 1: Daten werden bereits in der Kanzlei verschlüsselt, bevor sie in die Cloud eingestellt werden.

Regel 2: Es erfolgt keine Speicherung bei Cloud-Anbietern, die außerhalb der EU bzw. des EWR tätig sind, oder bei Cloud-Anbietern, die ganz oder teilweise ihre Cloud-Server außerhalb der EU bzw. des EWR betreiben.

Regel 3: Mit der Cloud wird nur über verschlüsselte Verbindungen kommuniziert.

Regel 4: Cloud-Computing befreit nicht von der Notwendigkeit, Daten zu sichern. Es muss stets dafür Sorge getragen werden, dass funktionierende Datensicherungen verfügbar sind.

Regel 5: Vor Nutzung einer Cloud-Lösung und danach regelmäßig müssen Sie sich von den zum Schutz der Daten getroffenen organisatorischen und technischen Maßnahmen beim Cloud-Anbieter überzeugen. Lassen Sie sich Zertifikate vorlegen und vertrauen Sie keinen noch so blumigen Versprechen, was Datenschutz und Datensicherheit angeht.

62 Ausführlich zum Cloud-Computing auch der Leitfaden Cloud-Computing der BITCOM, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf.

J. Outsourcing in der Anwaltskanzlei – Ein berufs- und strafrechtliches Problem?

Auch im Anwaltsleben hat das "Outsourcing" zwischenzeitlich an Bedeutung gewonnen.[63] Virtual Offices, externe Schreibbüros, virtuelle Sekretariate etc. stoßen auch beim Rechtsanwalt mehr und mehr auf Interesse. Wer als Rechtsanwalt externe Dienstleister durch das Outsourcing mit Mandantendaten in Berührung bringt, etwa im Wege der Auslagerung von elektronischen Aktenbeständen oder weil der externe Dienstleister als Telefonzentrale des Rechtsanwaltes fungiert, vollzieht datenschutzrechtlich relevante Vorgänge in Bezug auf die in seiner Kanzlei befindlichen personenbezogenen Daten. 1

Eine Einwilligung der Betroffenen, d.h. der Mandanten, liegt dabei regelmäßig nicht vor. Oftmals ist dem Mandant die Art und Weise der Büroorganisation des Rechtsanwaltes vielmehr gar nicht bekannt. Wer in der Rechtsanwaltskanzlei von Rechtsanwalt Mustermann anruft, geht (jedenfalls noch) davon aus, dass er auch in der Rechtsanwaltskanzlei Mustermann landet und nicht etwa in einer Telefonzentrale, die durch ein selbstständiges Unternehmen betrieben wird. Der Anrufer wird daher in der Regel davon ausgehen, dass die ihm am Telefon entgegentretenden Personen in die betriebliche Organisation des Rechtsanwaltes im Rahmen bestehender Beschäftigungsverhältnisse und damit im Rahmen der diesen Beschäftigten zustehenden Verschwiegenheitsverpflichtungen und Rechte[64] einbezogen sind. Tatsächlich handelt es sich hier jedoch um externe Dienstleister, die von den Privilegierungen des anwaltlichen Berufsstandes gerade nicht profitieren. Besondere spezialgesetzliche Tatbestände, die eine Übermittlung der Mandantendaten an Dritte und deren Speicherung und Nutzung gestatten würden, existieren nicht. 2

Die **anwaltliche Schweigepflicht** ist wesentliches Merkmal der besonderen Vertrauensbeziehung zwischen Anwalt und Mandant und damit eine der tragenden Säulen des Anwaltsberufes. Neben seiner besonderen Erwähnung in der Berufsordnung sind die anwaltliche Schweigepflicht (§ 203 StGB) und korrespondierend hierzu auch das anwaltliche Schweigerecht (§ 53 StPO) in den Strafgesetzen berücksichtigt worden. Nach § 203 Abs. 1 Nr. 3 StGB handeln Rechtsanwalt, Patentanwalt und Notar strafbar, wenn sie unbefugt ein fremdes Geheimnis, das ihnen im Rahmen ihrer Berufsausübung anvertraut oder sonst bekanntgeworden ist, Dritten gegenüber offenbaren. Pflichtwidrige Offenbarungen können mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden. Sie stellen sich gleichsam auch als Verstoß gegen die anwaltlichen Berufspflichten dar und können dementsprechend auch standesrechtlich mit Geldbußen, Verwarnungen und Rügen der zuständigen Kammern geahndet werden. Um den so verpflichteten Geheimnisträger davor zu schützen, die ihm offenbarten Geheimnisse, beispielsweise in strafrechtlichen Ermittlungsverfahren, Dritten gegenüber offenlegen zu müssen, korrespondiert hier auf strafprozessualer (§ 53 StPO) wie zivilprozessualer Ebene (§ 383 ZPO) ein Aussage- bzw. Zeugnisverweigerungsrecht des Rechtsanwalts. 3

Voraussetzung einer Strafbarkeit nach § 203 Abs. 1 Nr. 1 StGB ist die Offenbarung eines fremden Geheimnisses. Der **Geheimnis-Begriff** ist zwar nicht legal definiert, dennoch ist allgemein anerkannt, dass er mit Blick auf die Schutzrichtung des Gesetzes weit zu verstehen ist und damit grundsätzlich jede Tatsache umfasst, die nur einem Einzelnen oder einem beschränkten Kreis von Personen bekannt oder zugänglich ist und an deren Geheimhaltung der Betroffene ein von seinem Standpunkt aus berechtigtes Interesse hat.[65] Bereits die Tatsache des Bestehens eines Mandatsverhältnisses oder zumindest der (gewünschten) Inanspruchnahme anwaltlicher Dienste stellt nach allgemeiner Meinung damit bereits ein 4

63 Siehe hierzu auch die Beiträge von: *Jahn/Palm*, AnwBl. 2011, 613; *Brisch*, KammerForum RAK-Köln, 2010, 3; jüngst auch *Jandt/Nebel*, NJW 2013, 1570.

64 § 53a StPO, § 203 Abs. 3 StGB, § 2 Abs. 4 BORA.

65 *Lenckner/Eisele*, in: Schönke/Schröder (Hrsg.), StGB, 28. Aufl. 2010, § 203 Rn 5. Man spricht insoweit auch vom „Geheimhaltungswillen des Informationsherrn", vgl. *Popp*, in: Leipold/Tsambikakis/Zöller (Hrsg.), StGB, § 203 Rn 5; *Weidemann*, in: Beck-OK-StGB, § 203 Rn 4 m.w.N.; *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 11.

strafrechtlich relevantes Geheimnis dar, weil der (zukünftige) Mandant ein potentiell schutzwürdiges Interesse an ihrer Geheimhaltung haben kann.[66] Werden geschützte Geheimnisse unbefugt, d.h. ohne Einverständnis des betroffenen Mandanten (Schweigepflichtentbindungserklärung, vgl. § 385 Abs. 2 ZPO),[67] an Dritte weitergegeben ("offenbart"), stellt dies einen Verstoß gegen die in § 203 Abs. 1 Nr. 1 StGB normierte Geheimhaltungspflicht des Rechtsanwaltes dar. Eine **Offenbarung** in diesem Sinne liegt vor, sobald einem Dritten ein Wissen vermittelt wird, das diesem noch verborgen ist oder von dem er jedenfalls noch keine sichere Kenntnis hat.[68]

Da der Rechtsanwalt jedoch grundsätzlich nicht allein und ohne entsprechende Unterstützung von Mitarbeitern tätig werden kann, liegt ein strafbares Offenbaren erst und nur dann vor, wenn das Geheimnis aus der Sphäre des Geheimnisträgers hinausgelangt.[69] Der Straftatbestand wird daher nicht verwirklicht, wenn das Geheimnis lediglich im Kreis der zum Wissen Berufenen mitgeteilt wird. Ein strafrechtlich relevantes „Offenbaren" scheidet deswegen nach ganz herrschender Meinung gegenüber **Hilfskräften** (berufsmäßig tätige Gehilfen) des schweigepflichtigen Rechtsanwaltes aus. Die angestellte Rechtsanwaltsfachangestellte darf daher nicht nur über den Umstand des Bestehens eines Mandatsverhältnisses, sondern auch über den Inhalt desselben grundsätzlich ohne Einwilligung des betroffenen Patienten informiert werden. § 203 Abs. 3 Satz 2 StGB bezieht diese dauerhaft in die Kanzleiorganisation eingegliederten anwaltlichen Hilfspersonen folgerichtig in die anwaltliche Schweigepflicht mit ein;[70] auch die an die anwaltlichen Gehilfen mitgeteilten Informationen (Geheimnisse) unterliegen einem entsprechenden Aussage- oder Zeugnisverweigerungsrecht, vgl. § 53a StPO, § 383 Abs. 1 Nr. 6 ZPO.[71] 5

Mit Blick auf die dem Rechtsanwalt obliegende besondere Schweigepflicht ist die **anwaltliche Dokumentation vor Einsichtnahme und Zugriff unberechtigter Dritter zu schützen**. Der Rechtsanwalt hat daher sowohl bei konventionellen Handakten als auch beim Einsatz von Datenverarbeitungstechniken sicherzustellen, dass Dritte keinen unbefugten Zugriff (Einblick) in seine Akten erhalten. Handakten dürfen daher in keinem Fall so bereitgelegt werden, dass etwa Mandanten Daten anderer Mandanten zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Rechtsanwalt und dem Kanzleipersonal eingesehen werden können. Gegebenenfalls muss der EDV-Arbeitsplatz gesperrt werden, sodass auch wartende Mandanten in Abwesenheit von Rechtsanwalt und Kanzleipersonal keine Möglichkeit haben, Mandantendaten zur Kenntnis zu nehmen. 6

Vorsicht ist in diesem Zusammenhang auch bei der **Auslagerung von Dienstleistungen**, beispielsweise im EDV-Bereich, angebracht. So ist fraglich, wer unter den Begriff des berufsmäßig tätigen Gehilfen fällt. Unstreitig ist dies nur bei auf Dauer in der Rechtsanwaltskanzlei fest angestellten Mitarbeitern. Fest angestellte Mitarbeiter des Anwalts sind in seinen organisatorischen und weisungsgebundenen internen Bereich der vertrauensbegründenden Sonderbeziehung einbezogen und dementsprechend intern von der Geheimnispflicht befreit.[72] Auch der Rechtsanwalt ist ihnen gegenüber nicht zum Schweigen verpflichtet. Wie verhält es sich aber, wenn in der Rechtsanwaltskanzlei ein Computer defekt ist und dieser – mangels Sachkenntnis – weder der Anwalt noch seine Mitarbeiter beheben können? Der zur Reparatur berufene Techniker der Herstellerfirma ist sicher nicht als „Angestellter" in die anwaltliche Organisation eingebunden. Ist die Geheimniswahrungspflicht aus § 203 StGB verletzt, wenn anlässlich der Reparatur 7

66 *Weidemann*, in: BeckOK-StGB, § 203 Rn 5.2.

67 *Weidemann*, in: BeckOK-StGB, § 203 Rn 33 ff.; *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 54.

68 *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 48 m.w.N.; *Weidemann*, in: BeckOK-StGB, § 203 Rn 31 f. m.w.N.

69 *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 49 f.

70 *Weidemann*, in: BeckOK-StGB, § 203 Rn 22 m.w.N.

71 Vgl. *Reichold*, in: Thomas/Putzo (Hrsg.), ZPO, 34. Aufl. 2013, § 383 Rn 6.

72 Vgl. *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 50; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), StGB, 3. Aufl. 2010, § 203 Rn 38.

des Geräts auf gespeicherte Mandantendaten zugegriffen werden muss? Es erscheint auf den ersten Blick selbstverständlich, dass dies möglich sein muss. Ebenso wie in vielen vergleichbaren Fällen, bei denen Anwälte beispielsweise IT-Dienstleistungen auslagern (man denke nur an die Wartung von Praxis-EDV, über die Mandantendaten verarbeitet werden, oder auch externe Datenspeicherungen, Auslagerung von E-Mail-Diensten) oder sich externer Schreibdienste bedienen wollen, trifft dies jedoch auf rechtliche Hindernisse, die sich in der Gefahr strafbarer und berufsrechtswidriger Handlungen zeigen.

Damit ist die Frage aufgeworfen, ob ein enges Verständnis der Schweigepflicht aufgrund des rasanten technischen Wandels, der auch an Rechtsanwälten nicht spurlos vorbeischreitet, aufrechterhalten werden kann, erfordert eine effiziente Kanzleiorganisation doch in zahlreichen Fällen den Rückgriff auf externe Dienstleister ("Outsourcing"). Nachzugehen ist deshalb der Frage, ob unter dem Gesichtspunkt der Verletzung von Privatgeheimnissen tatsächlich straf- und berufsrechtliche Konsequenzen drohen können, wenn sich der Rechtsanwalt externer Dienstleister zur Erfüllung der ihm vom Mandanten übertragenen Aufgaben oder zur Aufrechterhaltung seines Kanzleibetriebes bedient. 8

Ein Blick in die strafrechtliche Literatur lässt hier Böses erahnen. So soll nach dort (noch) vorherrschender Auffassung eine organisatorische Einbindung des Gehilfen in den Betrieb des Berufsträgers notwendig sein, die sich in einer Weisungsabhängigkeit des Helfers niederschlägt.[73] Auch wenn das Bestehen eines Arbeitsvertrages dabei nicht gefordert wird, soll doch eine (arbeitsrechtlich) faktische, vom Direktionsrecht bestimmte Tätigkeit des Gehilfen zwingend erforderlich sein. Dies umfasst unter anderem das Recht des Rechtsanwaltes, einseitig insbesondere Inhalt, Ort und Zeit der Arbeitsleitung bestimmen zu können. Dies sei bei externem Personal grundsätzlich nicht der Fall, so dass jede Offenbarung von Geheimnissen an externe Dienstleister (ohne Einwilligung des betroffenen Patienten) gleichsam einen strafbaren Verstoß gegen die anwaltliche Geheimhaltungspflicht darstelle.[74] Nach wohl überwiegender Auffassung fallen damit externe Dritte, die für den Rechtsanwalt selbstständig Aufträge ausführen, wie z.B. ein EDV-Dienstleister, nicht unter den Gehilfenbegriff.[75] Teilweise wird darüber hinaus sogar ein Tätigwerden vor Ort verlangt, was Fernwartungen von Computersystemen gänzlich ausschließen würde.[76] 9

Dass dies nicht richtig sein kann, liegt auf der Hand. Dementsprechend sind in jüngerer Zeit zahlreiche Stimmen gegen ein restriktives Verständnis des Gehilfenbegriffes laut geworden.[77] Obgleich auch sie der Beauftragung externer Dienstleister nicht Tür und Tor öffnen wollen, soll ihr Einsatz dennoch unter Beachtung bestimmter Vorgaben zulässig und damit straffrei sein. So sei maßgeblich darauf abzustellen, ob der primär Schweigepflichtige eine **Steuerungsmacht über** seinen **Dienstleister** in dem Sinne innehabe, dass er die Herrschaft über die zur Verfügung gestellten Informationen behalte, diese Herrschaft tatsächlich ausüben könne und dies auch tue.[78] Für ein derart weites Verständnis des § 203 Abs. 3 Satz 2 StGB („Gehilfe“) spricht zunächst, dass die im Wortlaut der Norm zum Ausdruck kommende unterstützende Funktion des Gehilfen eine organisatorische Einbindung desselben nicht voraussetzt. Vorausgesetzt wird nur die unterstützende Teilnahme der Hilfsperson an der Berufstätigkeit des Schweigepflichtigen, d.h. dem Schweigepflichtigen zugearbeitet wird. Kein Gehilfe ist daher, wer lediglich die äußeren Bedingungen für die fragliche Berufstätigkeit schafft, wie etwa Reinigungskräfte.[79] Oder positiv gesprochen: Gehilfe ist jedenfalls, wer mit der Erledigung der anfallenden anwaltlichen Tätigkeit (mittelbar) beschäf- 10

73 *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 53 m.w.N.; *Knauer/Brose*, in: Spickhoff (Hrsg.), Medizinrecht, 2011, § 205 StGB Rn 23, für den ärztlichen Bereich.

74 *Knauer/Brose*, in: Spickhoff (Hrsg.), Medizinrecht, 2011, § 205 StGB Rn 23; *Jandt/Roßnagel/Wilke*, NZS 2011, 641.

75 FG Rheinland-Pfalz, Urt. v. 25.10.1989 – 1 K 48/87, juris.

76 Differenzierend *Ehmann*, CR 1991, 293.

77 *Hoenike/Hülsdunk*, MMR 2004, 788; *Krekeler/Schonard*, wistra 1998, 137; *Giesen*, NStZ 2012, 122, 125 ff.; *Kort*, NStZ 2011, 193; *Heghmanns/Niehaus*, NStZ 2008, 57.

78 Vgl. *Heghmanns/Niehaus*, NStZ 2008, 57, 61 f.; *Hoenike/Hülsdunk*, MMR 2004, 788; *Kort*, NStZ 2011, 193, 195.

79 *Kühl*, in: Lackner/Kühl (Hrsg.), StGB, 27. Aufl. 2011, § 203 Rn 11b.

tigt ist, wie etwa Buchhalter oder Dolmetscher, soweit diese in den informationellen Schutzbereich des Berufsgeheimnisträgers vertraglich wirksam einbezogen sind.

Auch ein Blick in die Datenschutzgesetzgebung spricht für ein derartiges Verständnis. Nach § 11 BDSG ist der Umgang mit Mandantendaten durch externe Dienstleister dann gestattet, wenn das Verhältnis zwischen dem Rechtsanwalt (verantwortlicher Stelle) und dem externen Dienstleister als **Auftragsdatenverarbeitung** ausgestaltet ist.[80] Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten durch eine andere verantwortliche Stelle im Auftrag erhoben, verarbeitet oder genutzt werden (§ 11 BDSG). Die andere Stelle muss dabei den Weisungen des Auftraggebers unterworfen sein und darf keine eigene Entscheidungsbefugnis darüber besitzen, wie sie mit den Daten umgeht (im Gegensatz zur sogenannten Funktionsübertragung[81]). Der Auftragnehmer ist zudem sorgfältig auszuwählen, der Auftrag muss schriftlich erteilt werden und der Auftraggeber muss den Auftragnehmer umfassend kontrollieren können und seine Kontrollen schriftlich dokumentieren. Vergibt der Rechtsanwalt Aufträge an externe Dienstleister ohne eine solche oder im Rahmen einer unzureichenden Auftragsdatenverarbeitungsvereinbarung, stellt dies gleichzeitig eine Ordnungswidrigkeit dar, die gemäß § 43 Abs. 1 Nr. 2b BDSG mit Bußgeldern in Höhe von bis zu 50.000 EUR sanktioniert werden kann. Datenschutzrechtlich würde es also genügen, die Auslagerung der technischen und organisatorischen Vorgänge der Datenverarbeitung als klassische Form der Datenverarbeitung im Auftrag auf § 11 BDSG zu stützen.[82] **11**

Auch das bürgerliche Recht stellt für den Erfüllungsgehilfen (§ 278 BGB) nicht die Voraussetzung einer organisatorischen Eingliederung im arbeitsrechtlichen Sinne auf. Vielmehr ist allgemein anerkannt, dass es weder eines sozialen Abhängigkeitsverhältnisses noch einer betrieblichen Einbindung bedarf, um von einem Gehilfen im zivilrechtlichen Sinne ausgehen zu können.[83] Auch hier ist allein entscheidend, ob der Gehilfe mit Wissen und Wollen des Geschäftsherren zur Erfüllung einer ihm obliegenden Verbindlichkeit als seine Hilfsperson eingesetzt wird (§ 278 BGB).[84] Im Falle eines Verrichtungsgehilfen (§ 831 BGB) und des ihm gegenüber erforderlichen Weisungsrechts ist es ausreichend, dass der Geschäftsherr die Tätigkeit des Handelnden jederzeit beschränken, untersagen oder nach Zeit und Umfang bestimmen kann.[85] **12**

Die vorbeschriebenen Argumente dürfen allerdings im Ergebnis nicht dazu führen, die Hinzuziehung von externen Hilfspersonen unbeschränkt zuzulassen. Vielmehr ist hier in jedem Einzelfall der Gefahr einer Verletzung des persönlichen Geheimhaltungsinteresses des Mandanten Rechnung zu tragen. Dies erfordert entweder eine konkrete auf den jeweiligen Dienstleister bezogene Einwilligung des betroffenen Mandanten oder eine starke Anbindung des externen Dienstleisters an den Geheimnisträger, durch die sichergestellt wird, dass die Weitergabe an den externen Dienstleister keine Risiken für das Persönlichkeitsrecht des Mandanten schafft, die über das mit der Bekanntgabe an den Anwalt selbst bereits bestehende Risiko signifikant hinausgehen. In diesem Sinne hat es beispielsweise das BVerfG im Falle der Einsichtnahme in Patientenakten einer Universitätsklinik durch einen Landesrechnungshof für ausreichend erachtet, dass die Prüfer ihrerseits zur Verschwiegenheit verpflichtet waren. Daraus folgert die Große Strafrechtskommission des Deutschen Richterbundes in einem für das Bundesministerium der Justiz er- **13**

80 *Kazemi/Leopold,* Datenschutzrecht in der anwaltlichen Beratung, 2011, § 3 Rn 875 f.; *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 52.

81 Vgl. dazu *Menzel*, RDV 2013, 59, 63.

82 Allg. hierzu *Kazemi/Leopold*, Datenschutzrecht in der anwaltlichen Beratung, 2011, § 3 Rn 488 ff.

83 Siehe etwa *Schulze*, in: Schulze u.a. (Hrsg.), BGB, 7. Aufl. 2012, § 278 Rn 5 f.; *Grüneberg*, in: Palandt, BGB, 72. Aufl. 2013, § 278 Rn 7.

84 *Grundmann*, in: Rixecker/Säcker (Hrsg.), MüKo zum BGB, 6. Aufl. 2012, § 278 Rn 42; *Wagner*, in: Rixecker/Säcker (Hrsg.), MüKo zum BGB, 5. Aufl. 2009, § 831 Rn 14 f.

85 BGH, Urt. v. 30.6.1966 – VII ZR 23/65, BGHZ 45, 311, 313; *Sprau*, in: Palandt, BGB, 72. Aufl. 2013, § 831 Rn 5; *Spindler*, in: BeckOK-BGB, § 831 Rn 10 f. m.w.N.; *Wagner*, in: Rixecker/Säcker (Hrsg.), MüKo zum BGB, 5. Aufl. 2009, § 831 Rn 14 m.w.N.

statteten Gutachten betreffend das Outsourcing von IT-Dienstleistungen, dass *„eine solche Zusicherung in vertraglicher Hinsicht bei den IT-Firmen als ausreichend angesehen werden müsste“*.[86]

Dies zugrunde gelegt ist es jedenfalls erforderlich, dass der Rechtsanwalt die für ihn tätigen externen Dienstleister in einer solchen Art und Weise in seine Verschwiegenheitsverpflichtung einbindet, dass die Wahrung der durch § 203 StGB geschützten Mandanteninteressen berücksichtigt wird. Möglich erscheint es z.B., externen Dienstleistern vertraglich eine Verschwiegenheitspflicht aufzuerlegen. Ergänzend empfiehlt sich die Vereinbarung von Vertragsstrafen für den Fall der Zuwiderhandlung, um solche bereits im Vorfeld auszuschließen bzw. die Gefahr solcher zu minimieren. Auch wenn weder die Rechtsprechung noch der Gesetzgeber sich bislang dazu geäußert haben, ob eine solche Vorgehensweise tatsächlich zu einem objektiven Strafbarkeitsausschluss zugunsten des betroffenen Rechtsanwaltes führt, dürfte sich im Falle derartiger Maßnahmen kaum noch vorsätzliches oder grob fahrlässiges Verhalten bejahen lassen. **14**

Der Umgang mit externen Dienstleistern ist unter Berücksichtigung der straf- und datenschutzrechtlichen Vorgaben kritisch zu überprüfen. Dabei gilt: Je konkreter die Ausgestaltung der Geheimnisschutzvorsorge beim Outsourcing ist, desto geringer ist auch das Risiko strafbarer Handlungen. Dort, wo die Übergabe von Mandatsinformationen nicht zwingend notwendig ist sollte gänzlich auf Offenbarungen verzichtet werden. Dort, wo dies nicht oder nur schwer möglich ist, ist der Mandant rechtswirksam zu informieren. Zudem ist zu fordern, dass **15**

- eine uneingeschränkte und jederzeitige Dispositionsbefugnis des Rechtsanwaltes über die seine Mandanten betreffenden Abläufe gegenüber dem externen Dienstleister ("Ob" und "Wie") sichergestellt ist,
- jeder Arbeitsschritt und jedes Arbeitsergebnis des externen Dienstleisters durch diesen ausreichend dokumentiert und unverzüglich an den Rechtsanwalt mitgeteilt wird,
- Mandantendaten auch beim externen Dienstleister durch ausreichende Sicherungsmaßnahmen gegen missbräuchliche Verwendung durch nicht autorisierte Dritte geschützt werden,
- technische wie unmittelbare betriebliche Abläufe so organisiert werden, dass der externe Dienstleister nur streng beschränkte Zugriffsrechte auf die Mandantendaten erhält,
- eine ausreichende Verschwiegenheitsvorsorge durch Schulungen und kontinuierliche Überwachung sowie ausreichende schriftliche Verschwiegenheitserklärungen des externen Dienstleisters gewährleistet wird und
- schließlich ausreichende Sicherheitsvorsorge in räumlicher Hinsicht beim externen Dienstleister gewahrt wird.

86 Große Strafrechtskommission des Deutschen Richterbundes, Auslagerung von Dienstleistungen durch Berufsgeheimnisträger und Datenaustausch zwischen Behörden, 2006, S. 71.

K. Aktenvernichtung und Archivierung

Immer wieder ist in den Tageszeitungen von brisanten Fundstücken in Müllcontainern zu lesen, immer wieder betreffen diese „Fundstücke" auch Rechtsanwaltsakten.[87] Auch wenn nicht davon auszugehen ist, dass die betroffenen Kollegen hier einfach unbedacht Mandanteninformationen im normalen Papiermüll entsorgt haben, wird deutlich, wie sensibel die Öffentlichkeit gerade mit dieser Fragestellung umgeht. Mit Blick auf die dem Rechtsanwalt obliegende besondere Schweigepflicht ist die **anwaltliche Dokumentation vor Einsichtnahme und Zugriff unberechtigter Dritter zu schützen**. Der Rechtsanwalt hat daher sowohl bei konventionellen Handakten als auch beim Einsatz von Datenverarbeitungstechniken sicherzustellen, dass Dritte keinen unbefugten Zugriff (Einblick) in seine Akten erhalten. Handakten dürfen daher in keinem Fall so archiviert oder gar entsorgt werden, dass etwa Mandantendaten Dritten zur Kenntnis gelangen können. 1

Aktenauslagerung

Soweit Akten in den eigenen Kanzleiräumen gelagert werden, sind diese vor dem Zugriff unberechtigter Dritter zu schützen. Dies wird meist ohnehin der Fall sein, befinden sich die Akten doch zum einen in der nicht öffentlich zugänglichen Kanzlei und darüber hinaus auch in hierfür vorgesehenen Aktenschränken. Soweit Akten aus „Platzgründen" in den Keller verbannt und dort gelagert werden, sind auch diese Räumlichkeiten mit einem entsprechenden Zugriffsschutz zu versehen. Hierbei sollte dem Umstand, dass die Anwaltsankten besonders vertrauliche Informationen enthalten, angemessen Rechnung getragen werden. Sicherlich empfiehlt es sich in diesem Zusammenhang auch, nicht nur den Zutritt zum Aktenstandort, sondern auch die jeweiligen Aktenschränke besonders zu sichern, wenn, wie beispielsweise bei einer Lagerung im Keller, eine dauerhafte Kontrolle durch Mitarbeiter der Kanzlei nicht sichergestellt ist. Auch bei Feuer oder Einbruch besteht die Gefahr, dass der Verlust der Mandantenakten zu einem enormen Schaden für die Kanzlei führt. Durch feuersichere Aktenschränke oder Tresorschränke kann Vorsorge getroffen werden, die den Schaden durch Feuer oder Einbruch begrenzt. 2

Was aber, wenn der Platz in der eigenen Kanzlei nicht reicht? Eine platzsparende Alternative bietet da die externe Lagerung des internen Aktenarchivs. Zu diesem Zweck bieten zahlreiche Anbieter die Lagerung der anwaltlichen Handakten in speziell dafür vorgesehene Archivkartonagen an. Der Transport erfolgt anschließend durch verschlossene und gesicherte Fahrzeuge in das externe Archiv. Einige Anbieter ermöglichen es, über ein zugangsgesichertes Webportal nach Legitimation jederzeit den Bestand Ihrer Akten – auch Einzelakten – einzusehen und anzufordern. Hier ist, wie beim Outsourcing generell, besondere Vorsicht geboten und ein etwaiger Auslagerungsanbieter sorgfältig auszusuchen. Dabei muss darauf geachtet werden, dass sowohl die Lagerung und alle damit verbundenen Prozesse absolut datenschutz- und berufsrechtskonform verlaufen. 3

So sollten die Handakten vor der Auslagerung so aufbereitet werden, dass der Aktendeckel keine personenbezogenen Mandantendaten (mehr) aufweist. Hier reicht auch schlicht der Aufdruck der internen Ablagenummer. Die Verpackung der Akten in die Archivkartonagen sollte durch kanzleieigenes Personal, jedenfalls aber unter Überwachung durch selbiges durchgeführt werden. Sobald die einzelnen Akten in die Archivkartonage verbracht wurden, empfiehlt sich die Versiegelung dieser Behältnisse und deren Wiederversiegelung nach Anforderung von Behältnissen oder Akteninhalten. Einige Unternehmen am Markt fordern bei der Einlagerung/Archivhaltung von Daten von Berufsgeheimnisträgern nicht nur die Versiegelung der Aktenbehältnisse, sondern die Versiegelung jeder einzelnen Akte selbst. Der Rechtsanwalt erhält dabei besondere Hinweise zur Versiegelung der Akten, die eine unbefugte Offen- 4

87 Hierzu: SHZ.de, 11.11.2011 – Anwalts-Akten im Altpapier; Bergedorfer Zeitung, 9.11.2011 – Brisante Anwalts-Akten im Papiermüll entsorgt; DIE WELT, 26.2.2008 – Feuerwehr entdeckt Anwaltsakten im Müllcontainer; DIE WELT, 28.12.2001 – Akten im Müll: Staatsanwälte schalten sich ein.

barung von Daten von vornherein verhindern helfen sollen. Jede versiegelte Akte erhält einen Barcode, der die schnelle Auffindbarkeit im Archiv ermöglicht. Durch die zusätzliche Versiegelung der Behältnisse, die Verwendung von Schließbehältern und besondere organisatorische Maßnahmen sollte zudem gewährleistet sein, dass eine unbefugte Offenbarung von Daten, die einem Anwaltsgeheimnis unterliegen, nicht erfolgt. Der Rechtsanwalt sollte zudem schriftlich festlegen, welche Personen welche Akten anfordern dürfen. Neben seiner eigenen Person werden dies regelmäßig sog. berufsmäßig tätige Gehilfen i.S.d. § 203 StGB sein. Die Auslieferung der eingelagerten Akten darf ausschließlich nach Autorisierung durch den angegebenen Personenkreis erfolgen.

Der Rechtsanwalt sollte sich zudem davon überzeugen, dass hinreichende Maßnahmen gegen einen unbefugten Zugriff Dritter auf seine Aktenbestände beim Dienstleister getroffen werden. Diese beinhalten insbesondere den geregelten und streng kontrollierten Zugang zum Gelände und zu den einzelnen Räumen des Dienstleisters, beispielsweise durch eine elektronische Videoüberwachung. 5

Nach § 11 BDSG erfordert der Umgang mit Mandantendaten durch externe Dienstleister zudem den Abschluss einer entsprechenden **Auftragsdatenverarbeitungsvereinbarung**.[88] Der Dienstleister muss hier den Weisungen des Rechtsanwalts als Auftraggeber unterworfen werden und darf keine eigene Entscheidungsbefugnis darüber besitzen, wie er mit den ausgelagerten Daten umgeht (im Gegensatz zur sogenannten Funktionsübertragung). Der Auftragnehmer ist zudem sorgfältig auszuwählen, der Auftrag muss schriftlich erteilt werden und der Auftraggeber muss den Auftragnehmer umfassend kontrollieren können und seine Kontrollen schriftlich dokumentieren. Vergibt der Rechtsanwalt Aufträge an externe Dienstleister ohne eine solche oder im Rahmen einer unzureichenden Auftragsdatenverarbeitungsvereinbarung, stellt dies gleichzeitig eine Ordnungswidrigkeit dar, die gemäß § 43 Abs. 1 Nr. 2b BDSG mit Bußgeldern in Höhe von bis zu 50.000 EUR sanktioniert werden kann. 6

Insgesamt ist hier in jedem Einzelfall der Gefahr einer Verletzung des persönlichen Geheimhaltungsinteresses des Mandanten Rechnung zu tragen. Dies erfordert eine starke Anbindung des externen Dienstleisters an den Geheimnisträger, durch die sichergestellt wird, dass die Weitergabe an den externen Dienstleister keine Risiken für das Persönlichkeitsrecht des Mandanten schafft, die über das mit der Bekanntgabe an den Anwalt selbst bereits bestehende Risiko signifikant hinausgehen. Dies zugrunde gelegt, ist es aus hiesiger Sicht zudem erforderlich, dass der Rechtsanwalt die für ihn tätigen externen Dienstleister in einer solchen Art und Weise in seine Verschwiegenheitsverpflichtung einbindet, dass die Wahrung der durch § 203 StGB geschützten Mandanteninteressen berücksichtigt wird. Den externen Dienstleistern ist daher vertraglich eine Verschwiegenheitspflicht aufzuerlegen. Ergänzend empfiehlt sich die Vereinbarung von Vertragsstrafen für den Fall der Zuwiderhandlung, um solche bereits im Vorfeld auszuschließen bzw. die Gefahr solcher zu minimieren. Auch wenn weder die Rechtsprechung noch der Gesetzgeber sich bislang dazu geäußert haben, ob eine solche Vorgehensweise tatsächlich zu einem objektiven Strafbarkeitsausschluss zugunsten des betroffenen Rechtsanwaltes führt, dürfte sich im Falle derartiger Maßnahmen kaum noch vorsätzliches oder grob fahrlässiges Verhalten bejahen lassen. 7

Der Umgang mit externen Dienstleistern ist unter Berücksichtigung der straf- und datenschutzrechtlichen Vorgaben kritisch zu überprüfen. Dabei gilt: Je konkreter die Ausgestaltung der Geheimnisschutzvorsorge beim Outsourcing ist, desto geringer ist auch das Risiko strafbarer Handlungen. Zudem ist zu fordern, dass 8

- eine uneingeschränkte und jederzeitige Dispositionsbefugnis des Rechtsanwaltes über die seine Mandanten betreffenden Akten gegenüber dem externen Dienstleister ("Ob" und "Wie") sichergestellt ist,
- jeder Arbeitsschritt und jedes Arbeitsergebnis des externen Dienstleisters durch diesen ausreichend dokumentiert und unverzüglich an den Rechtsanwalt mitgeteilt wird,

88 *Kazemi/Leopold,* Datenschutzrecht in der anwaltlichen Beratung, 2011, § 3 Rn 875 f.; *Cierniak*, in: Joecks/Miebach (Hrsg.), MüKo zum StGB, 2. Aufl. 2012, § 203 Rn 52.

- Mandantendaten auch beim externen Dienstleister durch ausreichende Sicherungsmaßnahmen gegen missbräuchliche Verwendung durch nicht autorisierte Dritte geschützt werden,
- technische wie unmittelbare betriebliche Abläufe so organisiert werden, dass der externe Dienstleister nur streng beschränkte Zugriffsrechte auf die Mandantendaten erhält,
- eine ausreichende Verschwiegenheitsvorsorge durch Schulungen und kontinuierliche Überwachung sowie ausreichende schriftliche Verschwiegenheitserklärungen des externen Dienstleisters gewährleistet wird und
- schließlich ausreichende Sicherheitsvorsorge in räumlicher Hinsicht beim externen Dienstleister gewahrt wird.

Aktenvernichtung

Jüngst hat die Novellierung einer überschaubaren DIN-Norm bezüglich der Vernichtung von Dokumenten oder Datenträgern eine Welle von Artikeln das Internet überschwemmen lassen, welche geeignet wären, eine Atmosphäre zwischen Panik und Endzeitstimmung auszulösen. Da wir regelmäßig mit derartiger Schwarzmalerei konfrontiert werden, gilt auch hier: Ruhe bewahren. 9

DIN-Normen sind keine Rechtsnormen. Sie spiegeln lediglich teilweise den Stand der Technik wieder. Was nun die Vernichtung von Papierdokumenten und den allgemeinen Umgang mit personenbezogenen Daten in den Rechtsanwaltskanzleien angeht, so ist es für uns nichts Neues, dass Mandantendaten der höchsten Schutzstufe unterliegen. Aber selbst für die höchste Schutzstufe erachtet die neue DIN 66399 eine Teilchengröße von maximal 160mm2 als ausreichend. Das entspricht einer Partikelgröße von z.B. 4 x 40 mm und damit einem Wert, der ohnehin von den meisten Aktenvernichtern erreicht werden dürfte. Letztlich muss man sich doch auch die Frage stellen, was hier überhaupt erreicht werden soll. Entsprechend dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik gilt es, Informationen so zu vernichten, „dass eine Rekonstruktion der Information mit hoher Wahrscheinlichkeit ausgeschlossen werden kann."[89] Richtig! Es geht also im Grunde genommen darum, dass Mandatsdokumente nicht lesbar oder rekonstruierbar im Hausmüll auftauchen. Ein alter Hut! 10

Möglich ist auch die externe Aktenvernichtung. Um Ihren Bedarf hierfür abschätzen zu können, machen Sie am besten folgende Bestandsaufnahme und vergleichen Sie diese dann mit den Angeboten am Markt: 11

- Fallen in Ihrer Kanzlei permanent Unterlagen zur Vernichtung an? Sollten entweder auf Abruf oder im vereinbarten Turnus abschließbare Behälter dauerhaft zur Verfügung gestellt und ausgetauscht werden?
- Oder ist nur einmaliger bzw. seltener Bedarf (z.B. für die Entsorgung eines Archivs) gegeben? Kann der Anbieter für diese Fälle abschließbare Behälter in unterschiedlichen Größen für mehrere Tage zur Verfügung stellen?
- Wollen Sie nur unregelmäßig kleinere Mengen entsorgen? Dann bieten sich eine Sofortbefüllung und die sofortige Mitnahme vor Ort an.

Bei der Auswahl eines kompetenten Dienstleisters, der die Kanzleiakten datenschutzkonform vernichten soll, ist darauf zu achten, dass die Prozesse und Vernichtungsanlagen hermetisch gesichert sind, die Qualitätssicherung einer ständigen externen Überwachung unterliegt und die Prozess-Sicherheit nach DIN EN ISO 9001 zertifiziert ist. Das bedeutet im Einzelnen, dass 12

- Spezialbehälter mit höchsten Sicherheitsansprüchen bereitgestellt werden,
- die Datenübernahme protokolliert wird,
- der Transport in speziell gesicherten Fahrzeugen erfolgt,

89 BSI-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Kategorie M2.167, http://www.bsi.bund.de, 2014.

- das Betriebsgelände und der Vernichtungsbereich optisch, akustisch und elektronisch gesichert sind,
- das Vernichtungsgut in hermetisch gesicherten Schleusen entladen wird
- und die Vernichtung nach höchsten Sicherheitsstandards über das BDSG hinaus zertifiziert ist.

Bei der Auswahl eines zuverlässigen Dienstleisters kann beispielsweise auf zertifizierte Unternehmen zurückgegriffen werden, wie sie beispielsweise auf den Internetseiten des ULD SH aufgeführt sind.[90] 13

Besonderheiten bei elektronischen Daten

Grundsätzlich sind Daten, die elektronisch übertragen werden, auch elektronisch zu archivieren, zumindest soweit hier eine Aufbewahrungsfrist besteht. Und genau hier kommen wir zu der Frage, wie denn revisionssicher archiviert werden kann. Die Revisionssicherheit impliziert, dass ein Dokument nicht mehr verändert werden kann und grundsätzlich ein Löschen eines archivierten Dokuments nicht mehr möglich ist. Andererseits besteht jedoch hinsichtlich personenbezogener Daten das Erfordernis, dass Daten nach Ablauf der Aufbewahrungsfrist zu löschen sind. Dieses Löschen kann nicht dadurch erreicht werden, dass entsprechende Dokumente lediglich ausgeblendet werden, weil i.d.R. dann ein Administrator des Systems diese immer noch einsehen kann. Jetzt könnte man das grundsätzlich dadurch lösen, dass jährlich eine Archivdatenbank erstellt wird, die nach Ablauf der Aufbewahrungsfrist gelöscht wird. Hier kommen uns jedoch unterschiedlichen Aufbewahrungspflichten in die Quere, da bestimmte Daten nach 6 Jahren gelöscht werden, andere Daten jedoch mindestens 10 Jahre aufbewahrt werden müssen. 14

Archivierung stellt also nicht nur die Kanzlei vor scheinbar unlösbare Probleme. Zunächst einmal ist es schon ein Fortschritt, für jedes Kalenderjahr eine neue Archivdatenbank einzurichten. Wenn dann auch noch deutlich unterschieden werden kann, welche Daten 6 Jahre aufzubewahren sind und welche 10 Jahre gespeichert werden müssen, können in einem Archivsystem jeweils für zwei oder drei Aufbewahrungsfristen Archivdatenbanken angelegt werden, die dann nach Ablauf der Aufbewahrungsfristen vollständig gelöscht werden. Nicht unbedingt einfacher wird es im Bereich der Email-Archivierung. Hier kann in einem Archivsystem ebenfalls eine Datenbank eingerichtet werden, in der Emails archiviert werden. Jetzt besteht einerseits die Pflicht, z.B. Rechnungen, die online eingehen, auch elektronisch zu archivieren, was natürlich zuweilen dazu führt, dass sämtliche eingehenden Mails archiviert werden. Dabei wird aber häufig nicht berücksichtigt, dass Mails privater Natur grundsätzlich nicht von einem solchen Archivierungsrundschlag betroffen sein dürfen. Wie kann man diesen Umstand, bei dem sich Archivierungsgebot und Archivierungsverbot gegenseitig zu behindern scheinen, in den Griff bekommen? Gleich vorab: Es wird nicht ohne Dienstanweisung möglich sein. Entweder Sie untersagen den Mitarbeitern – unter Einhaltung einer Übergangsphase – die private Email-Nutzung vollständig oder Sie weisen die Mitarbeiter an, dass alle archivierungspflichtigen Mails manuell zu archivieren sind. Derartige Lösungen sind i.d.R. mit relativ einfachen Mitteln umsetzbar. So können verschiedene E-Mail-Systeme z.B. um Buttons erweitert werden, durch welche die Funktionen „Senden u. Archivieren“ oder „Mail an Archiv“ ausgelöst werden. Eine entsprechende luxuriöse Lösung wird allerdings nicht in jeder Kanzlei und mit jedem E-Mail-System realisierbar sein. Grundsätzlich ist es jedoch die Beste der möglichen Alternativen, da Mitarbeiter oder E-Mailempfänger wissen, was zu archivieren ist, und die Archivierung einzelner Emails entsprechend auslösen. 15

Bei der Auswahl eines Archivsystems ist Vorsicht geboten. Ausländische, meist US-Amerikanische Zertifizierungen sind aus Sicht des Europäischen Datenschützers mitunter nicht das Papier wert, auf dem sie gedruckt sind. Allerdings neigen zuweilen auch inländische Wirtschaftsprüfer dazu, Testate für Archivsysteme auszustellen. Diese beziehen sich i.d.R. auf die überschaubare Welt der Anforderungen der Wirtschaftsprüfung an ein Archivsystem. Als Datenschutzzertifizierung kann etwas derartiges nicht ernsthaft 16

90 https://www.datenschutzzentrum.de/guetesiegel/register.htm, siehe bspw. auch das Angebot der Hans Soldan GmbH unter: http://www.soldan.de/aktenvernichtung.

angesehen werden. Optimal für eine Kanzlei ist es, wenn die Kanzlei-Software bereits über Archivfunktionalitäten verfügt. Hier sollte jedoch auch kritisch hinterfragt werden, wie Löschfristen eingehalten werden können.

17 Ebenso wie die revisionssichere Archivierung große Relevanz für die Kanzlei besitzt, sollte auch die Vernichtung von Akten und Datenträgern gewissen Vorgaben folgen. Sehr aggressiv werben hier zuweilen Händler oder Hersteller von Aktenvernichtern für ihre Produkte. Dabei verweisen sie häufig auf geänderte Normen, wie die relativ neue DIN 66399 und deren Vorgaben, und wollen uns damit zum Kauf neuer Geräte bewegen. Als Jurist wissen Sie natürlich, dass DIN-Normen keine Rechtsnormen sind. Also überlegen wir uns zunächst, um was es bei der Aktenvernichtung in der Kanzlei handelt. Es geht darum, dass keine unberechtigten Dritten sich Zugriff zu personenbezogenen Daten und sonstigen Informationen beschaffen. Entsprechend dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gilt es, Dokumente und Unterlagen so zu vernichten, „dass eine Rekonstruktion der Information mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.“.[91] Es soll mit anderen Worten also ausgeschlossen werden, dass auf diesem Weg Information an unberechtigte Dritte gelangen. Ob nun dabei die Schnipselgröße 12, 14, 16 oder 18 mm2 beträgt, ist im Grunde genommen nicht relevant. Nur eines ist sicher, dass nämlich eine entsprechende Aktenvernichtung in angemessener Weise erfolgen muss. Das kann über separate Sammlung der zu vernichtenden Unterlagen erfolgen oder über eine Vernichtung jeder einzelnen Akte oder jedes einzelnen Schriftstücks.

18 Bei der Vernichtung von Datenträgern, wird es schon etwas komplizierter. Während viele Papiershredder auch Disketten, DVD-, CD- und Bluray-Datenträger ausreichend gut zerstören, ist die Vernichtung von Festplatten ungleich schwieriger. Längst ist bekannt, dass Feuer oder magnetische Felder unter Umständen kein ausreichendes Mittel sind, Festplatten zu löschen oder zu zerstören. Soweit Daten auf einer Festplatte lediglich gelöscht werden sollen und diese weiterhin verwendbar bleiben soll, kann dies mit einer speziellen Software geschehen, die bis zu 36 mal den Datenträger oder gelöschte Dateien mit Datenmüll überschreibt. Keinesfalls sollten hierbei weniger als sieben Überschreibungen gewählt werden. Bei einfacher Löschung oder Formatierung eines Datenträgers können die Daten unter Umständen in einem Zeitraum von wenigen Minuten bis zu einigen Stunden wiederhergestellt werden. Die Vernichtung eines Datenträgers überlässt man derweil günstigerweise einem dafür zertifizierten und vertrauenswürdigen Fachunternehmen. Solche Unternehmen kommen je nach Umfang des zu vernichtenden Materials vor Ort, so dass man sich gleich von der ordnungsgemäßen Zerstörung der Datenträger überzeugen kann. Grundsätzlich gilt auch hier, dass die Datenträger so zu vernichten sind, dass die Rekonstruktion von Daten mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Einige tatsächlich schon beobachtete Verfahren, wie z.B. das Traktieren einer Festplatte mit einem Spalthammer, das Durchtreiben eines Baustahls durch den Datenträger und andere zum Teil brachiale Zerstörungsformen, die eher in Krisengebieten zu vermuten wären, sind zwar grundsätzlich nicht BSI-konform, verfehlen jedoch auch nicht ihren Zweck. Gelöschte Daten sind i.d.R. einfacher wiederherzustellen, als Papierschnipsel zusammengefügt werden können. Daher ist es unbedingt erforderlich, dass ausgesonderte Datenträger so zerstört werden, dass keine Daten davon wieder hergestellt werden können. Es wird insbesondere zu bedenken gegeben, dass Personen mitunter auf Flohmärkten und bei Entsorgungsunternehmen gezielt nach Festplatten suchen, um darauf gelöschte Daten wiederherzustellen und so illegal an Informationen wie Bankdaten, Kreditkartennummern oder andere sensible personenbezogene Daten zu gelangen.

91 BSI-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Kategorie M2.167, http://www.bsi.bund.de, 2014.

Regel 1: Alle elektronisch übermittelten Daten, die archiviert werden müssen, sind auch elektronisch zu archivieren. 19

Regel 2: Grundsätzlich dürfen keine Mails privater Natur gemeinsam mit den Kanzleikorrespondenzen (automatisch) archiviert werden.

Regel 3: Vertrauen Sie hinsichtlich des Datenschutzes nicht auf außereuropäische Zertifizierungen und Testate oder auf entsprechende Dokumente, die von anderen Berufsgruppen als Datenschützern ausgestellt wurden.

Regel 4: Achten Sie bei der Archivierung darauf, ob Sie die Löschfristen einhalten können und ob Daten tatsächlich gelöscht oder nur ausgeblendet werden.

Regel 5: Eine Vernichtung von Unterlagen hat so zu erfolgen, dass eine Rekonstruktion der Information mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.[92]

Regel 6: Ausgesonderte Datenträger sollten vollständig zerstört werden. Eine sichere Löschung von Daten soll durch spezielle Software und mehrfache Überschreibung der Datenblöcke erfolgen.

92 BSI-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Kategorie M2.167, http://www.bsi.bund.de, 2014.

L. Datenschutz im Internet – Was ist auf der Kanzleiseite zu beachten

Allgemeine Pflichten

§ 13 TMG verpflichtet den Diensteanbieter eines Telemediendienstes generell dazu, den Nutzer zu Beginn des jeweiligen Nutzungsvorganges über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereiches der EG-Datenschutzrichtlinie in allgemein verständlicher Form zu unterrichten. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens hierüber ebenfalls zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein. 1

Die vorgenannte Verpflichtung trifft grundsätzlich jeden Anbieter eines Telemediendienstes, gleich ob er diesen kostenpflichtig oder kostenlos anbietet. Dementsprechend ist immer dann, wenn es zu einer Verarbeitung, Erhebung und/oder Nutzung personenbezogener Daten durch den Diensteanbieter kommt bzw. kommen kann, eine Unterrichtung im Sinne des § 13 Abs. 1 TMG zwingend erforderlich. In der Praxis hat sich hierfür die Formulierung einer so genannten Datenschutzerklärung/oder auch Privacy Policy etabliert. Diese ist, da die Unterrichtung und ihr Inhalt für den Nutzer jederzeit abrufbar sein muss, im Rahmen eines permanenten Links im Angebot des jeweiligen Telemediendienstes vorzuhalten.[93] 2

Da die Unterrichtung nach dem Gesetzeswortlaut „zu Beginn des Nutzungsvorganges" zu erfolgen hat, ist eine vorherige Unterrichtung des Nutzers – beispielsweise in der Form, dass dem eigentlichen Telemediendienst eine „Unterrichtungsseite" vorgeschaltet wird – nicht notwendig. Es reicht vielmehr aus, wenn der Nutzer spätestens mit der Inanspruchnahme des jeweiligen Telemediendienstes von der Unterrichtung Kenntnis nehmen kann. Dies erfordert, dass der entsprechende Datenschutzhinweis klar, verständlich und für jeden Nutzer sichtbar auf der Startseite des jeweiligen Telemediendienstes angebracht ist. Nach allgemeiner Meinung reicht es dabei aus, dass der Nutzer die Möglichkeit hat, die Datenschutzerklärung selbsttätig aufzurufen; eine Verpflichtung dazu, den Nutzer aktiv auf die datenschutzrechtlichen Problemstellungen bei Nutzung des jeweiligen Telemediendienstes hinzuweisen, besteht nicht.[94] Für dieses Ergebnis spricht im Übrigen auch, dass der Gesetzestext in § 13 Abs. 1 Satz 3 TMG ausdrücklich davon spricht, dass der Nutzer den Inhalt der Unterrichtung „jederzeit" abrufen können muss. Eine aktive Unterrichtungspflicht, beispielsweise in der Form, wie sie im Fernabsatzgeschäft hinsichtlich des für Verbraucher bestehenden Widerrufsrechtes zu erfolgen hat, fordert § 13 Abs. 1 TMG ausdrücklich nicht. 3

In § 13 Abs. 1 Satz 2 TMG findet sich zudem eine Spezialregelung für automatisierte Verfahren, bei denen eine spätere Identifizierung des Nutzers möglich ist und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet wird. In diesem Fall ist der Nutzer ebenfalls über das Verfahren zu unterrichten. Die Regelung des § 13 Abs. 1 Satz 2 TMG ist vornehmlich auf Cookies zugeschnitten.[95] Durch die Unterrichtungspflicht soll der Gefahr vorgebeugt werden, dass durch die spätere Möglichkeit der Zuordnung der Daten ohne Wissen des Nutzers Profile gebildet werden können. 4

Die Datenschutzerklärung nach § 13 Abs. 1 TMG hat vor diesem Hintergrund auch dann besondere Bedeutung, wenn der Webseitenbetreiber Webtrackingtools, wie Google Analytics, auf seiner Internetseite einsetzt. Auch hier ist der Nutzer auf diesen Umstand konkret hinzuweisen. 5

93 *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 13 TMG Rn 5, *von Lewinski*, DuD 2002, 395, 398; *Hillenbrand-Beck/Greß*, DuD 2001, 389, 393.

94 Vgl. nur *Moos*, in: Taeger/Gabel (Hrsg.), BDSG 2010, § 13 TMG Rn 9; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 13 TMG Rn 2, 5.

95 *Scholz*, Datenschutz beim Internet-Einkauf, 2002, S. 315; *Schaar*, Datenschutz im Internet, 2002, Rn 713; *Selk*, Datenschutz im Internet, 2003, S. 144; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 13 TMG Rn 4.

Facebook-Like-Button

Immer mehr Kanzleien suchen den Weg in das Web 2.0. Insbesondere die Teilnahme an Netzwerken wie Facebook gewinnt dabei aus anwaltlicher Sicht zunehmend an Bedeutung. Facebook bietet Unternehmen den so genannten „Like-Button", den Webseitenbetreiber nutzen können, um Facebook-Usern eine Möglichkeit zu geben, die auf einer bestimmten Website angebotenen Webinhalte mit einem Klick in ihr Facebook-Profil zu verlinken. Der Facebook-Like-Button kann von Diensteanbietern auf ihrer eigenen Website integriert werden, um Facebook-Nutzern, die bereits bei diesem Dienst registriert sind, mit einem Klick auf diesen Button automatisch in ihrem Facebook-Profil eine Notiz zu hinterlassen, die darüber Aufschluss gibt, dass dem bestimmten Facebook-User die verlinkten Inhalte des Telemediendienstes gefallen. 6

Der einzubindende Facebook-Like-Button ist jedoch kein statistisches Bild, sondern er „kommuniziert" laufend mit seinem Hersteller, der Firma Facebook. Diese ist – nicht erst nach dem Kinostart des Filmes „The Social Network", der ein Portrait von Facebook-Erfinder *Zuckerberg* darstellt – datenschutzrechtlich in der jüngsten Vergangenheit oftmals unter Beschuss geraten. Auch bei der Verwendung von Like-Buttons ist besondere Vorsicht geboten.[96] 7

Die datenschutzrechtliche Kritik kam im Zusammenhang mit der Teilnahme der Stadt Hamburg[97] am Facebook-Like-Button-Programm auf. Die Stadt hatte sich im Sommer 2010 dazu entschieden, den Like-Button in ihr Portal zu integrieren. Diese Funktion – so der Webmaster der Freien und Hansestadt Hamburg, *Konjovic*,[98] „passte ideal in die Strategie von Hamburg.de". Die Stadt wollte „einerseits den Dialog mit ihren Besucherinnen und Besuchern gerne möglichst intensiv und überall wo sinnvoll führen", aber auch „die Vernetzung der User untereinander fördern". Der Facebook-Like-Button wurde als „eine einfache Möglichkeit, sein Gefallen an einem Web-Inhalt kundzutun" angesehen; insbesondere käme kaum ein Blog ohne die neue Funktion von Facebook aus, der Like-Button sei fast überall sehr schnell integriert worden und werde von Usern eifrig genutzt". 8

Circa zwei Wochen nach der Integration des Facebook-Like-Buttons entschied sich die Stadt Hamburg dennoch dazu, die Funktion wieder zu entfernen. Anlass waren umfassende Presseberichterstattungen darüber, dass der Facebook-Like-Button nicht nur Daten von Usern sammelt, die ihn anklicken, sondern von jedem User, der sich auf einem Internetportal bewegt, welches einen solchen Like-Button integriert hat.[99]

Freilich, diese Behauptung konnte nicht „bewiesen" werden, da niemand so recht weiß, was Facebook mit den per Like-Button gesammelten Daten überhaupt macht. Bedingt durch die Art und Weise der Realisierung dieses Buttons könnten auch Daten von nicht bei Facebook angemeldeten Usern gesammelt werden. Jeder Schritt, den ein User auf einer Internetseite vollzieht, die mit dem Like-Button ausgestattet ist, könnte so durch Facebook nachvollzogen und kontrolliert werden. Die Erstellung eines umfassenden Nutzerprofiles wäre so ein Leichtes. Facebook weist darauf hin, dass „eine Verarbeitung" personenbezogener Daten nicht stattfinde und die „gesammelten Daten" (von denen niemand weiß, was sie überhaupt beinhalten) nach „drei Monaten gelöscht würden". 9

Auch wenn, das OVG Schleswig[100] zwischenzeitlich entschieden hat, dass der Betreiber einer Facebook-Fanpage für die allein von Facebook vorgenommene Verarbeitung personenbezogener Daten von Besuchern der Fanpage datenschutzrechtlich nicht verantwortlich ist, da der Fanpage-Betreiber keinen Einfluss auf die technische und rechtliche Ausgestaltung der Datenverarbeitung durch Facebook habe, sei 10

96 Vgl. hierzu die ausführliche und informative Darstellung bei *Ernst*, NJOZ 2010, 1917.

97 Unter: http://www.hamburg.de.

98 Abrufbar unter: http://intern.hamburg.de/2010/06/22/wieso-wir-den-facebook-like-button-wieder-entfernten-./.

99 Vgl. http://www.iitr.de/datenschutz-und-der-facebook-like-button-was-webseiten-betreiber-beachten-muessen.html; http://www.zdnet.de/41534120/hamburg-de-entfernt-facebooks-like-button-aus-datenschutzgruenden/.

100 Urt. v. 4.9.2014 – 4 LB 20/13.

dem Rechtsanwalt, der die Integration eines Facebook-Like-Buttons auf seiner Internetseite plant, trotzdem empfohlen, seine Datenschutzerklärung nach § 13 Abs. 1 TMG um eine entsprechende Information mit Blick auf den Facebook-Like-Button zu ergänzen.

Google Analytics

Auch die Verwendung von Google Analytics ist datenschutzrechtlich höchst umstritten. Google Analytics ist ein kostenloser Dienst, der der Analyse von Zugriffen auf Webseiten dient. Neben den von anderen Analysesoftwares bekannten Funktionen, wie Herkunft der Besucher, Verweildauer und Suchbegriffe in Suchmaschinen, bietet Google Analytics eine Integration in die Benutzeroberfläche von Google AdWords und erlaubt so eine bessere Erfolgskontrolle von AdWords-Kampagnen. Google kann mit diesem Analysewerkzeug ein umfassendes Benutzerprofil vom Besucher einer Website anlegen. Wird ein anmeldepflichtiger Google-Dienst von dem Besucher verwendet, so kann dieses Benutzerprofil auch bestimmten Personen zugeordnet werden. **11**

Auch hier sind die Bestimmungen des TMG zu beachten. Nach § 12 Abs. 1 TMG gilt eine Verarbeitung von personenbezogenen Daten nur dann als zulässig, wenn der Benutzer vorher zugestimmt hat oder eine gesetzliche Ermächtigung vorliegt. Durch den Einsatz des Werkzeuges „Google Analytics" wird mitunter die vollständige IP-Adresse des Seitenbesuchers an einen Dritten (Google) übermittelt, was dem Datenschutz des jeweiligen Betroffenen entgegenstehen kann. Sofern der Benutzer nicht vorher eingewilligt hat, ergeben sich dadurch datenschutzrechtliche Probleme. **12**

Bisher ist juristisch nicht geklärt, welche Rechtsgrundlage die Übertragung der Daten an Google Analytics erlauben soll. Insbesondere § 15 Abs. 1 TMG wird hier als nicht ausreichend angesehen. **13**

Der Landesbeauftragte für den Datenschutz in Schleswig-Holstein[101] geht davon aus, dass „derzeit die Nutzung des kostenlosen Google Analytics Services durch Webseitenanbieter unzulässig ist". Solange Google die Konfiguration von Google Analytics nicht so ändert, dass die Betroffenen ihr Recht auf Widerspruch, Information und Auskunft zur Löschung der Daten wirksam wahrnehmen können, sei der Einsatz dieses Dienstes durch Webseitenbetreiber unzulässig und rechtswidrig. **14**

Google hat mittlerweile hierauf reagiert und bietet den Webseitenbetreibern die Möglichkeit an, den Google Analytics Code um die Funktion „_anonymizelp()" zu erweitern. Mit Anbringung dieses Zusatz-Codes werden vor jeder weiteren Verarbeitung der anfragenden IP-Adresse die letzten 8 Bit derselben gelöscht. Damit ist eine Identifizierung des Webseitenbesuchers ausgeschlossen. Eine grobe – datenschutzrechtlich zulässige – Lokalisierung bleibt hingegen möglich. **15**

Sind die Daten, insbesondere die IP-Adresse, die Google Analytics erhebt, damit nicht mehr personenbezogen, dürfte die Verwendung des Google Analytic Tools ebenso wie die Verwendung anderer – ebenso ausgestatteter – Webtracking-Tools datenschutzrechtlich als zulässig eingestuft werden. In allen anderen Fällen, also für den Fall, dass nach wie vor auch IP-Adressen an den Betreiber der Webtracking-Tools übermittelt werden, stellt sich die Frage der datenschutzrechtlichen Zulässigkeit. **16**

Da die Verwendung von Webtracking-Tools nicht nötig ist, um eine Website zu betreiben, scheidet § 15 Abs. 1 TMG als Rechtfertigungsgrundlage aus. Es bleibt dann noch § 15 Abs. 3 TMG, der dem Diensteanbieter gestattet, zu Zwecken der Werbung, Marktforschung und bedarfsgerechten Gestaltung seines Webauftrittes pseudonyme Nutzerprofile zu erstellen. Der Diensteanbieter muss den Nutzer nach § 15 Abs. 3 S. 2, 13 Abs. 1 TMG über diesen Vorgang unterrichten und ihn über sein Widerspruchsrecht aufklären (so genanntes Opt-Out-Prinzip). Soweit er die Analysen jedoch nicht pseudonymisiert vornimmt, greift § 15 Abs. 3 TMG als Rechtfertigungsgrund nicht. Auch dann, wenn die Daten – beispielsweise wie bei Goo- **17**

101 31. Tätigkeitsbericht vom 31.3.2009, abrufbar unter: http://www.fh-giessen-friedberg.de/zaftda/tb-bundeslaender/cat_view/25-tb-bundeslaender/19-schleswig-holstein-/63-landesdatenschutzbeauftragter.

gle Analytics – nicht durch den Webseitenbetreiber selbst, sondern durch einen Dritten (hier Google) ausgewertet werden, ist die Anwendung des § 15 Abs. 3 TMG ausgeschlossen. Denn diese Norm regelt nur das Verhältnis zwischen Diensteanbieter und Nutzer; sie sieht gerade nicht vor, dass ein Dritter die Datenerhebung vornimmt, sodass eine Rechtfertigung aus § 15 Abs. 3 TMG jedenfalls immer dann ausscheidet, sobald Dritte in die Datenverarbeitung eingeschaltet werden und diese personenbezogene Daten erhalten.

Es wird dementsprechend vertreten, dass die Datenübermittlung an Dritte in diesem Fall nur zulässig ist, soweit sie als Auftragsdatenverarbeitung im Sinne von § 11 BDSG ausgestaltet ist.[102] Die Ausgestaltung im Sinne einer Auftragsdatenverarbeitung nach § 11 BDSG wird in aller Regel daran scheitern, dass der Diensteanbieter und der „Statistikauswerter" keine schriftliche Vereinbarung über die Auftragsdatenverarbeitung geschlossen haben, die jedoch konstitutiv vorliegen muss. Auch wird es regelmäßig an Weisungs- und Kontrollmöglichkeiten des Auftraggebers (Diensteanbieters) gegenüber dem Auftragnehmer (Statistikauswerter) fehlen. Die Auftragsdatenverarbeitung zeichnet sich zudem dadurch aus, dass der Auftragnehmer die ihm zum Zwecke der Verarbeitung überlassenen Daten nicht im eigenen Interesse nutzt. Bezogen auf Google Analytics wird die Annahme einer rechtswirksamen Auftragsdatenverarbeitung spätestens an dieser Stelle scheitern, denn in Ziff. 8.2. der der Nutzung von Google Analytics zugrunde liegenden AGB[103] heißt es, dass sich der Nutzer damit einverstanden erklärt, „dass Google oder seine verbundenen Unternehmen Informationen über ihre Benutzung des Services (einschließlich und ohne Einschränkung auch von Kundendaten) speichert und für die Zwecke der Bereitstellung von Webanalyse- und Trackingdiensten zu nutzen", womit das eigene Interesse der Firma Google an den ihr übermittelten Nutzerdaten offensichtlich wird. **18**

Für den Fall, dass eine anonymisierte Übertragung der Nutzerdaten nicht erfolgt, wird die Nutzung des Webtrackingtools Google Analytics und anderer ähnlich aufgebauter Webstatistikauswertungsprogramme mit Sicherheit als datenschutzrechtlich unwirksam einzustufen sein. **19**

Muster: Datenschutzerklärung nach § 13 TMG **20**

Die Kanzlei XYZ (nachfolgend: Sozietät) nimmt den Schutz Ihrer persönlichen Daten sehr ernst und hält sich strikt an die Regeln des Bundesdatenschutzgesetzes. Die nachfolgende Erklärung gibt Ihnen einen Überblick darüber, wie die Sozietät diesen Schutz gewährleistet und welche Art von Daten zu welchem Zweck erhoben werden.

Die Sozietät erhebt als Betreiber der Services auf der Domäne von rechtswanwalt-mustermann.de personenbezogene Daten, sobald Sie über diese Domains eine Anfrage an die Sozietät stellen und/oder den von der Sozietät angebotenen Newsletter abonnieren.

Die Sozietät erhebt und speichert in diesem Zusammenhang:

- Ihren Namen
- Ihre Anschrift
- Ihre EMail-Adresse
- Telefon- und Faxnummer

Mit der Registrierung für den Newsletter der Sozietät und/oder der Stellung einer Anfrage über das unter http://www.rechtswanwalt-mustermann.de bereit gestellte Kontaktformular willigen Sie in die Speicherung der angegebenen Daten und ihre Verarbeitung durch die Sozietät ein.

102 So bspw. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Pressemitteilung vom 9.7.2008, abrufbar unter: https://www.datenschutzzentrum.de/presse/20080709-tracking-datenschutzkonform.html; *Gabriel/Cornels*, MMR 2008, XIV, XV.

103 Abrufbar unter: http://www.google.com/intl/de_ALL/analytics/tos.html.

Nach § 34 des BDSG haben Sie jederzeit das Recht auf Auskunft betreffend der über Sie gespeicherten Daten, deren Herkunft und Empfänger. Ebenfalls können Sie sich laut § 34 BDSG jederzeit Auskunft über den Zweck der Datenerhebung einholen. Auskunft über die gespeicherten Daten gibt die Sozietät unter den unten angegebenen Kontaktdaten.

Auf diesen Internetseiten werden Plugins des sozialen Netzwerkes facebook.com verwendet, das von der Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA betrieben wird ("Facebook"). Wenn Sie mit einen solchen Plugin versehene Internetseiten unserer Internetpräsenz aufrufen, wird eine Verbindung zu den Facebook-Servern hergestellt und dabei das Plugin durch Mitteilung an Ihren Browser auf der Internetseite dargestellt. Hierdurch wird an den Facebook-Server übermittelt, welche unserer Internetseiten Sie besucht haben. Sind Sie dabei als Mitglied bei Facebook eingeloggt, ordnet Facebook diese Information Ihrem persönlichen Facebook-Benutzerkonto zu. Bei der Nutzung der Plugin-Funktionen (z.B. Anklicken des „Gefällt mir"-Buttons, Abgabe eines Kommentars) werden auch diese Informationen Ihrem Facebook-Konto zugeordnet, was Sie nur durch Ausloggen vor Nutzung des Plugins verhindern können. Nähere Informationen zur Erhebung und Nutzung der Daten durch Facebook, über Ihre diesbezüglichen Rechte Möglichkeiten zum Schutz Ihrer Privatsphäre finden Sie in den Datenschutzhinweisen von Facebook.

Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc. („Google"). Google Analytics verwendet sog. „Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse der Benutzung der Website durch Sie ermöglichen. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website (einschließlich Ihrer IP-Adresse) wird an einen Server von Google in den USA übertragen und dort gespeichert. Google wird diese Informationen benutzen, um Ihre Nutzung der Website auszuwerten, um Reports über die Websiteaktivitäten für die Websitebetreiber zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen zu erbringen. Auch wird Google diese Informationen gegebenenfalls an Dritte übertragen, sofern dies gesetzlich vorgeschrieben oder soweit Dritte diese Daten im Auftrag von Google verarbeiten. Google wird in keinem Fall Ihre IP-Adresse mit anderen Daten von Google in Verbindung bringen. Sie können die Installation der Cookies durch eine entsprechende Einstellung Ihrer Browser Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website vollumfänglich nutzen können. Durch die Nutzung dieser Website erklären Sie sich mit der Bearbeitung der über Sie erhobenen Daten durch Google in der zuvor beschriebenen Art und Weise und zu dem zuvor benannten Zweck einverstanden. Sie können dieser Form der Datenerhebung und -speicherung jederzeit mit Wirkung für die Zukunft widersprechen [mit http://tools.google.com/dlpage/gaoptout?hl=de verlinken] werden. Angesichts der Diskussion um den Einsatz von Analysetools mit vollständigen IP-Adressen möchten wir darauf hinweisen, dass diese Website Google Analytics mit der Erweiterung „_anonymizeIp()" verwendet und daher IP-Adressen nur gekürzt weiterverarbeitet werden, um den Personenbezug von IP-Adressen auszuschließen.

M. Beschäftigtendatenschutz – Grundlagen und ausgewählte Probleme

Selbst diejenigen, die das Datenschutzrecht des BDSG im Rahmen der mandatsbezogenen Tätigkeit des Rechtsanwaltes für unanwendbar erachten, bestreiten seine Anwendbarkeit in Bezug auf die Mitarbeiter der Kanzlei nicht. Daher sollen an diese Stelle einige ausgewählte Problemkreise des sog. Beschäftigtendatenschutzes näher beleuchtet werden. Dass diese nicht rein theoretischer Natur sind, zeigt eine jüngere Entscheidung des Hessischen Landesarbeitsgerichts[104], die zur „Einstimmung" vorangestellt werden soll: 1

Muss eine Kanzlei die persönlichen Daten eines ausgeschiedenen Arbeitnehmers von ihrer Homepage löschen?

Das Landesarbeitsgericht Hessen sagt: Ja! 2

Die Verfügungsbeklagten betreiben eine Steuerberater- und Rechtsanwaltssozietät als GbR. Die Verfügungsklägerin war zunächst als Rechtsanwältin in der Kanzlei angestellt. Das Arbeitsverhältnis endete jedoch durch arbeitgeberseitige Kündigung in der Probezeit. Während dieser Zeit war die Verfügungsklägerin auf der Homepage der Kanzlei aufgeführt. Daneben befand sich im News-Blog der Internetseite der Verfügungsbeklagten ein Hinweis darauf, dass die Verfügungsklägerin in das Anwaltsteam im Bereich Handels- und Gesellschaftsrecht aufgenommen worden sei. Hierin waren auch Angaben zum Profil der Klägerin und ein Foto von dieser enthalten. Diese Veröffentlichungen erfolgten zunächst mit Wissen und Wollen der Verfügungsklägerin. Sie hatte darüber hinaus die Angaben zu ihrem Profil selbst ausgearbeitet. Nach Ausscheiden aus der Kanzlei forderte die Verfügungsklägerin die Verfügungsbeklagten zur Löschung dieses Beitrages auf, was die Verfügungsbeklagten ablehnten. Sie waren lediglich dazu bereit, eine Ergänzung dahingehend vorzunehmen, dass das Arbeitsverhältnis während der Probezeit beendet worden sei.

Die Verfügungsklägerin begehrte im Wege einer einstweiligen Verfügung die Unterlassung der Veröffentlichung. Das Arbeitsgericht Frankfurt[105] hatte der Verfügungsklägerin zunächst Recht gegeben, die Verfügungsbeklagten haben Berufung zum Landesarbeitsgericht eingelegt. 3

Das Landesarbeitsgericht Hessen hat der Verfügungsklägerin, wie auch das Arbeitsgericht Frankfurt zuvor Recht gegeben. 4

Kernpunkt war, dass das Gericht zu Recht darauf hinwies, dass es sich bei der Meldung keinesfalls nur um eine bloße Eintrittsmitteilung gehandelt hatte. Vielmehr sei die Mitteilung durch das Profil der Verfügungsklägerin geprägt gewesen. Dieses habe werbenden Charakter. Aus der Verbindung des Bildes der Verfügungsklägerin und Formulierungen wie: „langjährige Berufserfahrung in Deutschland und den USA, von der unsere Mandanten profitieren werden", die die persönliche Qualifikation der Verfügungsklägerin hervorheben, ergebe sich, dass konkret mit dem Bild der Verfügungsklägerin geworben werde. 5

Die Verfügungsklägerin habe ein Recht auf Löschung aus ihrem allgemeinen Persönlichkeitsrecht. Es entstehe zudem der unzutreffende Eindruck, die Verfügungsklägerin sei weiterhin bei den Verfügungsbeklagten tätig. Dies führe auch zu Wettbewerbsnachteilen der Verfügungsklägerin, da bspw. bei Internetrecherche auch auf die Kanzlei der Verfügungsbeklagten verwiesen würde. Nach Beendigung des Arbeitsverhältnisses bestehe für die Verfügungsbeklagten kein berechtigtes Interesse an der Veröffentlichung der Daten der Verfügungsklägerin. 6

Die Entscheidung des Landesarbeitsgerichts Hessen ist zutreffend. Das Gericht hat klargestellt, dass solche Daten auch als Werbung des Unternehmens selbst zu klassifizieren sind. Nach Ausscheiden des An- 7

104 Hessisches LAG, Urt. v. 24.01.2012 – 19 SaGa 1480/11.
105 ArbG Frankfurt, Urt. v. 05.10.2011 – 13 Ga 160/11.

gestellten besteht ein berechtigtes Interesse an dieser Werbung indes nicht mehr, das Persönlichkeitsrecht des Ausgeschiedenen überwiegt hier zu Recht. Zu beachten ist, dass dies umso mehr für Angaben gelten muss, die nicht lediglich in Form eines Blogs bzw. Newsletters entäußert worden sind. Für ausgeschiedenen Mitarbeiter bedeutet dies, dass ihre Position gegenüber ihren ehemaligen Arbeitgebern gestärkt wurde. Sollte ein Löschungswunsch bestehen, kann ein solcher insoweit gut begründet und dezidiert dargelegt werden.

So schnell wird Datenschutzrecht präsent. Beginnen wir aber von vorn.

Was ist Beschäftigtendatenschutz?

Der Schutz personenbezogener Daten im Arbeitsverhältnis ist durch eine unübersichtliche Vielzahl verschiedener Gesetzgebung gekennzeichnet. Der Schutz personenbezogener Daten innerhalb eines Beschäftigungsverhältnisses kann – im Einzelfall – sowohl nach den Regelungen des Telemediengesetzes (TMG), des Telekommunikationsgesetzes (TKG), allgemeiner arbeitsrechtlicher Bestimmungen (BetrVG) oder anhand der allgemeinen datenschutzrechtlichen Bestimmungen des BDSG (hier insbesondere §§ 4, 4a, 28, 32) sowie der Datenschutzgesetze der Länder zu beurteilen sein. 8

So bestehen beispielsweise keine expliziten arbeitsrechtlichen Bestimmungen für den Umgang mit betrieblichen Information- und Kommunikationsanlagen wie dem Internet oder E-Mail-Systemen. Weder das TMG noch das TKG enthalten spezielle arbeitsrechtliche Bestimmungen, die die Nutzung und Kontrolle derartiger Informationsmedien im Arbeitsverhältnis regeln. 9

Der Bundesgesetzgeber hat – nachdem bereits seit langem von verschiedenen Stellen die Schaffung eines bereichsspezifischen Arbeitnehmerdatenschutzgesetzes gefordert wurde[106] – auch bedingt durch die Vielzahl verschiedener Datenschutzskandale bei Großunternehmen im Jahre 2009[107] mit § 32 BDSG erstmals eine spezifische Regelung zum Arbeitnehmerdatenschutz geschaffen. Gleichzeitig wurde eine Arbeitsgruppe eingerichtet, die den Entwurf für ein umfassendes Arbeitnehmerdatenschutzgesetz erarbeiten sollte.[108] 10

§ 32 BDSG ist aufgrund von § 27 BDSG vornehmlich im Rahmen von Beschäftigungsverhältnissen bei nicht-öffentlichen Stellen im Sinne des § 2 Abs. 4 BDSG zu beachten. Aufgrund der Regelung in § 12 Abs. 4 BDSG (hier heißt es: „Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Abs. 2, die §§ 32–35 anstelle der §§ 13–16 und 19–20“) wird die Regelung des § 32 BDSG jedoch auch für die Beschäftigtendatenverarbeitung durch öffentliche Stellen des Bundes (§ 2 Abs. 1 BDSG) zunehmend an Bedeutung gewinnen. 11

§ 32 BDSG regelt – dem folgt die Darstellung in diesem Werk – die Erhebung, Verarbeitung und Nutzung von Daten von Beschäftigten durch alle Phasen der Datenverwendung, d.h. vom Bewerbungsverfahren bis über das Ende des Beschäftigungsverhältnisses hinaus. Die Vorschrift definiert den Kreis der Beschäftigten, auf den die dem neuen § 32 BDSG enthaltenen konkretisierenden Regelungen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses Anwendung findet, legal. Die Regelung stellt entsprechend dem Schutzzwecke des § 32 BDSG klar, dass zum Begriff des Beschäftigten nicht nur Arbeitnehmer im engeren Sinne gehören, sondern auch die zur Berufsbildung beschäftigten Personen, denen wie z.B. den Rehabilitanden eine arbeitnehmerähnliche Stellung zukommt. 12

106 *Tinnefeld/Viethen*, NZA 2000, 977; *Zilkens*, DuD 2005, 253; s.a. BT-Drucks 15/4597, S. 4; BT-Drucks 16/4882, S. 2.
107 BT-Drucks 16/13657, S. 20.
108 BT-Drucks 16/13657, S. 18.

Grundsätze der Datenverarbeitung im Beschäftigungsverhältnis

Einwilligung

Auch im Rahmen der Begründung, Aufrechterhaltung und Beendigung von Beschäftigungsverhältnissen bildet § 4 Abs. 1 BDSG die zentrale Erlaubnisnorm. Nach dieser Vorschrift ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet. Darüber hinaus kann die Verwendung von Daten im Arbeitsverhältnis erlaubt sein, wenn der Arbeitnehmer der Erhebung, Verarbeitung und Nutzung im Rahmen einer Einwilligung zugestimmt hat. **13**

Vor allem von Seiten der Landesdatenschutzbeauftragten und auch von Seiten des Bundesdatenschutzbeauftragten wird die Möglichkeit der Einwilligung nach § 4a BDSG im Rahmen eines Beschäftigungsverhältnisses jedoch kritisch gesehen. Hier stellt sich stets die Frage, ob eine Einwilligung freiwillig sein kann. Im Zusammenhang mit Arbeitsverhältnissen wird von verschiedenen Seiten die Freiwilligkeit regelmäßig verneint, weil der Arbeitnehmer praktisch immer auf den Arbeitsplatz zur Existenzerhaltung angewiesen sei.[109] Auch sei es zu berücksichtigen, dass der Arbeitnehmer die Tragweite seiner Einwilligung zur Datenverarbeitung durch den Arbeitgeber nur selten überschauen oder gar erkennen könne. Ihm sei oft nicht bewusst, dass hier sein informationelles Selbstbestimmungsrecht tangiert werde. Welcher Beschäftigte wisse schon Bescheid über die genauen Datenflüsse bei der Einführung und dem Betrieb von Personalverwaltungssystemen oder Personalinformationssystemen oder beim Einsatz von Videotechnik am Arbeitsplatz und den damit verbundenen Risiken für seine Persönlichkeitsrechte.[110] **14**

Die Annahme, eine Einwilligung zur Datenerhebung scheide im Rahmen von Arbeits- und sonstigen Beschäftigungsverhältnissen grundsätzlich aus, findet im Gesetz indes keine Grundlage. Nach hiesiger Auffassung muss vielmehr berücksichtigt werden, dass der Gesetzgeber – auch im Rahmen der Neuregelung in § 32 BDSG – bewusst darauf verzichtet hat, die Erteilung einer Einwilligung im Arbeitsverhältnis als Rechtfertigungsgrundlage für die Datenerhebung auszuschließen. Dementsprechend muss – auch im Beschäftigungsverhältnis – die Einwilligung des Beschäftigten als eine Zulässigkeitsvariante für das Erheben, Verarbeiten und Nutzen personenbezogener Daten anerkannt werden. **15**

Datenverwendung nach Maßgabe allgemeiner Datenschutzbestimmungen

Als einschlägige Rechtsnorm, auf deren Grundlage eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Arbeitsverhältnis gemäß § 4 Abs. 1 BDSG zulässig ist, kommt neben § 32 BDSG und der Möglichkeit einer konkreten Einwilligung des Betroffenen auch die Vorschrift des § 28 BDSG in Betracht. Nach dem Willen des Gesetzgebers verdrängt § 32 BDSG „die übrigen einschlägigen allgemeinen und bereichsspezifischen Vorschriften" des BDSG grundsätzlich nicht.[111] Somit können vor allem die Erlaubnistatbestände des § 28 BDSG, insbesondere die in § 28 Abs. 1 S. Nr. 2 und 3 BDSG genannten,[112] auch hier herangezogen werden. **16**

Speziell im Rahmen eines Bewerbungsverfahrens muss zudem § 3a BDSG beachtet werden, der das allgemeine Gebot der Datenreduzierung enthält, was bezogen auf die Bewerberauswahl eine Beschränkung auf die unbedingt notwendigen personenbezogenen Datenerhebungen beinhaltet. In diesem Rahmen dürfen beispielsweise Auskünfte zu beruflichen Qualifikationen oder zu Berufserfahrungen abgefragt wer- **17**

109 Vgl. *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 32 Rn 20; *Schaar*, Gesetzlich geregelter Arbeitnehmerdatenschutz – dringender denn je, in DGB-Profil Arbeitnehmerdatenschutz, Aug. 2009, S. 9 f., abrufbar unter: https://www.dgb-bestellservice.de/besys_dgb/pdf/DGB31098.pdf.

110 Vgl. *Schaar*, Gesetzlich geregelter Arbeitnehmerdatenschutz – dringender denn je, in DGB-Profil Arbeitnehmerdatenschutz, Aug. 2009, S. 10, abrufbar unter: https://www.dgb-bestellservice.de/besys_dgb/pdf/DGB31098.pdf.

111 BT-Drucks 16/13657, S. 20; z.T. a.A. *Gola*, in: Gola/Schomerus (Hrsg.), BDSG, 10. Aufl. 2010, § 32 Rn 2.

112 *Erfurth*, NJOZ 2009, 2914, 2922; *Polenz*, DuD 2009, 561, 563; *Schmidt*, RDV 2009, 193, 198.

den, nicht aber aus objektiver Sicht nicht erforderliche Informationen, beispielsweise zu Erkrankungen, zu Kinderwünschen oder zu Schwangerschaften.

Scheitert eine Bewerbung, müssen Arbeitgeber die erhobenen Daten mit Blick auf § 35 Abs. 2 Nr. 1 BDSG unverzüglich vollständig löschen; Ausnahmen sind nur soweit zulässig, als dass der Beschäftigte einer längerfristigen Speicherung mit dem Ziel einer späteren Einstellung ausdrücklich freiwillig zugestimmt hat oder die Gefahr der gerichtlichen Inanspruchnahme durch den abgelehnten Bewerber, beispielsweise wegen vermeintlicher AGG-Verstöße, droht. 18

Während bestehender Beschäftigungsverhältnisse kann zudem die Vorschrift des § 3 Abs. 9 BDSG von Relevanz sein, die die besonderen Arten personenbezogener Daten unter einen spezifischen gesetzlichen Schutz stellt. Ein Verstoß gegen geltendes Datenschutzrecht kann dementsprechend vorliegen, wenn ein Arbeitgeber gezielt Informationen zur Erkrankung von Beschäftigten sammelt. 19

Weitere normative Vorgaben mit Auswirkung auf den arbeitsrechtlichen Bereich lassen sich zudem aus § 9 BDSG ableiten, der technische und organisatorische Maßnahmen auflistet, die die Ausführung des Gesetzes gewährleisten sollen. Aus dem Katalog der Schutzmaßnahmen lässt sich beispielsweise folgern, dass der Zugriff auf personenbezogene Daten von Beschäftigten durch Kollegen oder Vorgesetzte auch im Arbeitsverhältnis im Regelfall nicht zulässig ist, was aus dem in § 9 Abs. 1 BDSG normierten Grundsatz der Zugangs- und Zugriffskontrolle folgt. 20

Werden bestimmte Personalverwaltungsaufgaben an externe Dienstleister übertragen, kann zudem die Vorschrift des § 11 BDSG Bedeutung erlangen, die die Auftragsdatenverarbeitung regelt. 21

Übersicht über datenschutzrechtliche Rechtsgrundlagen im Beschäftigungsverhältnis 22

- **§ 4a BDSG Einwilligungserfordernis**: Strittig, ob die Regelung des § 4a BDSG grundsätzlich Anwendung findet oder nur als Rechtsgrundlage für zusätzliche freiwillige soziale Leistungen des Arbeitgebers dienen kann.
- **§ 28 Abs. 1 Satz 1 Nr. 1 BDSG** findet keine Anwendung, da dieser durch § 32 BDSG verdrängt wird.
- **§ 28 Abs. 1 Satz 1 Nr. 2 BDSG** findet Anwendung bei automatisierter Datenverarbeitung.
- **§ 28 Abs. 1 Satz 1 Nr. 3 BDSG** findet Anwendung bei automatisierter Datenverarbeitung.
- **§ 28 Abs. 2 BDSG** findet Anwendung bei automatisierter Datenverarbeitung.
- **§ 28 Abs. 3 BDSG** findet keine Anwendung.
- **§ 28 Abs. 6–8 BDSG** finden bei automatisierter Datenverarbeitung Anwendung.
- **§ 32 BDSG** ist als „lex specialis" immer zu beachten.
- **§§ 3, 9 BDSG** finden Anwendung.
- **§ 11 BDSG** findet Anwendung im Rahmen von Outsourcing-Maßnahmen.

Datenschutz im Bewerbungsverfahren

Bereits vor Begründung eines Arbeitsverhältnisses können Fragen des Datenschutzrechtes in verschiedenen Konstellationen Bedeutung erlangen. 23

Bewerberprofilerstellung anhand öffentlich zugänglicher Quellen

Nach § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten beim Betroffenen zu erheben, soweit keine Rechtsvorschrift eine anderweitige Erhebung vorsieht oder zwingend voraussetzt (sog. Grundsatz der Direkterhebung). Der Grundsatz der Direkterhebung findet auch auf Beschäftigungsverhältnisse Anwendung. 24

Als Erlaubnisnorm kommt § 28 BDSG in Betracht. Nach § 28 Abs. 1 Satz 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten und ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke „unter bestimmten Voraussetzungen zulässig". 25

Soweit es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist, bedarf es nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG keiner Einwilligung in das Erheben, Speichern, Verändern oder Übermitteln der personenbezogenen Daten durch den Betroffenen. Insoweit ist die mit der Direkterhebung verbundene Kenntnisnahme des Betroffenen von einer Datenerhebung suspendiert. Entscheidend ist nur, dass die Datenerhebung im Zusammenhang mit der Begründung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt, ohne dass es in diesem Zusammenhang (anders als im Rahmen der Datenerhebung gemäß § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG) auf etwaige entgegenstehende schutzwürdige Belange des Betroffenen ankäme. 26

Mit Blick auf § 32 Abs. 1 Satz 1 BDSG, der bestimmt, dass personenbezogene Daten eines Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses **erforderlich** ist, stellt sich die Frage, ob die Erlaubnisnorm des § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Zusammenhang mit der Begründung von Beschäftigungsverhältnissen überhaupt Anwendung finden kann. 27

Wollte man § 28 Abs. 1 Satz 1 Nr. 1 BDSG isoliert betrachten und allein darauf abstellen, ob die Datenerhebung im Rahmen eines bestehenden oder zu begründenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt, so könnte sicherlich angenommen werden, dass der Bewerber und sein potenzieller Arbeitgeber bereits durch die Übersendung der Bewerbungsunterlagen ein zumindest rechtsgeschäftsähnliches Schuldverhältnis in Form eines vorvertraglichen Schuldverhältnisses begründen. Die Datenerhebung aus öffentlich zugänglichen Quellen, wie dem Internet, könnte dementsprechend nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt sein. Ein derartiges Verständnis greift jedoch zu kurz und lässt die klaren Wertungen des § 32 Abs. 1 Satz 1 BDSG außer Betracht, der konkret auf die Erforderlichkeit der jeweiligen Datenerhebung abstellt. 28

Ein derartiges **Erforderlichkeitskriterium** ist in § 28 Abs. 1 Satz 1 Nr. 1 BDSG hingegen nicht vorhanden, so dass ein isolierter Rückgriff auf diese Erlaubnisnorm im Ergebnis dazu führen würde, dass die in § 32 Abs. 1 Satz 1 BDSG normierten Grundvoraussetzungen der Datenerhebung, -verarbeitung, und -nutzung für Zwecke des Beschäftigungsverhältnisses unterlaufen würden. Dementsprechend geht auch die Gesetzesbegründung zu § 32 BDSG[113] davon aus, dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Hinblick auf Beschäftigungsverhältnisse durch § 32 BDSG konkretisiert und insoweit verdrängt wird. Die Datenerhebung aus allgemein zugänglichen Quellen, insbesondere dem Internet, kann dementsprechend nicht unter dem Gesichtspunkt des § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt werden.[114] 29

Die Bewerberprofilerstellung aus allgemein zugänglichen öffentlichen Quellen kann folglich nur nach § 28 Abs. 1 Satz 1 Nr. 2 oder Nr. 3 BDSG erfolgen. Diese Regelungen sind nach herrschender Meinung auch im Rahmen von Beschäftigungsverhältnissen anwendbar.[115] 30

Im Rahmen der nach § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG vorzunehmenden Interessenabwägung ist dementsprechend stets zu überprüfen, ob ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an dem Erhalt der Informationen begründet werden kann, hinter welches das Interesse 31

113 BT-Drucks 16/13657, S. 20.

114 So auch *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 32 Rn 25.

115 Vgl. nur *Erfurth*, NJOZ 2009, 2914, 2922; *Polenz*, DuD 2009, 561, 563; *Schmidt*, RDV 2009, 193, 198; *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 32 Rn 26; *Oberwetter*, BB 2008, 1562, 1564 ff.; *Zöll*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 32 Rn 19; *Heuchemer/Zöll*, Personalmagazin 2008, 70 f.; *Ostmann/Kappel*, AuA 2008, 656, 657; *Thum/Szczesny*, BB 2007, 2405 ff.; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437.

des Arbeitnehmers, seine persönlichen Lebensumstände zum Schutz seines Persönlichkeitsrechtes und zur Sicherung der Unverletzlichkeit der Individualsphäre geheim zu halten, zurück zu treten hat. Nur wenn dies zu bejahen ist, kann die einwilligungslose Datenerhebung über einen Bewerber überhaupt zulässig sein.

Dabei ist zu beachten, dass ein Bewerber, der Daten in das Internet eingestellt hat, grundsätzlich damit rechnen muss, dass diese öffentlich zugänglich sind und von potenziellen Arbeitgebern im Rahmen des Einstellungsverfahrens wahrgenommen werden können. Gleiches gilt für Daten, die ein Bewerber in sozialen Netzwerken einstellt, die über eine Suchmaschinenanfrage erhoben werden können, ohne dass eine gesonderte Anmeldung oder Bestätigung für die Freigabe der Daten für den Bewerber notwendig wäre.[116] Derartige Daten sind allgemein zugängliche Daten im Sinne des § 28 Abs. 1 Satz 1 Nr. 3 BDSG, denn sie sind sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu geeignet, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[117] **32**

Dies bedeutet jedoch nicht, dass alle Informationen aus dem Internet oder sozialen Netzwerken für die Personalentscheidungen erhoben werden dürfen. Zweifel können sich beispielsweise in Bezug auf bestimmte Mitgliederdienste ergeben, wie bei den freizeitorientierten Netzwerken StudiVZ, SchülerVZ oder auch Facebook. Bereits die AGB der Betreiber der vorgenannten Plattformen sehen ausschließlich eine Nutzung der Netzwerke für private Zwecke vor, sodass die Erstellung von Bewerberprofilen oder die Verifizierung von Angaben eines Bewerbers durch den Arbeitgeber bereits nicht von dem eigentlichen Nutzungszweck dieser freizeitorientierten Netzwerke erfasst ist .[118] **33**

Das Überwiegen schutzwürdiger Interessen des Betroffenen an der Erhebungsfreiheit derartiger Daten liegt auf der Hand. Vergegenwärtigt man sich beispielsweise, dass ein Bewerber in seinem Facebook-Profil Bilder aus Urlauben, in Freizeitkleidung, von Partys etc. eingestellt haben kann, erschließt sich gleichsam, dass dieser derartige Fotos ganz offensichtlich seiner Bewerbungsmappe nicht beigefügt hätte. Auch wenn ein Arbeitgeber ein berechtigtes Interesse an dem Erhalt derartiger Informationen begründen könnte („wir wollen seriöse Arbeitnehmer"), verstieße eine Datenerhebung hier sicherlich und ganz offensichtlich gegen die berechtigten Interessen des Arbeitnehmers, dessen freizeitliche Aktivitäten in aller Regel auch keine negativen Auswirkungen auf seine berufliche Tätigkeit entfalten. Auch ohne Inkrafttreten der vorbeschriebenen Neuregelungen in § 32 Abs. 6 BDSG-E scheitert eine Datenerhebung aus freizeitorientierten sozialen Netzwerken am Überwiegen schutzwürdiger Interessen des von der Datenerhebung betroffenen Bewerbers. **34**

Eine andere Beurteilung wird dementsprechend für die berufsorientierten Netzwerke, wie Xing oder LinkedIn, anzunehmen sein. Die Informationen, die ein Bewerber im Rahmen derartiger Netzwerke preisgibt, dienen konkret beruflichen Zwecken. **35**

So wurde beispielsweise die Unternehmensplattform Xing (bis Ende 2006 „openBC") als webbasierte Plattform konzipiert, in der natürliche Personen vorrangig ihre geschäftlichen Kontakte zu anderen Personen verwalten können. Kernfunktion des Netzwerkes ist das Sichtbarmachen des Kontaktnetzes; beispielsweise kann ein Benutzer abfragen, über „wie viele Ecken" – also über welche anderen Mitglieder – er einen anderen kennt, dabei wird das so genannte Kleine-Welt-Phänomen sichtbar. Dabei bietet das System zahlreiche Community-Funktionen wie Kontaktseite, Suche nach Interessensgebieten, Foren, Unternehmenswebsites und unzählige Fachgruppen. Das Portal bietet die Möglichkeit, berufliche Daten in das jeweilige Nutzungsprofil einzutragen. So ist es möglich, Studium, Ausbildung, beruflichen Werdegang in tabellarischer (bewerbungsähnlicher) Form darzustellen, eingescannte Zeugnisse und Referenzen hoch- **36**

116 *Rolf/Rötting,* RDV 2009, 263, 266; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437; *Oberwetter*, BB 2008, 1562, 1564.
117 *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, § 28 Rn 189.
118 *Forst*, NZA 2010, 427, 432; *Rolf/Rötting*, RDV 2009, 263, 266 f.; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437.

zuladen sowie ein Profilbild (z.B. ein Passfoto) einzustellen. Zwar besteht eine Verpflichtung zum vollständigen Ausfüllen des Profils mit allen Feldern nicht, Bewerber, die derartige Daten in berufsorientierten Netzwerken einstellen, tun dies jedoch gerade im Bewusstsein der Berufsorientiertheit derartiger Netzwerke. Überwiegende Interessen des (potenziellen) Arbeitnehmers stehen der Erhebung dementsprechend regelmäßig nicht entgegen, da dieser die entsprechenden Dateien freigegeben und demgemäß einen entscheidenden Beitrag für den Zugriff auf die Daten geleistet hat.

Die Datenerhebung aus derartigen berufsorientierten Netzwerken ist ohne Einwilligung des Betroffenen nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG zulässig. **37**

Datenerhebung im Bewerbungsgespräch

Hat der Bewerber die Hürde genommen, sich aus einer Vielzahl von Bewerbungen als potenziell geeigneter Kandidat herausgestellt zu haben, folgt das persönliche Kennenlernen im Rahmen eines Vorstellungsgespräches. Auch im Rahmen der persönlichen Kontaktaufnahme zwischen Arbeitgeber und Bewerber kommt es zu mehr oder minder umfassenden Datenerhebungsmaßnahmen. Wie im Bereich der Bewerberprofilerstellung anhand öffentlich zugänglicher Informationsquellen, wie dem Internet, sind der Datenerhebung durch den Arbeitgeber auch hier Grenzen gesetzt. **38**

Hinsichtlich der zulässigen Fragen, die ein Arbeitgeber an einen Bewerber im Rahmen eines Vorstellungsgespräches stellen darf, kann auf die obigen Ausführungen verwiesen werden. Auch hier ist stets im Einzelfall zu überprüfen, ob eine bestimmte Datenerhebung (Frage) gegenüber dem Bewerber von der Rechtsordnung als berechtigtes Interesse gebilligt ist. **39**

Ist dies nicht der Fall, kann eine Zulässigkeit der Datenerhebung auch nicht etwa daraus hergeleitet werden, dass der Bewerber die (unzulässige) Frage des Arbeitgebers beantwortet. Hierin eine Einwilligung im Sinne des § 4a BDSG in die Datenerhebung zu erblicken, verstieße gegen eindeutige gesetzgeberische Wertungen, die grundsätzlich nicht zur Disposition der Parteien stehen. Wenn also die Frage nach einer bestehenden Schwangerschaft im Rahmen des Bewerbungsverfahrens als grundsätzlich gegen schutzwürdige Belange des Betroffenen verstoßendes Verhalten und damit konkreten Eingriff in das informationelle Selbstbestimmungsrecht des Bewerbers eingestuft wird, kann eine Zulässigkeit der Datenerhebung nicht daraus hergeleitet werden, dass man in der Beantwortung der unzulässigen Frage eine (konkludente) Einwilligung des Betroffenen im Sinne des § 4a BDSG erblickt. Eine solche scheitert – unter Zugrundlegung der klaren gesetzgeberischen Wertung – jedenfalls am Freiwilligkeitskriterium, welches jedenfalls dann als nicht mehr gegeben angesehen werden muss, wo der Gesetzgeber die Unzulässigkeit einer bestimmten Fragestellung konkret festgestellt hat. **40**

Nicht berücksichtigte Bewerber

Die weitere Speicherung personenbezogener Daten von abgewiesenen Bewerbern ist in aller Regel nicht mehr erforderlich.[119] Das allgemeine Persönlichkeitsrecht schließt das Recht ein, darüber zu bestimmen, ob der Arbeitgeber die im Bewerbungsverfahren erfragten persönlichen Daten aufbewahren darf oder ob deren Vernichtung verlangt werden kann. **41**

Datenschutz im Rahmen bestehender Beschäftigungsverhältnisse

Weitergehende Informationen benötigt der Arbeitgeber für die Durchführung laufender Arbeitsverhältnisse. Auch die Berechtigung hierfür leitet sich seit dem 1.9.2009 nicht mehr aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG, sondern maßgeblich aus § 32 BDSG ab. **42**

119 BAG, Urt. v. 6.6.1984 – 5 AZR 286/81, NJW 1984, 2910; *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 32 Rn 62.

Soweit es sich um personenbezogene Daten handelt, die eindeutig für die Durchführung des Beschäftigungsverhältnisses erforderlich sind, wie etwa Name, Anschrift oder Ausbildungsverlauf, aber auch Religionszugehörigkeit, Bankverbindung, das Vorhandensein von Kindern oder Ehegatten etc., darf der Arbeitgeber diese als Bestandteil der Vertragsbeziehung erheben und verarbeiten. Der zweckbezogene Umgang mit diesen Daten ist aus datenschutzrechtlicher Sicht im Regelfall unproblematisch. 43

Internet-, E-Mail, Telefon- und Handynutzung am Arbeitsplatz

In nahezu allen Rechtsanwaltskanzleien hat die Telekommunikationstechnik zwischenzeitlich Einzug gehalten, neben Telefon und Fax sind die Verwendung von E-Mail und Internet zur Selbstverständlichkeit geworden. Welche datenschutzrechtlichen Regelungen der Rechtsanwalt im Rahmen der Verwendung von E-Mail und Internetkommunikation am Arbeitsplatz zu beachten hat, richtet sich entscheidend danach, ob er seine betrieblichen Kommunikationseinrichtungen seinem Beschäftigten (auch) zu privaten Zwecken überlassen hat. Dabei muss der Rechtsanwalt als Arbeitgeber im Bereich der erlaubten Privatnutzung deutlich strengere datenschutzrechtliche Anforderungen beachten, als bei einer rein dienstlichen Nutzung. Bereits hier findet aus datenschutzrechtlicher Sicht die entscheidende Weichenstellung statt. 44

Die Entscheidung, ob und in welchem Umfang Beschäftigte Telefon, Internet und E-Mail am Arbeitsplatz für private Zwecke nutzen dürfen, liegt dabei grundsätzlich im **freien Ermessen** des Arbeitgebers.[120] Der Arbeitgeber kann die private Nutzung von Internet und E-Mail am Arbeitsplatz **ausdrücklich verbieten**, sie aber auch ausdrücklich erlauben. Ohne eine (ggf. konkludent) erteilte Erlaubnis des Arbeitgebers steht dem Arbeitnehmer jedoch **kein Anspruch auf private Nutzung von Internet und E-Mail am Arbeitsplatz** zu.[121] Auch in den Fällen, in denen die private Nutzung nicht ausdrücklich verboten ist, können Arbeitnehmer nicht davon ausgehen, dass sie Internet und E-Mail am Arbeitsplatz für private Zwecke nutzen dürfen.[122] 45

Soweit der Arbeitgeber sich dazu entscheidet, die private Nutzung von Internet und E-Mail am Arbeitsplatz zu gestatten, kann er, da es sich hierbei um eine zusätzliche freiwillige Leistung des Arbeitgebers handelt, die nicht im Austauschverhältnis der mit dem Arbeitgeber zu erbringenden Arbeitsleistung steht,[123] seine Einwilligung sowohl unter einen **Widerrufsvorbehalt** stellen und diese später nach billigem Ermessen **einschränken** oder **widerrufen**, als auch die Privatnutzung der betrieblichen Onlinesysteme einer inhaltlichen **Nutzungsbeschränkung** unterwerfen, z.B. hinsichtlich des Zeitrahmens oder der zugelassenen Bereiche; er kann seine Einwilligung auch an regelmäßig durchzuführende Kontrollmaßnahmen knüpfen.[124] Darüber hinaus können im Rahmen der Einwilligung die technischen und organisatorischen Einzelheiten einer privaten Nutzung der betrieblichen EDV-Ressourcen durch den Arbeitgeber **einseitig bestimmt** werden. Hier sind beispielsweise Vereinbarungen über die Einrichtung einer persönlichen Mail-Adresse für private Kommunikation neben einer funktionsbezogenen Mail-Adresse, die ausschließlich für die dienstliche E-Mail-Kommunikation genutzt wird, denkbar.[125] 46

Auch wenn ein Recht des Arbeitnehmers auf private Nutzung der betrieblichen EDV-Anlagen grundsätzlich nicht besteht, empfiehlt es sich bereits deshalb eine **ausdrückliche Nutzungsregelung** zu treffen, 47

120 *Ernst*, NZA 2002, 585; *Thüsing*, RDV 2009, 1, 4; *Weißnicht*, MMR 2003, 448; *Busse*, in: Besgen/Prinz (Hrsg.), Handbuch Internet.Arbeitsrecht, 2. Aufl. 2009, § 10 Rn 10.

121 Anders kann dies ggf. im Rahmen der Telefonnutzung zu beurteilen sein.

122 *Altenburg/von Reinersdorff/Leister*, MMR 2005, 135; BAG, Urt. v. 7.7.2005 – 2 AZR 581/04, NJW 2006, 540, 542.

123 Vgl. *Däubler*, K&R 2000, 323, 325; *Elschner*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 26. Ergänzungslieferung 2010, Teil 22.1 Rn 30 m.w.N.

124 *Schaar*, Gesetzlich geregelter Arbeitnehmerdatenschutz – dringender denn je, in DGB-Profil Arbeitnehmerdatenschutz, Aug. 2009, S. 5, abrufbar unter: https://www.dgb-bestellservice.de/besys_dgb/pdf/DGB31098.pdf.

125 Vgl. *Elschner*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 26. Ergänzungslieferung 2010, Teil 22.1, Rn 31.

weil nach herrschender Auffassung insbesondere auch eine konkludente Gestattung der privaten Nutzung von E-Mail und Internet im Arbeitsverhältnis in Betracht kommt.[126] Hierfür genügt allerdings nicht die tatsächliche private Nutzung durch den Beschäftigten. Erforderlich ist vielmehr, dass der Arbeitgeber Kenntnis von der privaten Nutzung hatte oder diese zumindest für ihn erkennbar war und er diese über einen längeren Zeitraum geduldet hat, so dass der Arbeitnehmer dementsprechend darauf vertrauen durfte, dass er die betrieblichen EDV-Anlagen auch zukünftig für private Zwecke nutzen kann.

Wegen des mit der Einwilligung in die private Nutzung von Telefon, Internet und E-Mail am Arbeitsplatz verbundenen Risikos für den Arbeitgeber, insbesondere in Bezug auf die erheblichen Schwierigkeiten der Kontrolle des Nutzungsverhaltens, sind an die Voraussetzungen für das Vorliegen einer konkludenten Einwilligung des Arbeitgebers strenge Anforderungen zu stellen. 48

Merke! 49

- Selbst bei rein dienstlicher E-Mail-Nutzung ist eine lückenlose Überwachung von E-Mails nicht zulässig, weil damit die ständige Kontrolle des Arbeitnehmers verbunden wäre und eine derartige automatisierte Vollkontrolle als schwerwiegender Eingriff in das Persönlichkeitsrecht des Beschäftigten nicht zulässig ist.
- Der Arbeitgeber darf aber eine stichprobenhafte und zeitnahe Auswertung der Protokolldaten vornehmen, wobei das Verfahren möglichst transparent zu gestalten ist.
- Das ständige Mitlesen von E-Mails ist dementsprechend nicht zulässig.

Die Grundsätze zur Zulässigkeit der Kontrolle der Verbindungsdaten und des Inhaltes geschäftlichen E-Mail-Verkehrs gilt nicht bei Arbeitnehmern mit Sonderstatus, wie Rechtsanwälten, denen in § 203 StGB eine besondere Verschwiegenheitsverpflichtung auferlegt wird. Sie dürfen die ihnen dienstlich anvertrauten Geheimnisse nicht an Dritte und damit grundsätzlich auch nicht an ihren eigenen Arbeitgeber weitergeben. Eine Überwachung des dienstlichen E-Mail-Verkehrs und der aufgerufenen Internetseiten dieser Arbeitnehmer ist dementsprechend regelmäßig aufgrund der vorrangigen schutzwürdigen Interessen der Beschäftigten bzw. ihrer Kommunikationspartner unzulässig.[127] Dies gilt sowohl für die äußeren Verbindungsdaten als auch für die Inhaltsdaten einer dienstlichen E-Mail. 50

Soweit den Beschäftigten die Nutzung ihrer betrieblichen E-Mail-Accounts auch für private Zwecke gestattet wird, stellt sich die Frage, wie mit den E-Mail-Accounts ausgeschiedener Beschäftigter verfahren werden soll. 51

Wegen der Möglichkeit, dass an das E-Mail-Account nach wie vor E-Mails mit privatem Inhalt an den ehemaligen Mitarbeiter gerichtet werden, scheidet eine „Übernahme“ des E-Mail-Accounts durch den Arbeitgeber nach Ausscheiden des Arbeitnehmers aus dem Beschäftigungsverhältnis grundsätzlich aus. Auch nach Beendigung des Beschäftigungsverhältnisses ist der Arbeitgeber in Bezug auf das privat genutzte E-Mail-Account an das Fernmeldegeheimnis des § 88 TKG gebunden. 52

Um datenschutzrechtliche Probleme zu vermeiden, sollte der E-Mail-Server im Falle des Ausscheidens eines Beschäftigten so konfiguriert werden, dass eingehende E-Mails automatisch an den Absender zurückgesendet werden und diesem erklärt wird, dass der E-Mail-Account nicht mehr in Verwendung ist. Hier muss sichergestellt werden, dass der Arbeitgeber selbst vom Nachrichteninhalt keine Kenntnis nehmen kann. Hier bietet sich an, dass in der automatisch an den Absender zurückgesendeten Erklärung auf 53

126 *Busse*, in: Besgen/Prinz (Hrsg.), Handbuch Internet.Arbeitsrecht, 2. Aufl. 2009, § 10 Rn 13; *Elschner*, in: Hoeren/Sieber (Hrsg.) Handbuch Multimedia-Recht, 26. Ergänzungslieferung 2010, Teil 22.1., Rn 41.

127 BAG, Urt. v. 13.1.1987 – 1 AZR 267/85, DB 1987, 1153; *Beckschulze/Henkel*, DB 2001, 1491, 1495.

einen neuen Ansprechpartner im Unternehmen unter Angabe seiner Kontaktdaten hingewiesen wird, um sicherzustellen, dass betrieblich veranlasste E-Mails nach wie vor den Weg in das Unternehmen finden.

Arbeitnehmerdaten im Internetauftritt des Unternehmens

54 Viele Rechtsanwaltskanzleien geben mittlerweile personenbezogene Daten ihrer Beschäftigten auf der Kanzleiinternetseite bekannt- Veröffentlicht werden meist Name, Titel, Arbeitsgebiet und Erreichbarkeit per Telefon, Telefax oder E-Mail, häufig gehen die Angaben aber auch darüber hinaus und beinhalten zudem Veröffentlichungen des Lebenslaufes oder eines Fotos des Mitarbeiters.

55 Hier richtet sich die datenschutzrechtliche Zulässigkeit nach den Bestimmungen des BDSG. Grundsätzlich gilt hier ebenso, dass ohne Einwilligung des betroffenen Arbeitnehmers die Veröffentlichung der Daten nur in besonderen Ausnahmefällen zulässig sein wird, z.B. wenn die Angaben über den Mitarbeiter auf der Homepage für einen Kunden- bzw. Interessentenkontakt notwendig sind. In allen anderen Fällen wird die Veröffentlichung von Arbeitnehmerdaten im Internet grundsätzlich nur auf Grundlage einer konkreten Einwilligung des Arbeitnehmers erfolgen dürfen. Neben den Bestimmungen des BDSG unterliegen Fotos zudem den speziellen Regelungen des Gesetzes betreffend des Urheberrechts an Werken bildender Künste und Fotografie (KUG). Nach §§ 22 ff. KUG, die das Recht am eigenen Bild regeln, ist die Verbreitung und öffentliche Zurschaustellung von Personenfotos dann unzulässig, wenn keine Einwilligung des Abgebildeten vorliegt.

56 Vorsicht ist geboten, wenn es um die Mitteilung spezifischer Informationen geht. Über einen interessanten Fall berichtet der Hessische Datenschutzbeauftragte in seinem Tätigkeitsbericht aus dem Jahr 2010[128]:

57 An ihn wurde telefonisch eine Beschwerde über die Homepage eines Reisebüros herangetragen, auf der neben den Kontaktdaten der Mitarbeiter mit Angabe über den jeweiligen Zuständigkeitsbereich auch die Kontaktdaten eines Auszubildenden veröffentlicht wurden, die darüber hinaus die zusätzliche Information: „Herr X befindet sich z. Z. im Krankenstand" enthielten. Die Veröffentlichung dieser Daten stellte einen Verstoß nach § 28 Abs. 6 BDSG dar, wonach u.a. die Übermittlung sensibler Daten, zu denen auch Gesundheitsdaten gehören, nur unter ganz bestimmten Voraussetzungen zulässig sind. Die Angabe „z. Z. im Krankenstand" war von dem Landesdatenschutzbeauftragten[129] – zu Recht – als besonderes personenbezogenes (Gesundheits-)Datum eingestuft worden.[130] Seine Veröffentlichung war dementsprechend nicht zulässig.

58 Ebenso wie die Bekanntgabe von Gesundheitsdaten grundsätzlich gegen die schutzwürdigen Interessen des Beschäftigten verstößt, wird auch die Bekanntgabe von privaten Daten, wie beispielsweise der privaten Anschrift und Telefonnummer, der Anzahl der Kinder, dem Familienstand, Geburtsdatum usw. regelmäßig nicht ohne ausdrückliche Einwilligung des Betroffenen zulässig sein.

59 **Mitarbeiterdaten – was darf veröffentlicht werden?**

- Unproblematisch:
  - Vor- und Nachname
  - Titel, akademischer Grad
  - Berufsqualifikation
  - Aufgabenbereich / Funktion
  - Postalische Dienstanschrift
  - Telefonische Erreichbarkeit (ohne Durchwahlnummer), Telefax und E-Mail

128 Hessischer Landtag, Drucks. 18/2027 vom 28.9.2010, abrufbar unter http://www.datenschutz.hessen.de/taetigkeitsberichte.htm.
129 Hessischer Landtag, Drucks. 18/2027 vom 28.9.2010, abrufbar unter http://www.datenschutz.hessen.de/taetigkeitsberichte.htm.
130 Ähnlicher Fall in: EuGH, Urt. v. 6.11.2003 – Rs. C-101/01, Slg. 2003, I-12971 = EuZW 2004, 245.

- Nur mit Einwilligung des Betroffenen zulässig:
  - Bekanntgabe der Privatanschrift
  - Private Erreichbarkeit per Telefon
  - Fotos
  - Staatsangehörigkeit
  - Angaben zur Konfession
  - Gewerkschaftszugehörigkeit

Glossar

Begriff	Erläuterung
Anonymisierung	Anonymisierung ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG).
Arbeitnehmerdatenschutz	Unter dem Begriff „Arbeitnehmerdatenschutz" wird die Gesamtheit aller datenschutzrechtlichen Regelungen, die ein Dienst- oder Arbeitsverhältnis betreffen, verstanden.
ASP (Application Service Providing):	Bei ASP stellt ein Anbieter dem Nutzer Anwendungen über das Internet zur Verfügung. Dieses Softwaremietmodell gibt es schon seit über einem Jahrzehnt. Es konnte sich lange nicht durchsetzen, da entsprechende schnelle Datennetze fehlten. Der neue Name für ASP ist Software as a Service (SaaS). Es ist ein Teil von Cloud-Computing.
Auftragsdatenverarbeitung	Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten durch eine andere verantwortliche Stelle im Auftrag erhoben, verarbeitet oder genutzt werden (§ 11 BDSG). Die andere Stelle muss dabei den Weisungen des Auftraggebers unterworfen sein und darf keine eigene Entscheidungsbefugnis darüber besitzen, wie sie mit den Daten umgeht (Gegensatz zur sog. Funktionsübertragung).
Auftragskontrolle	Maßnahmen zur Gewährleistung, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Anlage zu § 9 BDSG Nr. 6).
Auskunftei	Privatrechtlich organisiertes Unternehmen mit dem Zweck, wirtschaftlich relevante Daten, wie z.B. Informationen über Kreditwürdigkeit und Zahlungsfähigkeit von Privaten oder Unternehmen, zu sammeln und an anfragende Unternehmen oder sonstige Dritte weiterzugeben. Regelungen finden sich in §§ 28a, 29 BDSG.
Automatisierte Einzelentscheidung	Es ist grundsätzlich verboten, Entscheidungen, die für den Betroffenen eine rechtliche Folge gleich welcher Art nach sich ziehen oder ihn in der Entscheidung erheblich beeinträchtigen, ausschließlich auf eine automatisierte Verarbeitung oder Nutzung personenbezogener Daten zu stützen (§ 6a BDSG). Z.B. Scoring-Verfahren der Kreditwirtschaft sind in der Regel automatisierte Einzelentscheidungen.
Automatisierte Verarbeitung	Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (§ 3 Abs. 2 BDSG).
Automatisiertes Abrufverfahren	Verfahren, mit welchem automatisiert der Abruf von Daten und so deren Übermittlung ermöglicht wird (vgl. § 10 BDSG).

Begriff	Erläuterung
Besondere Arten personenbezogener Daten	Besonders sensible Arten von personenbezogenen Daten, die in § 3 Abs. 9 BDSG aufgelistet sind. Darunter fallen alle Angaben und Daten über: ■ rassische oder ethnische Herkunft ■ politische Meinungen ■ religiöse oder philosophische Überzeugungen ■ Gewerkschaftszugehörigkeit ■ Gesundheit ■ Sexualleben
Bestandsdaten	Personenbezogene Daten, welche für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen einem Nutzer und dem Diensteanbieter über die Nutzung von Telemediendiensten erforderlich sind (§ 14 Abs. 1 TMG).
Betroffener	Zentraler Begriff des Datenschutzrechtes. Betroffener ist die bestimmte oder bestimmbare Person, über die Daten vorliegen (§ 3 Abs. 1 BDSG).
Binding Corporate Rules (BCR)	Verbindliche Unternehmensregelungen, durch die ausreichende Garantien für Datentransfers in Drittländer hergestellt werden sollen, in denen ein angemessenes Datenschutzniveau nicht sichergestellt ist.
Cloud-Computing	Cloud-Computing ist eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen, bereitgestellt als Echtzeit-Service über das Internet und abgerechnet nach Nutzung. Neben SaaS kommen beim Cloud-Computing noch die Ebenen PaaS (Platform as a Service) und IaaS (Infrastructure as a Service) hinzu, die aber für Kanzleien unerheblich sind. Zentral ist vielmehr der Gedanke, dass nicht nur die Anwendungen, sondern auch die daraus erzeugten Daten in einem externen Rechenzentrum gespeichert werden. Im Unterschied zu ASP sind die Anwendungen beim Cloud Computing außerdem rein browserbasiert, sodass überhaupt nichts mehr auf dem Rechner installiert werden muss. Siehe auch: **Public-Cloud-Computing** und **Private-Cloud-Computing**
Codes of Conduct	Wohlverhaltenserklärungen, insbesondere in Großunternehmen, Datenschutzvorschriften und entsprechende Verträge einzuhalten.
Data Mining	Unter dem Begriff des „Data Mining“ (mining (engl.) = Bergbau) werden verschiedene Techniken verstanden, mit denen sich aus umfangreichen, sehr detaillierten und verteilten Datenbeständen bislang unerkannte Informationen und Zusammenhänge zwischen den einzelnen Daten extrahieren lassen (bspw. Erstellung von Kundenprofilen aus vorhandenen Bestell-, Adress-, Zahlungs- oder Reklamationsdateien).
Data Warehouse (auch: Datenlager)	System zur zentralen Sammlung von Daten in einem Unternehmen oder einer sonstigen Organisation mit dem Ziel der Informationsintegration.
Datenerhebung	Datenerhebung ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG).
Datenexport	Transfer von Daten ins Ausland.
Datenimport	Transfer von Daten ins Inland.
Datenlöschung	Datenlöschung ist die endgültige, nicht mehr rückgängig zu machende Vernichtung personenbezogener Daten, die dazu führt, dass die Informationen nicht mehr lesbar gemacht werden können.

Begriff	Erläuterung
Datenschutzrechtlicher Erforderlichkeitsgrundsatz	Das BDSG normiert an verschiedenen Stellen, dass Maßnahmen, die in die Rechte des Betroffenen eingreifen, unabdingbar sein müssen, um einen bestimmten Zweck zu erreichen, und keine gleichermaßen wirksame Maßnahme zur Zweckerreichung zur Verfügung steht.
Datensparsamkeit	Nach dem Grundsatz der Datensparsamkeit dürfen nicht mehr Informationen, als für den erstrebten Zweck erforderlich sind, erhoben und verwendet werden. Dieser Grundsatz wird durch die Pflicht, von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, geschützt.
Datenspeicherung	Datenspeicherung ist das Vorrätig-Halten von Daten in elektronischen Dateien und in Akten, soweit diese so angeordnet sind, dass ein gezielter Zugriff auf personenbezogene Daten möglich wird.
Datensperrung	Datensperrung führt dazu, dass Daten nicht mehr verarbeitet oder genutzt werden können. Um dies sicherzustellen, sind gesperrte Daten zu kennzeichnen (§ 3 Abs. 4 Nr. 4 BDSG). Ein Anspruch auf Datensperrung durch den Betroffenen besteht beispielsweise dann, wenn die Richtigkeit von Daten umstritten ist (§ 20 Abs. 4 BDSG, § 35 Abs. 4 BDSG).
Datenübermittlung	Datenübermittlung ist die Weitergabe von personenbezogenen Daten von der speichernden Stelle an eine andere Stelle zum Zwecke der Weiterverarbeitung und/oder Nutzung durch diese. Die Übermittlung unterliegt den Vorschriften in §§ 16 bis 18 BDSG sowie §§ 28, 29 BDSG.
Datenveränderung	Datenveränderung ist jedes inhaltliche Umgestalten von gespeicherten Daten, z.B. das Hinzuspeichern weiterer Informationen („schlechte Zahlungsmoral“).
Datenverarbeitung	Datenverarbeitung (Abk.: DV) bezeichnet im weiteren Sinn jeden Prozess, bei dem Daten mit oder ohne technische Hilfsmittel erfasst (erhoben), gespeichert, verändert, übermittelt, gesperrt oder gelöscht werden. Die Datenverarbeitung ist von der Datennutzung abzugrenzen, die jede Verwendung von Daten umfasst, soweit es sich nicht bereits um eine Verarbeitung handelt (bspw. „**Data Mining**“).
Datenverarbeitungsanlage	Unter einer Datenverarbeitungsanlage (Abk.: DVA) ist ein elektronisches System zu verstehen, welches Daten annimmt, speichert, verarbeitet und abgibt (beispielsweise PC, aber auch große Rechenzentren).
Datenvermeidung	Grundsatz des Datenschutzrechts, wonach möglichst wenig personenbezogene Daten erhoben, verarbeitet oder genutzt werden sollen (§ 3a Satz 1 BDSG).
Direkterhebung	Erhebung von personenbezogenen Daten beim Betroffenen selbst.
Drittländer	Solche Staaten, die nicht dem EU-/EWR-Raum zugeordnet werden. Der Begriff wird in der Regel mit dem Datenim- und -export verwendet.

Begriff	Erläuterung
Funktionsübertragung	Eine Funktionsübertragung ist das „Gegenstück" zur → **Auftragsdatenverarbeitung**. Sie liegt nach der herrschenden Meinung vor, wenn ■ der Datenverarbeiter eigene Entscheidungsbefugnisse hinsichtlich des „Wie" der Datenverarbeitung und der Auswahl der Daten hat, ■ neben der Übertragung der Datenverarbeitung eine Übertragung der zugrunde liegenden Aufgabe auf den Dienstleister erfolgt, ■ der Datenverarbeiter für die Zulässigkeit der Verarbeitung der Daten verantwortlich ist, ■ dem Datenverarbeiter Rechte zur Nutzung an den Daten für eigene Zwecke überlassen sind und ■ er ein eigenes Interesse an der Datenverwendung hat.
Geschäftsmäßige Datenerhebung	Eine geschäftsmäßige Datenerhebung liegt vor, wenn die Datenerhebung den Hauptzweck der Geschäftstätigkeit der verantwortlichen Stelle darstellt, diese also mit den Daten selbst einen Haupt- und nicht nur Nebenzweck verfolgt, beispielsweise die (entgeltliche) Weitergabe der gesammelten Daten an Dritte. Rechtsgrundlagen der geschäftsmäßigen Datenerhebung finden sich in §§ 29, 30 und § 30a BDSG.
IP-Adresse	Auf dem Internetprotokoll ("IP") basierende Adresse eines einzelnen Rechners in netzgebundenen Systemen, welche den einzelnen Computer erreichbar macht.
Koppelungsverbot	Im Datenschutzrecht bedeutet Koppelungsverbot grundsätzlich, dass die Erbringung von Leistungen nicht von der Einwilligung in die Verarbeitung oder Nutzung von Daten abhängig gemacht werden darf. Das Koppelungsverbot gilt grds. nur dann, wenn dem Betroffenen kein anderer Zugang zu einer gleichwertigen vertraglichen Leistung offensteht oder zugemutet werden kann. Letztlich betrifft es also nur Unternehmen mit marktbeherrschender Stellung. Im Verstoßensfalle ist die Einwilligung des Kunden unwirksam.
Lettershopverfahren	Beim Lettershopverfahren stellt das werbende Unternehmen sein Werbematerial (z.B. Prospekte) einem Dritten (sog. Lettershop) zur Verfügung. Der Lettershop bekommt von einem Dritten (z.B. einem Verlag) die Adressen von dessen Abonnenten bzw. Interessenten und versendet dann an diese das Werbematerial. Das werbende Unternehmen (Versandhaus) erhält nur und erst dann Kenntnis von der Adresse, wenn der angeschriebene mit einer Bestellung reagiert. Damit werden die Daten des Verlags für Zwecke der Werbung für fremde Angebote genutzt. Dies ist nach § 28 Abs. 3 S. 5 BDSG zulässig.
Listenprivileg	Das sog. Listenprivileg ist in § 28 Abs. 3 Satz 2 Nr. 1 BDSG geregelt. Es erlaubt die Übermittlung und/oder Nutzung von bestimmten listenmäßig zusammengestellten Daten über Angehörige einer Personengruppe.
Nicht-öffentliche Stellen	Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts (§ 2 Abs. 4 BDSG). Hierunter fallen die GmbH, AG, KG, OHG, PartG, BGB-Gesellschaft, Vereine, Stiftungen, Parteien sowie natürliche Personen, etwa Einzelkaufleute und Freiberufler.

Begriff	Erläuterung
Öffentliche Stellen	Im Bereich der öffentlichen Stellen unterscheidet das BDSG die öffentlichen Stellen des Bundes (§ 2 Abs. 1 BDSG), die öffentlichen Stellen der Länder (§ 2 Abs. 2 BDSG) sowie die Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder (§ 2 Abs. 3 BDSG). Hierunter fallen insbesondere Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der Länder und der Gemeinden. Siehe auch: **Nicht-öffentliche Stellen**
Personenbezogene Daten	Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG) Siehe auch: **Besondere Arten personenbezogener Daten**
PNR	= Passenger Name Records (engl. für Fluggastdaten).
Private-Cloud-Computing	Dabei werden virtualisierte Infrastrukturen nur von einem Unternehmen genutzt, um beispielsweise mehrere Unternehmensbereiche und -standorte zentral mit IKT-Ressourcen zu versorgen. Private Clouds können vom Unternehmen selbst, aber auch von einem externen Dienstleister betrieben oder gehostet werden. Siehe auch: **Cloud-Computing** und **Public-Cloud-Computing**
Pseudonymisierung	Pseudonymisierung ist eine Aktivität, im Rahmen derer Identifikationsmerkmale einer Person, vorrangig der Name, durch ein Kennzeichen ersetzt wird, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
Public-Cloud-Computing	Hier nutzen die Anwender Applikationen von einem externen Dienstleister über das öffentliche Internet. Viele Kunden teilen sich dabei eine virtualisierte Infrastruktur. Daten und Anwendungen werden zwar logisch getrennt, aber auf denselben physischen Rechnern gespeichert. Siehe auch: **Cloud-Computing** und **Private-Cloud-Computing**
Quik freeze (auch: quick freezing)	Vorgang, bei welchem Daten im Verdachtsfall von Telekommunikationsdiensteanbietern oder Internet-Providern "eingefroren" werden, wenn ein darauf gerichtetes Begehren von Strafverfolgungsbehörden zulässig ist (Alternative zur Vorratsdatenspeicherung).
Safe-Harbor-Principles	Vom Handelsministerium der Vereinigten Staaten von Amerika ausgearbeitete Grundsätze zum Schutze personenbezogener Daten durch dort ansässige Unternehmen. US-Unternehmen können sich diesen Prinzipien anschließen, um mit Blick auf den Erhalt von Daten aus der Europäischen Union bzw. ihren Mitgliedstaaten ein angemessenes Schutzniveau sicherzustellen.
Scoring	Scoring ist ein mathematisch-statistisches Verfahren, mit dem die Wahrscheinlichkeit für ein zukünftiges Verhalten des Betroffenen berechnet wird. Je höher der Score-Wert, desto höher die Bonität.

Begriff	Erläuterung
Standardvertragsklauseln	Von der EU-Kommission für privatwirtschaftliche Unternehmen entworfene Vertragsklauseln, durch welche der Schutz personenbezogener Daten bei einer Übermittlung in das Ausland sichergestellt werden soll, wo kein angemessenes Schutzniveau im Sinne des Art. 25 RiL 95/46/EG bzw. § 4b Abs. 2 BDSG besteht.
Standortdaten	Personenbezogene Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geographischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben (Art. 2 lit. c RiL 2002/58/EG, vgl. § 3 Nr. 19 TKG).
SWIFT	= Society for Interbank Financial Telecommunications; Finanzdienstleister in Form einer Genossenschaft, deren Mitglieder Geldinstitute sind und die Nachrichten, z.B. solche betreffend Geldüberweisungen, an die Mitglieder weiterleitet.
Trennungsprinzip	Grundsatz, demzufolge eine Verwaltungsstelle nur Zugriff auf solche personenbezogenen Daten haben darf, die zur Erfüllung der wahrzunehmenden Aufgabe jeweils erforderlich sind.
Verantwortliche Stelle	Die „verantwortliche Stelle“ ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG).
Verfügbarkeitskontrolle	Maßnahmen, mit welchen gewährleistet werden soll, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Anlage zu § 9 BDSG Nr. 7).
Verkehrsdaten	Personenbezogene Daten, welche zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung des Vorgangs verarbeitet werden (Art. 2 lit. b RiL 2002/58/EG, vgl. § 3 Nr. 30 TKG).
Vorabkontrolle	Prüfung der Beherrschbarkeit neuer Datenerhebungs-, -verarbeitungs- und -nutzungsverfahren vor deren Einführung in einem Unternehmen oder einer Behörde. Zur Vorabkontrolle verpflichtet ist regelmäßig der Datenschutzbeauftragte.
Weitergabekontrolle	Maßnahmen, mit welchen gewährleistet werden soll, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können; des Weiteren Maßnahmen, durch welche überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübermittlung vorgesehen ist (Anlage zu § 9 BDSG Nr. 4).
Zugangskontrolle	Maßnahmen, mit welchen verhindert werden soll, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Anlage zu § 9 BDSG Nr. 2).

Begriff	Erläuterung
Zugriffskontrolle	Maßnahmen, durch welche gewährleistet werden soll, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können; des Weiteren Maßnahmen, mit welchen sichergestellt werden soll, dass personenbezogene Daten bei der Verarbeitung und Nutzung wie auch nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Anlage zu § 9 BDSG Nr. 3).
Zutrittskontrolle	Maßnahmen, mit welchen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, verwehrt wird (Anlage zu § 9 BDSG Nr. 1).

Umfrageergebnisse
Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

Zeitraum der Umfrage: 21.-27.3.2014
Anzahl der Teilnehmer: 214
Zielgruppe: Rechtsanwälte

Frage	Anzahl	Prozent
Wie verwalten Sie Ihre Aktenbestände?		
Papier-Handakten und elektronische Akten	153	71,50 %
„klassische“ Papier-Handakten	57	26,64 %
ausschließlich elektronisch	4	1,87 %
Im Rahmen der Mandantenkommunikation nutze ich:		
sowohl elektronische Kommunikationsmittel als auch den klassischen Postweg	209	97,66 %
ausschließlich den Postweg	4	1,87 %
ausschließlich elektronische Kommunikationsmittel (eAkte, E-Mails, sonstige)	1	0,47 %
Im Rahmen der Kommunikation mit Gerichten und Behörden nutze ich:		
ausschließlich den Postweg	116	54,21 %
sowohl elektronische Kommunikationsmittel als auch den klassischen Postweg	98	45,79 %
ausschließlich elektronische Kommunikationsmittel (eAkte, E-Mails, sonstige)	0	0,00 %
Nutzen Sie Chipkartenlesegeräte für die qualifizierte elektronische Signatur?		
Nein	134	62,62 %
Ja	80	37,38 %
Soweit Sie elektronische Akten führen, ist der Zugriff nur innerhalb der Kanzlei oder auch von außen möglich?		
ausschließlich innerhalb der Kanzlei	138	64,49 %
externer Zugriff möglich	76	35,51 %
Soweit Sie externe Zugriffsmöglichkeinen eingerichtet haben, sind diese besonders gesichert?		
Ja	153	71,50 %
Nein	61	28,50 %
Wo erfolgt die Speicherung Ihrer elektronischen Daten?		
ausschließlich auf eigenen Servern in der Kanzlei	188	87,85 %
in einem Rechenzentrum durch einen Dienstleister / Service-Anbieter	16	7,48 %
teilweise oder vollständig in einer „Cloud“	10	4,67 %
ausschließlich an externen Orten	0	0,00 %

Wie erfolgt die Wartung von EDV-Systemen innerhalb Ihrer Kanzlei?		
Die Wartung wird ganz oder teilweise von externen Dienstleistern erbracht	101	47,20 %
Die IT-/EDV-Systeme werden ausschließlich durch eigene Mitarbeiter gewartet	79	36,92 %
Es existieren zu Wartungszwecken externe Zugänge zu den Systemen (z.B. RDP, VPN)	34	15,89 %

Ist in Ihrer Kanzlei ein Datenschutzbeauftragter bestellt und falls nein, wissen Sie momentan, ob Sie (nach Gesetz) einen Datenschutzbeauftragten bestellen müssen?		
Ja	75	35,05 %
Nein	139	64,95 %

Gibt es Regelungen für den Transport oder den Versand von Datenträgern?		
Ja	86	40,19 %
Nein	128	59,81 %

Gibt es Regelungen für die Behandlung und Übertragung personenbezogener Daten?		
Ja	127	59,35 %
Nein	87	40,65 %

Gibt es ein Zutrittskontrollsystem für wichtige IT-Systeme, Netzwerkkomponenten und Räume?		
Ja	116	54,21 %
Nein	98	45,79 %

Gibt es Passwortkonventionen technischer oder organisatorischer Struktur?		
Ja	103	48,13 %
Nein	111	51,87 %

Ist ein Berechtigungskonzept vorhanden?		
Ja	132	61,68 %
Nein	82	38,32 %

Gibt es eine Backup-Strategie und wird das Rückspielen von Daten regelmäßig auf Funktionalität und Richtigkeit geprüft?		
Ja	167	78,04 %
Nein	47	21,96 %

Marktübersicht – Dienstleister Kanzleisoftware

Advolux GmbH
Advolux
www.advolux.de
Advolux-Support@haufe.de
0800 7234246

Advo-web GmbH
Advoware Kanzleisoftware
www.advo-ware.de
info@advo-web.net
02335 84760

B&L Firmengruppe
Advolux
www.renostar.de
info@renostar.de
06022 205580

Carlos Claussen Consulting GmbH & Co. KG
a-jur Kanzleisoftware
www.a-jur.de
ccc@a-jur.de
040 30964033

DATEV eG
DATEV Anwalt classic pro
www.datev.de/anwalt
anwalt@datev.de
0800 3283863

GKO Gesellschaft für Kanzlei Organisation mbH
Kanzlei Manager
www.gko.de
info@gko.de
0221 9556230

Hitcon AG
K@nzlei/SOZIUS®
www.hitcon.de
Helmut.Holtstiege@hitcon.de
0251 28010

Lawconsult GmbH
Syndicus
www.lawconsult.de
info@lawconsult.com
089 12393980

LAWgistics
LAWgistics Mandatsverwaltung
www.lawgistic.de
info@lawgistic.de
02192 2696

NoRa GmbH
NoRa Advanced
www.nora-software.de
info@nora-software.de
05451 9210

RA WIN 2000 Software GmbH
RA WIN 2000
www.ra2000.de
info@rawin.net
030 4177960

RA-MICRO GmbH & Co. KGaA
RA-MICRO 1
www.ra-micro.de
info@ra-micro.de
030 43598500

Rummel AG
WinMacs
www.rummel-ag.de
info@rummel-ag.de
09123 18300

Wolters Kluwer Deutschland GmbH
AnNoText
www.annotext.de
info@annotext.de
0221 943736000

Marktübersicht Dienstleister sicher e-Mailen

Deutsche Post AG
E-Postbrief
www.epost.de
E-Post@deutschepost.de
0228 1820

mail.de
De-Mail
www.mail.de
info@mail.de
05241 7434982

RitLabs
The Bat/The Bat Voyager/Batpost
www.ritlabs.com
office@ritlabs.com
0373 22808404

Giegerich & Partner GmbH
gpg4o
www.giepa.de
info@giepa.de
06103 58810

Telekom Deutschland GmbH
De-Mail
De-Mail@telekom.de
kundenservice.festnetz@telekom.de-mail.de
0800 330 9415

Tutao GmbH
TutaNota
www.tutanota.de
hello@tutao.de
0511 2028010

web.de Club
De-Mail
www.web.de
info@web.de
0721 9609740

login2work
Virtuell Exchange
www.login2work.de
hofmann@login2work.de
09721 67594650

Marktübersicht Dienstleister Cloudlösungen

adesso AG
drebis
www.adesso.de
info@adesso.de
0231 9309330

ACI EDV-Systemhaus GmbH
ASP
www.aci-edv.de
info@aci-edv.de
04131 8590

login2work
Virtuell Workspace
www.login2work.de
hofmann@login2work.de
09721 67594650

e.Consult AG
WebAkte
www.webakte.de
service@e-consult.de
0681 9508280

T-Systems
doculife law
http://testen-und-bestellen.t-systems.de/ecp-de/testen-bestellen/doculife-ihr-document-management-system-aus-der-cloud/6422

Datev
Datev-Cloud
www.datev.de
info@datev.de
0911 3190

hagel IT-Services GmbH
Cloud-Computing
www.hagel-it.de
info@hagel-it.de
040 28410260

Marktübersicht – Dienstleister Chipkartenlesegeräte

Identive GmbH
SCM Chipdrive pinpad (spr532)
www.identive-infrastructure.com
info@identive-infrastructure.com
089 95955000

Kobil Systems GmbH
Chipkartenterminal KAAN Advanced
www.kobil.com
marketing@kobil.com
06241 30040

REINER Kartengeräte GmbH und Co. KG
cyberJack RFID komfort
www.reiner-sct.com
mail@reiner-sct.com
07723 50560

ZF Friedrichshafen AG Electronic Systems
SmartBoard, SmartTerminal
www.cherry.de
info@cherry.de
09643 180

OMNIKEY GmbH
CardMan Trust
www.hidglobal.de
06123 7910

OpenLimit SignCubes GmbH
truedentity, SignatureService, Reader
www.openlimit.com
info@openlimit.com
030 400351020

Marktübersicht – Dienstleister Akten- und Datenvernichtung

DATA Kill Aktenvernichtung bundesweit
Akten - und Datenvernichter
www.datakill.de
aktenvernichtung@datakill.de
06108 9885420

MAMMUT Dokumentenservice GmbH & Co. KG
Akten - und Datenvernichter
www.mammut-hamburg.de
info@mammut-hamburg.de
040 8547600

Reisswolf Deutschland GmbH
Akten - und Datenvernichter
www.reisswolf.de
info@reisswolf.de
040 25304240

Shred-it GmbH
Akten - und Datenvernichter
www.shredit.de
munich@shredit.com
06102 882740

Zimmermann Datenvernichtung GmbH
Akten - und Datenvernichter
www.zimmermann-datenex.de
info@zimmermann-datenex.de
0251 6207500

Diese Auflistung wurde vom Deutschen Anwaltverlag erstellt und erhebt keinen Anspruch auf Vollständigkeit.

Stand: 19.9.2014

Wolters Kluwer

AnNoText®

Vorteil durch Weitblick

Mit AnNoText® die aktuellen Herausforderungen an Datenschutz und Datensicherheit meistern.

AnNoText® setzt auf modernste Microsoft® .NET und SQL-Datenbanktechnologien, um jederzeit die Sicherheit Ihrer Datenhaltung zu ermöglichen. Und mit AnNoNet verfügen Sie darüber hinaus über das Schutzschild für alle Ihre Internet-Aktivitäten – ob mobil oder in Ihrer Kanzlei.

Mehr erfahren Sie unter www.annotext.de
Oder rufen Sie uns an: 0221 – 94373 6000

Mit Sicherheit besser beraten

Datensicherheit als kritischer Aspekt bei Mobilität und Vernetzung

Indem Rechtsanwaltskanzleien ihre geschäftlichen Abläufe zunehmend elektronisch abbilden und miteinander vernetzen, können sie von Rationalisierungspotenzialen profitieren. Mandantenakten und die interne Organisation werden in elektronischen Systemen geführt und sollen in vielen Fällen via Notebook, Tablet-PC oder Smartphone zugänglich sein. Solche digitalen Kommunikations- und Abwicklungsmöglichkeiten bringen Kostenersparnis, generieren Wettbewerbsvorteile und ermöglichen einen engen Kundenkontakt. Dem gegenüber stehen ernst zu nehmende Sicherheitsrisiken, die es zu minimieren gilt.

Mit der professionellen Kanzleiorganisationssoftware DATEV Anwalt classic pro zur Steuerung der Kanzlei und IT-Security-Lösungen hilft die DATEV eG dabei, den Gefahren aus dem Netz zu begegnen. Mit den Lösungen können sensible Daten, wie beispielsweise anvertraute Mandantendaten, im elektronischen Rechts- und Geschäftsverkehr effektiv gegen unbefugten Zugriff abgesichert sowie revisions- als auch archivierungssicher gespeichert werden. Auch bei mobiler Nutzung lassen sich die Daten wirkungsvoll und praktikabel schützen. Weitere Services zielen darauf ab, die Funktionsfähigkeit der IT-Infrastruktur zu gewährleisten.

Umfassende Leistungen rund um die Sicherheit

Ein Kernelement für den sicheren Zugang zum Internet ist DATEVnet pro. Eine zentrale Sicherheitszone bei DATEV schützt dabei die Anwender zuverlässig vor Viren, Trojanern oder Phishing-Versuchen. Die Mehrstufigkeit des Sicherheitssystems bedeutet auch bei neu auftretenden Angriffen schnellstmöglichen Schutz. Sollte dennoch einmal ein bisher unbekannter bösartiger Code durch das Netz schlüpfen, sorgt das Reverse-Scan-Verfahren für seine umgehende Enttarnung. Das DATEV Web-Radar hilft dabei, die Verbreitung von Schadcode durch präparierte Web-Inhalte einzudämmen. Dafür aktualisiert das Informationssystem permanent die Liste der bekannten mit Viren oder Trojanern verseuchten Seiten. Der Zugriff darauf wird bei DATEV zentral geblockt. Über den Dienst DATEVnet pro mobil lässt sich der sichere Zugriff von mobilen Endgeräten auf das eigene Netzwerk realisieren. Er setzt auf eine systematische, über das Rechenzentrum abgewickelte zentrale Verwaltung von Smartphones und Tablets sowie auf durchgängige Authentifizierungsverfahren.

Ist Ihre Kanzlei-IT wirklich sicher?

Mit dem **DATEV Sicherheitscheck** erfahren Sie es – schnell, kostenlos und selbstverständlich anonym. Mehr Informationen unter:

www.datev.de/sicherheitscheck

Über diese Infrastruktur können Kanzleiinhaber ihren Mitarbeitern auf Wunsch auch mit deren privaten Endgeräten einen abgesicherten Zugriff auf das Kanzleinetz ermöglichen. Um Heimarbeitsplätze sicher mit dem Kanzleinetzwerk zu verbinden, steht DATEVnet pro Telearbeitsplatz zur Verfügung. Damit sind Sie an Ihrem PC oder Notebook von überall sicher mit dem Büro verbunden.

E-Mails automatisch sicher

Mit der DATEV E-Mail-Verschlüsselung sind vertrauliche Daten auf Knopfdruck sicher. Beim Versenden wird die E-Mail automatisch so verschlüsselt, dass der Empfänger sie lesen kann. Eine Softwareinstallation ist dabei weder in der Kanzlei noch beim Empfänger erforderlich. Ebenso werden ankommende verschlüsselte Nachrichten zentral entschlüsselt, ohne die Abläufe in der Kanzlei zu behindern.

Für den Schutz von Datenbeständen vor Verlust oder Zerstörung bietet DATEV mit der „Datensicherung online“ ein Backup im Nürnberger Rechenzentrum an. Dabei erfolgt die Sicherung softwaregestützt und automatisch über eine abgesicherte Internetverbindung. Darüber hinaus gehören differenzierte IT-Beratungsleistungen zum Leistungsspektrum der DATEV.

→ Mehr Infos unter

- www.datev.de/anwalt-sicherheit
- Kontakt: anwalt@datev.de

REINERSCT

Bestens vorbereitet für den elektronischen Rechtsverkehr

Rechtsanwälte und Behörden sollen zukünftig u.a. Schriftsätze, Anträge und Erklärungen als elektronische Dokumente bei den Gerichten einreichen. Erforderlich für den Zugang zum elektronischen Gerichts- und Verwaltungspostfach (EGVP) sind neben einer Berechtigungskarte des Trustcenters ein Kartenlesegerät wie z.B. das preisgekrönte Chipkartenlesegerät cyberJack RFID komfort aus dem Hause REINER SCT.

Die Highlights:

- Elektronische ID-Funktion mit dem neuen Personalausweis (nPA)
- Qualifizierte elektronische Signatur (QES)
- Online-Banking via FinTS, Secoder, EBICS
- Geeignet für ELSTER, das elektronische Abfallnachweisverfahren und das Elektronische Gerichts- und Verwaltungspostfach (EGVP)
- Sicherheitsklasse 4
- Weitere Infos unter www.reiner-sct.com

Unverbindliche Preisempfehlung

159,90 € (inkl. MwSt.)

Business&IT 9.2014 HERVORRAGEND

reddot design award winner 2009

www.reiner-sct.com

DE-MAIL: RECHTSANWÄLTE KOMMUNIZIEREN SICHER DIGITAL

Vertrauliche Daten und Mandantenakten online versenden? Bislang mussten Anwälte Dokumente mit Rechtswirkung postalisch auf den Weg bringen. Mit De-Mail der Telekom geht das nun auch digital – einfach, sicher und nachweisbar.

Mandantenvereinbarungen, Rechnungen oder Verträge: Wer als Anwalt vertrauliche und rechtswirksame Dokumente verschickt oder empfängt, kann dies auch digital erledigen. Wie? Mit De-Mail der Telekom. Der Dienst ist so sicher wie die Briefpost und so einfach zu nutzen wie eine Mail. Anwälte können so schnell, einfach, sicher und nachweisbar mit ihren Mandanten kommunizieren. So sparen sie Kosten, gestalten Abläufe effizienter, reduzieren Aktenstapel auf ein Minimum – und heben nicht zuletzt die Servicequalität. Dabei ist ein per De-Mail versendetes Dokument ohne Unterschrift gültig.

AM PULS DER ZEIT

Einige Kanzleien nutzen bereits die Vorteile von De-Mail. So etwa die Luther Rechtsanwaltsgesellschaft. Als führende deutsche Wirtschaftskanzlei möchte sie in allen Bereichen am Puls der Zeit sein. Das gilt zum einen für die Spezialisierung auf zukunftsträchtige Beratungsfelder wie IT, Energy oder Healthcare. Vor allem aber passt die Firma ihre internen Strukturen an den digitalen Wandel an. Im elektronischen Austausch mit Mandanten nutzen die Rechtsanwälte und Steuerberater der Kanzlei De-Mail und gehen damit auf Nummer sicher. Denn Versender und Empfänger sind eindeutig identifiziert und die Zustellung erfolgt nachweisbar.

SCHNELL UND VERTRAULICH

Auch die Advofaktur Rechtsanwälte mit Standorten in Dresden und Zittau wollen künftig auf De-Mail setzen. Die Spezialisten für Immobilienrecht vertreten Bauherren und Bauträger, Eigentümer, Eigentümergemeinschaften, Verwalter, Vermieter und Mieter. Entscheidend für die Juristen: Die elektronische Kommunikation mit Mandanten, Gerichten, Rechtsschutzversicherern, Behörden und öffentlichen Einrichtungen muss nicht nur schnell, sondern auch vertraulich und sicher sein. Mit De-Mail der Telekom reduziert die Kanzlei ihren Bearbeitungsaufwand, da der Ausdruck und der postalische Versand der Dokumente entfallen.

VERSCHLÜSSELT UND NACHWEISBAR

Gesetzliche Grundlage von De-Mail ist das De-Mail-Gesetz. Darin ist festgelegt, dass nur zertifizierte Provider den Dienst anbieten dürfen. De-Mails werden nicht wie bei einer E-Mail üblich über das offene Netz übertragen, sondern verschlüsselt über ein sicheres, staatlich geprüftes System. So kann kein Dritter auf die Daten zugreifen, sie mitlesen oder manipulieren. Außerdem lassen sich Empfang und Versand einer De-Mail nachweisen. Dazu fordert der Sender eine Sende- und Empfangsbestätigung beim Provider an. Insbesondere bei Schreiben mit gesetzter Antwortfrist spielt dies eine große Rolle.

Weitere Informationen: **www.telekom.de/de-mail-anwaelte**

DIE DIGITALE KANZLEI
DOKUMENTENMANAGEMENT MIT DOCULIFE

Doculife bildet die Basis für ein klar strukturiertes, chronologisch geordnetes Ablagesystem und begünstigt den effizienten Informationsaustausch – innerhalb von Kanzleien genauso wie mit Mandanten und Partnern. Die Lösung ist mit §203 StGB für Berufsgeheimnisträger konform und erfüllt sämtliche Anforderungen an den Beschlagnahmeschutz vertraulicher Informationen. Die Dokumente befinden sich auf Servern in zertifizierten Rechenzentren innerhalb Deutschlands. Doculife schafft einen neuen digitalen Standard für ein sicheres und effizientes Dokumentenmanagement aus der Cloud. **www.t-systems.de/cloudportal**

10% RABATT FÜR DAVIT-MITGLIEDER*

DAV IT-RECHT
davit.de

T · · Systems ·

*Ihr individuelles Angebot zum Abschluss eines doculife® Law-Nutzungsvertrages erhalten Sie als davit-Mitglieder unter www.davit.de

Arbeitsgemeinschaft
IT-Recht im Deutschen Anwaltverein

Wir fördern die Aus- und Fortbildung sowie die Vernetzung der Kolleginnen und Kollegen, die sich mit Fragen des ITK-Rechts, des Multimediarechtes und mit Rechtsfragen im Bereich der digitalen Güter, Services und Medien befassen. Mit der davit Reihe der IT-Rechtstage treffen Sie uns im gesamten Bundesgebiet.

Die Anwaltschaft unterstützen wir bei der Bewältigung der Herausforderungen der elektronischen Kommunikation und IT-Sicherheit in der Anwaltskanzlei durch Workshops, Informationen und die davit-ITK Grundregeln.

Für nur 80,- € zusätzlich zum Jahresbeitrag Ihres örtlichen Anwaltsvereins vermitteln wir durch Fachtagungen, Seminare, Publikationen und intensiven Austausch unter den Mitgliedern Basis- und Spezialwissen. Vielfältige Kooperationen mit Verlagen und Lösungsanbietern sowie unser monatlicher Newsletter und Pressedienst runden das davit-Mitgliederangebot ab.

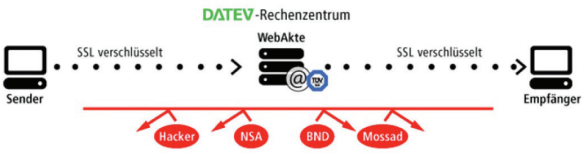
Schauen Sie mal vorbei.
www.davit.de/veranstaltungen

Wir freuen uns auf Sie!

Dr. Astrid Auer-Reinsdorff
Vorsitzende davit

DAV IT-RECHT
davit.de

Schnell wie eine E-Mail, aber so **sicher** wie ein Posteinschreiben.



Mehr als 10.000 Rechtsanwaltskanzleien, -kammern, -vereine, Versicherungen und Verbände vertrauen im elektronsichen Rechtsverkehr auf die WebAkte der e.Consult AG.

Testen Sie WebAkte jetzt 30 Tage kostenlos unter:
www.webakte.de

- **höchste Sicherheit**
- **einfach zu bedienen aus der Kanzleisoftware**
- **Flatrate schon ab 69,- Euro pro Kanzlei**

e.Consult® Aktiengesellschaft
WebAkte®
Empfohlen von: DeutscherAnwaltVerlag

e.Consult® Aktiengesellschaft
Robert-Koch-Str. 18 • 66119 Saarbrücken • Telefon: 0681 9508280
www.e-consult.de • www.e-consult.de

Bestellen Sie jetzt das Fachbuch zum Datenschutz – ein hochaktuelles Thema mit Beratungspotential!

Datenschutzrecht
in der anwaltlichen Beratung
Von RA Dr. Robert Kazemi
und Ri Dr. Anders Leopold
1. Auflage 2011,
488 Seiten, broschiert,
59,00 €
ISBN 978-3-8240-1107-0
Anwaltverlag-Titelnr.:
80347-69

Datenschutzrecht – vor wenigen Jahren noch ein Exot in der anwaltlichen Beratung – **gewinnt** für die tägliche Praxis **zunehmend an Bedeutung**. Das Thema steht dabei nicht nur **für große Unternehmen**, mit denen jüngste Daten-Skandale schnell in Verbindung gebracht werden, ganz oben auf der Agenda. Besonders **für Mittelständler und deren juristische Vertreter** steckt darin eine Brisanz, die bisher von vielen noch nicht oder nur unzureichend erkannt wird.

Datenschutzrecht in der anwaltlichen Beratung legt genau hier den Finger auf das mangelnde Problembewusstsein und liefert konkrete Hilfestellung für dieses sensible Thema.

Kompakt aufbereitet und direkt für die Beratung nutzbar, bereiten die Autoren eine Vielzahl von **konkreten Fallkonstellationen** auf, geben **wertvolle Praxishinweise** für die Beratung von Unternehmen, Gewerbetreibenden und Freiberuflern.

Das Werk bietet Antworten und **Beratungshinweise u.a. zu** folgenden Fragestellungen:

- **Wie hält es der Mandant mit der Nutzung von Internet am Arbeitsplatz?**
- **Welche Vorgaben sind beim Adressdatenhandel zu berücksichtigen?**
- **Wie erfolgt Datenschutz im Rahmen von Werbemaßnahmen?**
- **Wie können Compliance-Regelungen rechtssicher umgesetzt werden?**
- **Was ist bei Outsourcing-Maßnahmen zu beachten?**

Und: Nur hier finden Sie zudem den zwingend erforderlichen Bezug zu den benachbarten Rechtsgebieten, wie dem **Urheberrecht und Wettbewerbsrecht.**

Bestellen Sie schnell und bequem per Fax unter 0800/6611661, per Bestellhotline unter 0228/919110 oder online hier.

Einfach ausfüllen und faxen oder Ihrer Buchhandlung übergeben. Sie erhalten das Buch mit 4-wöchiger Ansichtsfrist. Preisänderung/Irrtum vorbehalten. Alle Preise inkl. MWSt. und zzgl. Versand. AGBs einzusehen unter www.anwaltverlag.de.

Hiermit bestelle ich den Titel „Datenschutzrecht in der anwaltlichen Beratung“:

Stempel oder Adresse

QX3

Datum _____ Unterschrift _____

Deutscher Anwaltverlag und Institut der Anwaltschaft GmbH
Wachsbleiche 7, 53111 Bonn

Geschäftsführer: Uwe Hagemann
Handelsregister: HRB Bonn 3417

DeutscherAnwaltVerlag