eBroschüre

Kazemi/Lenhard

Mit der freundlichen Unterstützung von:

DATEV

iDGARD
Sichere Mandantenkommunikation

Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

3. Auflage

978-3-8240-5777-1

DeutscherAnwaltVerlag

eBroschüre

Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

3. Auflage 2017

Von

Rechtsanwalt
Dr. Robert Kazemi
Bonn

und

Dr. Thomas H. Lenhard
Rodalben

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

Hinweis:
Die Ausführungen in diesem Werk 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. Herausgeber, Autoren und Verlag übernehmen keinerlei Haftung für die Richtigkeit und Vollständigkeit der in diesem Buch enthaltenen Ausführungen.

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

Copyright 2017 by Deutscher Anwaltverlag, Bonn
ISBN 978-3-8240-5777-1

DeutscherAnwaltVerlag

Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei

Inhalt

	Rdn
Editorial	
A. Datenschutz – Welche rechtlichen Rahmenbedingungen sind zu beachten	1
B. Pflicht zur Bestellung eines Datenschutzbeauftragten in der Anwaltskanzlei?	19
C. Keine Auskunftspflichten im Rahmen der Mandatsbearbeitung	32
D. Kommunikation und Datensicherheit	54
E. Voice-over-IP in der Anwaltskanzlei	83
F. Datenverlust trotz Datensicherung – Gefahren, die häufig unterschätzt werden	90
G. Warum Sie die Datenträger in Ihrer Kanzlei verschlüsseln sollten	97
H. Cloud-Computing und Weblösungen in der Anwaltskanzlei	105
I. Betriebssystem und Datenschutz	121
J. Beschäftigtendatenschutz – Grundlagen und ausgewählte Probleme	129
K. Die EU-Datenschutzgrundverordnung	187
Glossar	

Editorial

Seit der 2. Auflage dieser Informationsbroschüre ist erneut ein ganzes Jahr vergangen. In Sachen Datenschutz(recht) ist das Jahr 2016 durch zahlreiche Neuerungen gekennzeichnet, die eine Neuauflage des Werkes erforderlich machen.

Nicht nur die Entscheidung des EuGH in Sachen Safe-Habor, sondern allen voran, der noch im Dezember 2015 voran getriebene Abschluss der Verhandlungen über eine neue Datenschutzgrundverordnung (DSGVO), sind Meilensteine im Datenschutzrecht.

Mit der DSGVO kommen auch auf uns Rechtsanwälte zahlreiche Neuerungen zu; nicht nur in der anwaltlichen Beratung, sondern auch im Rahmen der eigenen Büroorganisation. Vieles ist – wie bei neuen Gesetzen üblich – noch nicht abschließend geklärt und wird sich bis zum Wirksamwerden der Neuregelungen im Sommer 2018 sicherlich konkretisieren; viele Anforderungen der DSGVO lassen bereits jetzt hellhörig werden und erfordern entsprechende Aufmerksamkeit.

Leider ist ein erster Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU), der im September „geleakt" worden war, bereits wieder zurückgezogen worden: hier war in den eigenen Reihen (zwischen den Ministerien) schnell erhebliche Kritik aufgekommen, bevor wissenschaftlich eine ernsthafte Auseinandersetzung mit dem Referentenentwurf des Bundesministeriums des Innern überhaupt erfolgen konnte. Der Referentenentwurf sah – in den durch die DSGVO belassenen Grenzen – die Aufrechterhaltung zahlreicher Bestimmungen des BDSG neben der DSGVO vor. Der EU-Gesetzgeber hat den Nationalstaaten derartige Möglichkeiten belassen und die DSGVO in zahlreichen Bereichen mit sog. **Öffnungsklauseln** versehen, die – entgegen dem, einer EU-Verordnung eigentlich zukommenden, Zweck der unmittelbaren Vollharmonisierung – weiterhin Raum für nationale Alleingänge geben. Offenbar aus Angst, eine ungefilterte Anwendung der DSGVO könne das hohe Datenschutzniveau in Deutschland herabsenken, scheint die Bundesregierung bzw. das federführende BMI hier in jedem Fall noch handeln zu wollen.

Wir hätten dazu gerne Stellung genommen, sehen dies jedoch angesichts der unklaren Rechtslage bislang (noch) nicht als sinnvoll an. Sicherlich werden wir im Rahmen der Aktualisierung dieses Werkes im kommenden Jahr ausführlicher auf etwaige deutsche Sonderwege eingehen und diese noch rechtzeitig vor Wirksamwerden der DSGVO beleuchten und bewerten.

In der vorliegenden Auflage unseres Werkes beschränken wir uns darauf, Ihnen einen kurzen Überblick über die Neuregelungen zu vermitteln und insbesondere mögliche Auswirkungen auf das rechtsanwaltliche Wirken zu beleuchten. Wir laden Sie ganz herzlich zu einer breiten Diskussion der dadurch aufgeworfenen Fragen ein!

Doch nicht nur auf rechtlicher, sondern auch auf technischer Ebene ergaben sich im Jahr 2016 zahlreiche Neuerungen, auf die wir an den entsprechenden Stellen näher eingegangen sind. Herr Dr. Lenhard konnte in diesem Zusammenhang auf zahlreiche Praxisbeispiele zurückgreifen und die hieraus erwachsenden Problemlagen näher beleuchten.

Wie bereits seit der Erstauflage dieses Werkes verfolgen wir weiterhin das Ziel, Sie nicht nur mit Problemen zu konfrontieren, sondern auch mögliche Lösungswege aufzuzeigen.

Wir hoffen, dies ist auch in der aktuellen Auflage wieder gelungen und wünschen Ihnen viel Spaß beim Durcharbeiten des Werkes.

Mit freundlichen kollegialen Grüßen

Dr. Robert Kazemi

A. Datenschutz – Welche rechtlichen Rahmenbedingungen sind zu beachten

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. 1

§ 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. 2

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 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. 3

§ 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). 4

§ 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. 5

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. 6

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 mindestens 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. 7

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. 8

§ 2 BORA

Unter dem 1.7.2015 ist eine umfassende Neuregelung des § 2 BORA in Kraft getreten, mit der das sog. „non-legal outsourcing" berufsrechtlich geregelt wird. Bereits zuvor regelt § 2 BORA die berufsrechtliche Pflicht zur Verschwiegenheit des Rechtsanwaltes. Diese war hier indes „absolut" ausgestaltet, jede Durchbrechung erforderte zwingend die Zustimmung des Mandanten. Die Rechtsanwaltschaft sah hierin ein Problem, nachdem die zunehmende Technisierung des beruflichen Alltages zunehmend den Einsatz externer Dienstleister in der Kanzlei erforderlich macht. Hier jedes Mal eine konkrete Einwilligung einzuholen, erschien da kaum praktikabel. Die BRAK hatte zunächst versucht, dieses Problem gänzlich über die Neuregelung des § 2 BORA zu entschärfen und die Grenzen der anwaltlichen Verschwiegenheitspflichten zugunsten „sozialadäquater" Verhaltensweisen zu erweitern, war aber mit diesem Vorhaben am Widerstand des BMJ gescheitert. Nachdem dieses der geplanten Änderung des § 2 BORA zunächst gänzlich widersprochen hatte, ist die Neuregelung zwar zum 1.7.2015 in Kraft getreten; sie betrifft indes allein die berufsrechtliche Bewertung und hat ausdrücklich keine Auswirkungen auf die strafrechtliche Beurteilung. Insoweit fehlt der BRAK schlicht die Kompetenz dazu, Erlaubnistatbestände im Sinne des § 203 StGB zu schaffen.[1] Daher ist grundsätzlich auch weiterhin eine Einwilligung des Mandanten erforderlich, wenn die Einschaltung externer Dienstleister erwogen wird. Berufsrechtlich soll ein Verstoß gegen die Verschwiegenheitspflicht indes nicht anzunehmen sein, wenn die Bekanntgabe „im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter er- 9

1 Vgl. http://anwaltsblatt.anwaltverein.de/de/news/non-legal-outsourcing-bora-kommt-nun.

folgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)“ (§ 2 Abs. 3 lit. a BORA). Nimmt der Rechtsanwalt die Dienste von Unternehmen in diesem Sinne in Anspruch, hat er diesen Unternehmen aufzuerlegen, ihre Mitarbeiter zur Verschwiegenheit zu verpflichten, soweit die dienstleistenden Personen oder Unternehmen nicht kraft Gesetzes zur Geheimhaltung verpflichtet sind oder sich aus dem Inhalt der Dienstleistung eine solche Pflicht offenkundig ergibt.

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),[2] dass es zum Wesen der Berufstätigkeit des Rechtsanwaltes gehört, 10

> *„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.“*

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). 11

§§ 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). 12

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.

Neben dem Berufsrecht gelten die Datenschutzgesetze

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 13

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

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. Insbesondere 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.[3]

Die herrschende Meinung[4] 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. **14**

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. **15**

Telemediengesetz (TMG)

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. Auch hier hat sich erst kürzlich eine Änderung in den Anforderungen ergeben, die leider weitgehend unbeachtet geblieben ist. So ist am 25.7.2015 das sog. IT-Sicherheitsgesetz[5] in Kraft getreten mit dem „eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden"[6] soll. Zwar zielt das Gesetzespaket mit Änderungen im BSI-Gesetz vorgreiflich auf Betreiber sog. Kritischer Infrastrukturen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen (§ 2 Abs. 10 Nr. 1 BSI-Gesetz) und scheint damit für Rechtsanwälte auf den ersten Blick nicht relevant. Dennoch bringt die Gesetzesnovelle auch Änderungen im TMG mit sich, die sich im neuen § 13 Abs. 7 TMG niederschlagen. Dieser verpflichtet „Diensteanbieter" dazu, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener **16**

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

4 *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.

5 BGBl I, 24.7.2015, S. 1324 ff.

6 BT-Drucks 18/4096, S. 1.

Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen in diesem Sinne müssen

den Stand der Technik berücksichtigen. Eine Maßnahme ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens (beispielsweise https-Verschlüsselung). In der Gesetzesbegründung heißt es hierzu: „Ein wesentliches Ziel der Regelung ist es, einen der Hauptverbreitungswege von Schadsoftware einzudämmen: das unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads). Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software (Einspielen von Sicherheitspatches) seitens der Websitebetreiber könnten zahlreiche dieser Angriffe vermieden werden. Kompromittierungen können zudem auch durch Inhalte erfolgen, auf die der Diensteanbieter keinen unmittelbaren technischen Einfluss hat (zum Beispiel über kompromittierte Werbebanner, die auf der Webseite eingebunden sind). Dagegen sind organisatorische Vorkehrungen zu treffen. Hierzu zählt beispielsweise, Werbedienstleister, denen Werbefläche eingeräumt wird, vertraglich zu notwendigen Schutzmaßnahmen zu verpflichten. Die entsprechenden Maßnahmen sind im Rahmen der jeweiligen Verantwortlichkeit zu treffen." Auch wenn der Fall der Fremdwerbung auf Internetseiten des Rechtsanwaltes schon aus berufsrechtlichen Regelungen nicht in Betracht kommt, kann die Relevanz dieser Bestimmung auch für den Rechtsanwalt nicht gänzlich abgesprochen werden. Man denke insoweit nur an die Kollegen, die ein sog. Content Management System (CMS) zur Erstellung und Pflege Ihrer Webseiten nutzen. Hier wird wohl zumindest die regelmäßige Aktualisierung der CMS-Software gefordert werden. Ebenso dort, wo Newsletterfunktionen im Einsatz sind. Mit Blick auf die Anordnung des Gesetzes stellen sich hier nicht nur datenschutzrechtliche, sondern auch deliktsrechtliche Fragen. So zum Beispiel, wenn es – mangels Aktualisierung – tatsächlich zu einer Verbreitung von Schadsoftware über die Webseiten des Rechtsanwaltes kommt. Dieser betreibt insoweit mit seiner Kanzleiseite einen „Telemediendienst" und wäre hier – wollte man die Haftung tatsächlich so weit reichen lassen – ggf. voll verantwortlich.

Telekommunikationsgesetz (TKG)

Das TKG sieht 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. **17**

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.[7] 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[8] 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,[9] die vor allem im Rahmen der sogenannten Massenabmahnungsfälle Bedeutung erlangen. Ebenfalls von zentraler Bedeutung ist **18**

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

8 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.

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

§ 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.

B. 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.[10] 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.[11] 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. Daher ist § 4f BDSG nach hiesiger Meinung auch von Rechtsanwälten zu beachten. 19

Externe Bestellung eines Datenschutzbeauftragten zulässig 20

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[12] – gerade nicht erforderlich. Auch die im BDSG normierten Aussageverweigerungsrechte, Beschlagnahme- und Verwertungsverbote gelten ebenso für den internen, wie für den externen Datenschutzbeauftragten.

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[13] stellt hier hohe Mindestanforderungen. 21

10 Zahlen der RA MICRO.

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

12 Siehe hierzu den Beitrag „Outsourcing" in der Rechtsanwaltskanzlei – Ein Berufs- und strafrechtliches Problem?

13 Das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich.

Unabhängig von der jeweiligen Branche und Größe des Unternehmens muss jeder Datenschutzbeauftragte über erhebliches Wissen im Datenschutzrecht verfügen. Dies umfasst u.a. 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. 22

Der DAV[14] 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. 23

Anforderungen an den und Aufgaben des Datenschutzbeauftragten 24

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.

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. 25

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 Ver- 26

14 Http://www.anwaltverein.de/downloads/praxis/mustervertrag/ChecklisteDatenschutz.pdf.

pflichtung, sich durch geeignete Fortbildungen und das Studium aktueller Gesetzgebungsvorhaben auf dem Laufenden zu halten.

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. 27

Die Bestellung eines externen 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. 28

Wen trifft die Verpflichtung zur Bestellung eines Datenschutzbeauftragten? 29

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.

Die Pflicht gilt, sobald **mindestens 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. 30

Sobald innerhalb einer Rechtsanwaltskanzlei damit ständig mehr als 10 Personen, einschließlich des anwaltlichen Hilfspersonals, Zugriff auf die elektronische Mandantenverwaltung 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). 31

C. 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 32

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.[15]

Die herrschende Meinung[16] 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. 33

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. 34

Auskunfts- und Benachrichtigungspflichten gegenüber dem Mandanten? 35

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.

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 Mandanten einholt. In diesem Fall wären die zu diesem Zwecke erhobenen personenbezogen Daten des potenziellen Mandanten, sollte es 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. 36

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

16 *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.

Personenbezogene Daten der gegnerischen Partei oder sonstiger Dritter 37

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.

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. 38

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. 39

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. 40

Keine Auskunftspflichten gegenüber Datenschutzkontrollinstanzen 41

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.

Vor allem die Datenschutzbeauftragten der Länder[17] 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. 42

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.[18] 43

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. 44

Sonderproblem: „Onlinebestellungen" von Kanzleimaterialien 45

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.

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 46

17 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.

18 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.".

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.[19] 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.

47 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.

48 Nach nicht rechtskräftiger Auffassung des FG Nürnberg[20] 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 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 herbei-

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

20 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.

zuführen. Wenn er diesbezüglich „seine Hausaufgaben“ nicht gemacht habe, könne er hiermit eine zulässige Prüfungshandlung nicht blockieren.

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.[21] 49

Mit Urt. v. 28.10.2009[22] 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. 50

Die Entscheidung des FG Nürnberg,[23] 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. 51

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. 52

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. 53

D. 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. 54

WLAN in der Kanzlei 55

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 An-

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

walt 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) zurückgegriffen 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.

Beim Einsatz neuerer Router und insbesondere beim Einsatz selbstkonfigurierender oder vorkonfigurierter Geräte ist ebenfalls Vorsicht geboten. Einige dieser Geräte werden mit einem vorbereiteten Gastzugang ausgeliefert. Das entspricht faktisch einem vollständig offenen WLAN. Wird dieser Gastzugang dann nicht explizit deaktiviert, steht er jedem in Reichweite befindlichen WLAN-Nutzer zur Verfügung. Es sind bereits Fälle bekannt, bei denen der Gastzugang solcher Router für kriminelle Aktivitäten genutzt wurde.

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.[24] 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 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.[25] **56**

Sonstiger Systemschutz **57**

Virenscanner und Firewalls bieten einen relativen Schutz Ihrer Systeme. Die Anwender sind jedoch immer aufgefordert, verantwortungsvoll mit Technik und personenbezogenen Daten umzugehen, so haben z.B. private USB-Datenträger an einem beruflich genutzten System nichts zu suchen. Was den meisten Lesern eigentlich als selbstverständlich erscheint, ist allerdings eine der größten Gefahren. So sind aus der Praxis durchaus Fälle bekannt, in denen sich Mitarbeiter über die technische Sperrung von USB-Da-

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

tenträgern beschwert haben, weil sie ihren Kolleginnen und Kollegen die neuesten Urlaubsbilder nicht präsentieren konnten. Wird solch 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 E-Mail-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 verwendet wird. In einigen Fällen ist bei einer solchen Infektion aufgefallen, dass die Systeme langsamer reagierten, als das gewöhnlich der Fall war. Andere Systeme sind dadurch aufgefallen, dass permanente Zugriffe auf die Festplatte erfolgten, die anhand einer LED an der Frontseite des Rechners bemerkt wurden. 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. 58

Aktuelle Bedrohungen 59

Ein Blick in den Spamfilter eines Emailservers oder auch in die gelöschten Dateien oder die ungefilterten Emaileingänge zeigt uns, dass immer noch zahlreiche Spam-Mails versendet werden, die ganz speziell uns „persönlich“ offerieren, uns einige Millionen Dollar zu schenken, die man zufällig im Keller einer Bank entdeckt hat und von denen keiner der Beteiligten eine Idee hat, was man damit anfangen könnte. Eigentlich trägt ein derartiger Blödsinn, noch dazu erkennbar mit automatischen Übersetzungsprogrammen in unsere Sprache übertragen, eher zur Belustigung bei. Allerdings dürfte den meisten Empfängern nicht mehr zum Lachen zumute sein, wenn sie bedenken, welche kriminellen Absichten sich hinter einer solchen Mail verstecken. Und spätestens wenn die Geschichte zum 100sten Mal zum Überlauf des ohnehin prall gefüllten Postfachs des Empfängers beiträgt, kann darüber niemand mehr lachen.

Hinsichtlich der Datensicherheit haben die Kanzleien in den letzten Jahren deutlich aufgerüstet. Allerdings ist auch die Entwicklung im kriminellen Sektor der Internetnutzung nicht stehen geblieben. Statt der dümmlichen Geschichte vom gefundenen Geld, gehen nämlich mittlerweile sehr professionell aufgebaute E-Mails mit anhängenden Schadprogrammen ein, die selbst für IT-Sicherheitsexperten auf den ersten Blick nur schwer zu erkennen sind. Die Bedrohung einer Kanzlei ist dabei dermaßen schwerwiegend und zielgerichtet, dass diesem Thema hier ein eigener Abschnitt gewidmet wird. 60

Einige Kanzleien haben mit der neuesten Methode krimineller Subjekte bereits unangenehme Erfahrungen sammeln können. Dabei nehmen Kriminelle im Betreff einer E-Mail Bezug auf Stellenausschreibungen der Kanzlei und senden eine vermeintliche Bewerbung als E-Mail-Anhang. In einem dieser Fälle, die in jüngster Vergangenheit bekannt wurden, wurde sogar vor dem Öffnen des Anhangs überprüft, ob es sich bei dem angeblichen Absender tatsächlich um eine reale Person bzw. um einen möglichen Bewerber handeln könnte. Den vermeintlichen Absender gab es wirklich! Er hatte allerdings die Nachricht nicht selbst verschickt. Statt dann beim Anklicken des Anhangs wie erhofft Bewerbungsunterlagen lesen zu können, wurde der gesamte Online-Datenbestand der Kanzlei verschlüsselt und die Kanzlei erhielt hiernach eine Lösegeldforderung. 61

Betroffene sollten das Lösegeld in keinem Fall zahlen. Zwar wird vereinzelt in diversen Online-Medien von Fällen berichtet, in denen tatsächlich nach Zahlung des Lösegelds ein Programm zur Entschlüsselung 62

der Daten zur Verfügung gestellt worden sein soll. Hier stellt sich jedoch die grundlegende Frage, wieso Kriminelle, die eine sehr gut durchdachte Vorgehensweise zeigen, sich der zusätzlichen Gefahr der Identifizierung aussetzen sollten, in dem Sie nach Erhalt des erpressten Geldes erneut eine E-Mail an Ihr Opfer senden.

Wie sollte man sich verhalten, wenn man auf diese Weise erpresst wird und die Datenbestände verschlüsselt wurden? 63

Sie sollten einerseits die Polizei informieren, die mittlerweile über hervorragende Computerforensiker verfügt. Für eine Vielzahl von Verschlüsselungsviren bieten mittlerweile die Hersteller von Antivirenprogrammen auch Werkzeuge an, mit denen Sie die Verschlüsselung rückgängig machen können. Sie sollten nicht selbst versuchen, Ihre Datenbestände zu entschlüsseln und diesbezüglich immer auf einen Experten zurückgreifen. Vorsicht ist auch geboten, wenn Sie im Internet nach Entschlüsselungsprogrammen suchen. Falls Sie bei der Suche nämlich nicht auf die seriöse Seite eines Herstellers von Antivirensystemen oder auf eine sonst als vertrauenswürdig bekannte Seite stoßen, ist durchaus möglich, dass das erhoffte Entschlüsselungsprogramm sich wiederum als neues Datenverschlüsselungsprogramm erweist. Gerade dann, wenn bereits das System der Kanzlei verschlüsselt ist und man unter Zeitdruck versucht, dem Abhilfe zu schaffen, ist die Gefahr besonders groß, in die nächste Fußangel Internetkrimineller zu treten.

Wie kann ich die Kanzlei vor einer solchen Attacke wirksam schützen? 64

Der wirksamste Schutz vor solchen Attacken ist die Prävention. Im konkreten Fall besteht diese darin, dass Sie immer aktuelle **Datensicherungen** offline zur Verfügung haben. „**Offline**“ deswegen, weil einige Verschlüsselungsviren die äußerst negative Angewohnheit haben, sämtliche verknüpften Netzlaufwerke zu verschlüsseln, was mitunter dann ebenfalls Datensicherungen auf laufenden Systemen betrifft.

Eine weitere aktuelle Bedrohung für die Systeme einer Kanzlei ist das seit Jahren praktizierte und ebenfalls immer ausgefeilter werdende „**Social Engineering**“. Dabei werden dem Angerufenen die unterschiedlichsten Geschichten „aufgetischt“. Ähnlich wie bei Mails mit Schadsoftware, werden auch hier die Geschichten und Methoden immer professioneller. Aber vollkommen unabhängig davon, welche Geschichte erzählt wird, ist der Ablauf einer solchen Attacke in der Regel gleich: Man versucht Sie dazu zu bewegen, irgendetwas im Internet aufzurufen, anzuklicken oder herunter zu laden. 65

Wieso sollen sich Kriminelle noch damit aufhalten, mühsam in Systeme einzubrechen, wenn der Angerufene bereitwillig die Installation des erforderlichen Trojaners oder Schadprogramms selbst vornimmt? 66

Sehr häufig geben sich die Anrufer als Vertreter bekannter Internet-, Software- oder Kommunikationskonzerne aus. Üblicherweise werden bei den Anrufen Nummern unterdrückt oder es werden recht exotische Telefonnummern wie z.B. aus Samoa, Papua Neuguinea oder aus dem Libanon angezeigt. Vorsicht ist in jedem Fall auch geboten, wenn sich der Anrufer als Mitarbeiter eines Konzerns ausgibt und seine Rufnummer anhand der Vorwahl als Mobilfunknummer identifiziert werden kann.

E-Mail-Kommunikation 67

E-Mail ist per se ein unsicheres Kommunikationsmedium. Selbst wenn Sie zu einem externen Provider eine SSL- oder TLS-Verschlüsselung nutzen, was seit Ende des Jahres 2013 von vielen E-Mail-Providern gefordert wurde, so ist zwar die Kommunikation zwischen Ihrem Rechner und dem E-Mail-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. Dass derartige Unterfangen illegal sind, verhindert nicht deren Existenz.

68 Ein weiterer Fallstrick, der sich im Umgang mit E-Mail zeigt, ist die Fähigkeit der meisten gängigen Mailprogramme, eine einzelne E-Mail gleichzeitig an mehrere Empfänger zu versenden. Soweit ein eingesetztes Programm über eine verknüpfte Adressdatenbank verfügt, die dann mitunter automatisch die E-Mail-Adressen ergänzt, werden hier unter Umständen personenbezogene Daten mitgeteilt, deren Weitergabe weder gewünscht noch legitimiert ist. Das heißt, dass eventuell E-Mail-Adressen, die sonst vielleicht noch keinen Rückschluss auf den Nutzer zulassen würden, automatisch um den vollständigen Namen ergänzt werden. Geht z.B. eine E-Mail an die Adresse koksnase@irgendeinprovider.de, so würde diese E-Mail-Adresse eventuell um den vollständigen Namen aus der Datenbank des E-Mail-Programms ergänzt und würde, soweit sich die Adresse unter der Versendekategorie „CC“ oder „AN“ befindet, an alle anderen Empfänger ebenfalls vollständig übermittelt werden. E-Mail-Adressen sind personenbezogene Daten und daher sollte tunlichst vermieden werden, dass diese unbedacht weiter gegeben werden. Letzteres wäre dann nämlich der Fall, wenn zehn oder zwanzig E-Mail-Empfänger sich allesamt unter den Versendekategorien „CC“ (Kopieempfänger) oder „AN“ (Primäre E-Mail-Empfänger) befinden würden. Es geht also nicht nur darum, keine vollständigen Namen der E-Mail-Empfänger zu versenden, sondern vielmehr darum, ggf. gar keine Informationen zu anderen E-Mail-Empfängern jedem einzelnen Adressaten zukommen zu lassen. Die meisten E-Mail-Programme verfügen daher auch über die Funktion einer Blindkopie („BC“). Soweit eine E-Mail-Adresse darin eingetragen wird, ist diese für andere E-Mail-Versender nicht sichtbar, weil jede Blindkopie separat vom E-Mail-System versendet wird, auch wenn es so aussieht, als würde nur eine E-Mail gesendet werden. Bedauerlicherweise begrenzen viele E-Mail-Programme die Anzahl der gleichzeitig versendbaren Blindkopien, so dass hier eventuell eine Nachricht mehrfach versendet werden muss und jeweils andere Blindkopieempfänger angegeben werden müssen. Ein E-Mail-Server, der dem Stand der Technik entspricht, kann hier Abhilfe schaffen und die Versendung von einer größeren Zahl an Blindkopien organisieren. Beachten sollte man aber auch, dass ggf. ein Empfänger im Feld „AN“ bei vielen E-Mail-Systemen immer erforderlich sein könnte, um Blindkopien versenden zu können. Hier kann man relativ einfach Abhilfe schaffen, indem man seine eigene E-Mail-Adresse (Versender) als primären Empfänger der E-Mail einträgt. In diesem Zusammenhang wird auch darauf hingewiesen, dass das Hochladen kompletter E-Mail-Datenbanken in ein soziales Netzwerk u.U. eine zweckfremde Verwendung in Form der Weitergabe von personenbezogenen Daten darstellt, die i.d.R. ohne Zustimmung der Betroffenen erfolgt. Gehen Sie also sehr sorgsam mit den E-Mail-Adressen um.

69 Die 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 versenden, so ist darauf zu achten, dass eine nach dem Stand der Technik als sicher angesehene Verschlüsselung zum 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. Dabei sollte aber keinesfalls vergessen werden, dass eine Ende-zu-Ende-Verschlüsselung erforderlich ist, was üblicherweise mit einem Mandanten abgestimmt werden müsste.

De-Mail als Alternative? 70

Eine Alternative zur „einfachen" E-Mail bietet das sog. **De-Mail-Verfahren**.[26] Die De-Mail ist ein durch Bundesgesetz geregeltes Kommunikationsverfahren über das „auf einer elektronischen Kommunikationsplattform" ein „sicherer, vertraulicher und nachweisbarer Geschäftsverkehr für jedermann im Internet sichergestellt" werden soll (§ 1 Abs. 1 De-Mail-Gesetz). De-Mail-Dienste dürfen vor diesem Hintergrund nur von akkreditierten Diensteanbietern betrieben werden (§ 1 Abs. 2 S. 2 De-Mail-Gesetz), die die im De-Mail-Gesetz aufgestellten Sicherheitsanforderungen erfüllen. Zu diesen Anbietern zählen neben der Deutschen Telekom, u.a. Francotyp-Postalia sowie United Internet mit ihren Angeboten1&1, Web.de und GMX.[27] Glaubt man den Ausführungen des Beauftragten der Bundesregierung für Informationstechnik, scheint die De-Mail die (!) sichere Lösung für die anwaltliche Kommunikation zu sein. Denn „*De-Mails sind auf dem Transportweg immer verschlüsselt und werden verschlüsselt abgelegt. Ein Mitlesen oder Verändern einer De-Mail ist nicht möglich.*"[28] Eine klare und deutliche Aussage. Gleichwohl steckt der Teufel auch hier im Detail. Denn der Beauftragte der Bundesregierung für Informationstechnik spricht hier nicht von einer generellen, sondern nur von einer sog. Transportverschlüsselung, die das „Mitlesen oder Verändern" einer De-Mail auf dem Wege zum Empfänger durch Dritte verhindert. Doch ist wirklich jeder Dritte ausgeschlossen? Ein Blick in die De-Mail Leistungsbeschreibung beispielsweise der Deutschen Telekom verrät, dass dem nicht so ist. So sehen die De-Mail-Anbieter einen sog. Postfach-Schutz (vgl. Ziffer 2.2.6. der De-Mail Leistungsbeschreibung der Telekom[29]) vor, über den „alle über De-Mail versandten De-Mails automatisch auf evtl. Viren oder Malware überprüft" werden. „Vom System als auffällig klassifizierte De-Mails werden dem Kunden in einen besonderen Ordner seines De-Mail-Postfachs zugestellt. Erkennt das System bereits bei beim Versand eine Schadsoftware in der zu versendenden De-Mail, wird die Nachricht nicht zugestellt und der Kunde informiert." Dieser Scan mag Vorteile haben, er bedingt indes, dass die auf dem Server abgelegten De-Mails selber nicht verschlüsselt abgelegt werden; denn eine verschlüsselte Datei kann nicht auf Viren geprüft werden. Ein gewisses, wenn auch geringes, Sicherheitsrisiko verbleibt insoweit. Dieses verbleibt auch, soweit der De-Mail-Anbieter verpflichtet sein kann, „Daten an staatliche Stellen zu übermitteln, wenn dies gesetzlich vorgeschrieben ist bzw. ein entsprechender Gerichtsbeschluss vorliegt (z.B. im Rahmen der Strafverfolgung oder der Terrorismusbekämpfung)".[30] Wer hier ganz auf „Nummer sicher" gehen wollte, dem war der Weg in die De-Mail bis Mitte diesen Jahres verschlossen. Hier wurde indes zwischenzeitlich nachgebessert und die De-Mail für die sog. Ende-zu-Ende-Verschlüsselung geöffnet. Die Verschlüsselung basiert auf dem sog. PGP (**Pretty Good Privacy)-Verfahren**.[31] Den Kollegen, die auf De-Mail setzen, ist der Einsatz dieser Technik dringend zu empfehlen.

Natürlich stellt sich vor dem Hintergrund vieler Enthüllungen und zahlreicher Vorstöße durch die Innen- 71
minister 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

26 Eine ausführliche Darstellung der De-Mail findet man beim BMI, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/de_mail_072012.pdf?__blob=publicationFile.

27 Eine vollständige Liste der akkreditierten Anbieter ist unter http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/Gesetzlich-geregeltes-Sicherheitsniveau/gesetzlich_geregeltes_sicherheitsniveau_node.html;jsessionid=51C8380BE4A6B074F52828A781EDE3DD.2_cid324 abrufbar.

28 Http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html.

29 Abrufbar unter: http://www.telekom.de/dlp/agb/pdf/43269.pdf.

30 So beispielsweise die Datenschutzhinweise für De-Mail der Telekom Deutschland GmbH, abrufbar unter: http://www.telekom.de/is-bin/INTERSHOP.enfinity/WFS/EKI-TELEKOM-Site/de_DE/-/EUR/ViewAGB-Start?AGBID=1162&Char=D&ArchivOnly=.

31 Vgl. hierzu: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2015/03/de-mail-ende-zu-ende-verschluesselung-kommt.html; siehe auch: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2015/08/internetprovider-bieten-ende-zu-ende-verschluesselung.html.

Kriminelle im Internet dürfte es jedoch ungleich schwieriger werden, sich bei Verwendung von De-Mails Informationen zu beschaffen.

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 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 ausreichend auf Vertrauenswürdigkeit und Zuverlässigkeit überprüft wurde oder ob es sich um den Mitarbeiter irgendwelcher Personalvermittler oder Subunternehmer handeln könnte, konnte im Rahmen der Recherche zu dieser Publikation nicht ermittelt werden. Eine Nachfrage bei der Deutschen Telekom AG hat ergeben, dass dort ein dem Postident vergleichbares Verfahren angeboten wird, bei dem man sich in einem Telekom-Shop oder in einem Hermes PaketShop identifizieren kann. Auf Wunsch des Nutzers kann auch ein Telekom-Mitarbeiter in die Kanzlei kommen, so dass hier drei Alternativen der Identifizierung angeboten werden. Alles in allem bietet De-Mail mit der Rechtssicherheit in Bezug auf Datenschutz und Zustellung wesentliche Vorteile bei gleichzeitig einfacher Nutzung und wird daher zum sicheren und schnellen Datenaustausch empfohlen. 72

Für denjenigen, der sich für De-Mail entscheidet, ist noch wichtig zu wissen, dass die De-Mail nicht einfach ein „Add-On" zur bestehenden Kanzleiadresse, sondern eine „neue" eigene Mailadresse darstellt. Wer sich hier also daran gewöhnt hat, über seine Mailserver und seine Domäne „@rechtsanwalt-mustermann.de" E-Mails zu versenden, der wird dies über die De-Mail nicht mehr tun können, sondern ist auf die Nutzung der Domain des jeweiligen De-Mail-Anbieters (beispielsweise „@t-online.de-mail.de") angewiesen. Auch gilt es zu beachten, dass die De-Mail auf den innerdeutschen Kommunikationsverkehr gerichtet ist. Wer also viel mit ausländischen Mandanten kommuniziert, sollte sich nach einer anderen Lösung umsehen. Auch, wer regelmäßig große Datenmengen versendet, sollte das Kleingedruckte lesen. So bietet die Basis-Version der De-Mail bei der Telekom beispielsweise nur die Möglichkeit der Übermittlung von Anhängen bis zu 10 MB an. 73

E-POSTBRIEF als Alternative 74

Seit 2010 bietet auch die Deutsche Post AG eine neue Versendungsform an, den sog. E-POSTBRIEF. Dieser bietet – ebenso wie die De-Mail – eine Möglichkeit der sicheren elektronischen Kommunikation und schafft für den Nutzer eine Alternative zur „normalen" E-Mail-Kommunikation. Die Teilnahme am E-POSTBRIEF erfordert die vorherige Registrierung mittels POSTIDENT-Verfahren;[32] eine anonyme Registrierung, wie sie bei vielen klassischen E-Mail-Anbietern durchaus möglich ist, scheidet damit aus. Die Nutzerdaten können als vielmehr authentifiziert angesehen werden, so dass grundsätzlich[33] davon ausgegangen werden kann, dass der Versender eines E-POSTBRIEFES auch tatsächlich der dort benannte Absender ist.[34] Zur Überprüfung der Postadresse des Nutzers wird dem Nutzer nach der Aktivierung eine AdressTAN an die von ihm angegebene Postadresse klassisch zugesendet, die anschließend im

32 Leistungsbeschreibung E-POSTBRIEF, abrufbar unter: http://www.epost.de/content/dam/dp/dokumente/leistungsbeschreibung.pdf.

33 Freilich mit der Ausnahme der „unbefugten" Verwendung des E-POSTBRIEFES durch von Inhaber nicht autorisierte Nutzer. Hierfür müssten diesen jedoch die Zugangsdaten durch den Berechtigten bekannt gegeben werden.

34 Insoweit ergeben sich hier Vorteile auch zum normalen Brief, der grundsätzlich auch mit „falscher" oder gänzlich ohne Absenderkennung aufgegeben werden kann.

POSTBRIEF Portal eingegeben werden kann.[35] Die anschließende Nutzung des E-POSTBRIEFS erfordert die zusätzliche Vergabe eines Passwortes durch den Nutzer.[36] Grundsätzlich erfolgt die Übermittlung von E-POSTBRIEFEN in der Folge nur zwischen E-POSTBRIEF Adressen registrierter und identifizierter Nutzer, diese können hier noch zwischen verschiedenen Varianten wählen, insbesondere können E-POSTBRIEFE „mit hohem Ident-Nachweis" übermittelt werden. In diesem Fall erfordert der Versand eines E-POSTBRIEFS nicht nur die Anmeldung des Nutzers am Portal,[37] sondern die Eingabe einer HandyTAN, die dem Nutzer jeweils vor Übermittlung an die bei der Online- Registrierung angegebene Mobilfunknummer übermittelt wird. Anders als dies bei der De-Mail der Fall ist, bietet der E-POSTBRIEF zusätzlich die Möglichkeit der Übermittlung an normale Postadressen. Die E-POST spricht hier vom sog. **Hybridbrief**. Hybridbriefe werden als klassische Briefe auf dem Postweg zugestellt. Im Rahmen des Service für den Hybridbrief wird der E-POSTBRIEF durch die Post ausgedruckt, kuvertiert und dem Empfänger zugestellt. Dieser Service kann nur für Empfängeradressen in Deutschland und bis zu einer Briefgröße von maximal 94 Seiten genutzt werden.

Wie die De-Mail verzichtete der E-POSTBRIEF bei der vollelektronischen Übermittlung auf eine Ende-zu-Ende-Verschlüsselung und bot seinen Kunden hier auch nicht die Möglichkeit, diese zu verwenden. E-POSTBRIEFE wurden vielmehr allein mit einem Portalschlüssel integritätsgeschützt und unter Nutzung einer sog. Transportverschlüsselung (Transport Layer Security) auf die Server der Post übertragen. Da eingehende E-POSTBRIEFE und deren Anhänge durch die Post automatisch auf Viren und andere schadhafte Inhalte geprüft werden, scheidet eine vollständig verschlüsselte Übertragung dem Grunde nach aus. Auch wenn der Betrieb des Portals nach Angaben der Deutschen Post in einem nach BM/BSI-IT-Grundschutz (BSI = Bundesamt für Sicherheit in der Informationstechnik) zertifizierten Rechenzentrum erfolgt, findet eine Verschlüsselung daher „nur" zwischen dem Absender und dem E-Postserver und zwischen dem E-Post-Server und dem Empfänger statt. Aus anwaltlicher Sicht fragte sich hier, 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 und hierfür auch zu bezahlen, so sollte diese auch wirklich komplett sicher und nicht nur teilweise sicher sein. Die Post hat hier nachgebessert und bietet neuerdings den ePost-Brief End-to-End an.[38] Rechtsanwälten, die auf den ePost-Brief setzen, ist die Nutzung dieses Angebotes dringend anzuraten. **75**

In diesem Fall entfällt freilich die Möglichkeit der Nutzung des Hybridbriefes, 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. Auch wenn der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) in seinem 23. Tätigkeitsbericht[39] ausführt, dass „die vertrauliche Behandlung der übermittelten Daten beim Hybridbrief dadurch gewährleistet werden soll, dass die mit dem Ausdruck der Briefe betrauten Mitarbeiter/innen sich strafbar machen, falls sie das Post- und Fern- **76**

35 Leistungsbeschreibung E-POSTBRIEF, abrufbar unter: http://www.epost.de/content/dam/dp/dokumente/leistungsbeschreibung.pdf.

36 V. 2. 1. der E-POST-AGB, abrufbar unter: http://www.epost.de/privatkunden/footer/rechtliches/agb.html.

37 Mittels Eingabe des Anmeldenamens und des Passworts.

38 Http://www.epost.de/geschaeftskunden/fuer_unternehmen/end2end/funktionen.html.

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

meldegeheimnis (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 94 Seiten beschränkt ist, eignet er sich für längere Schriftstücke ohnehin nicht.

Mit Blick auf die Verbesserung des Datenschutz- und Sicherheitsniveaus elektronischer Post kann die Nutzung des vollelektronischen E-POSTBRIEFES jedoch eine sinnvolle Lösung darstellen.[40] Dies belegt nicht zuletzt auch die Zertifizierung des vollelektronischen Verfahrens mit dem Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.[41] 77

Web-Akte 78

Eine weitere alternative Kommunikationsform bietet der Branchenprimus eConsult AG mit seiner „WebAkte", die mit dem Slogan „Vertraulich wie ein persönliches Gespräch und beweissicher vor Gericht..." wirbt. Die „WebAkte" stellt indes keine E-Mail-Lösung, sondern eine Cloud-Lösung dar. Die Kanzlei legt für ihren Mandanten eine „elektronische Akte" an, auf die der Mandant zugreifen und sowohl bereitgestellte Dokumente herunterladen, als auch eigene Dokumente zum Abruf hochladen kann. Wird ein neues Dokument in die „WebAkte" eingestellt, erhält der Empfänger eine E-Mail, die ihn hierüber benachrichtigt. Dies kann entweder „einmal täglich" oder auch sofort geschehen. Im direkten Vergleich mit der E-Mail bietet die „WebAkte" den Vorteil, dass sich hierüber auch größere Datenmengen einfach austauschen und an den Mandanten übermitteln lassen.

In diesem Zusammenhang ist beispielsweise an Marken- und Wettbewerbsprozesse zu denken, die – über die Einbindung von Bildern, Zeichnungen usw. – schnell ein größeres Datenvolumen einnehmen. Vor dem Hintergrund der üblichen Postfachbeschränkungen im E-Mail-Verkehr sind derartige Dokumente kaum per E-Mail zu übermitteln, was insbesondere im Abstimmungsprozess Probleme bereiten kann. So zum Beispiel, wenn es auf die genaue Farbgebung von Dateien ankommt und damit nicht auf das Fax als schnellem Übertragungsweg zurückgegriffen werden kann. Da die Dateien zunächst auf den WebAkte-Server, der im DATEV-Rechenzentrum betrieben wird, hochgeladen werden müssen, sollte die Kanzlei, die sich für die WebAkte interessiert, in jedem Fall über eine hinreichend leistungsstarke Internetverbindung verfügen. Dabei bietet sich in der Praxis die sog. synchrone DSL-Leitung an, bei der Up- und Downloadgeschwindigkeit gleich hoch sind. Wer hier auf eine „klassische" Leitung setzt, der verzweifelt in der Regel an den langen Upload-Zeiten größerer Dokumente.

Up- und Download der über die WebAkte bereitgestellten Dokumente erfolgen über verschlüsselte Verbindungen, sind also vor unberechtigtem Zugriff gesichert. Ein weiterer Vorteil dürfte zudem in der Einbindung der WebAkte in zahlreiche Kanzleisoftwarelösungen zu sehen sein, die es ermöglichen, Dateien unmittelbar aus dem Kanzleiprogramm heraus an die WebAkte und damit an den Mandanten zu übermitteln.

40 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.

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

Die Weboberfläche der „WebAkte“ ist momentan indes allein auf den deutschen Markt ausgerichtet; eine wünschenswerte englische Softwareoberfläche fehlt leider, so dass sich insbesondere internationale Mandanten eher schwer im System zurechtfinden werden. Hier besteht in jedem Fall Nachholbedarf.

Nicht täuschen lassen, sollte man sich auch in Punkto „**Beweissicherheit**“. Diese bezieht sich nämlich allein auf die Zustellung eines Dokuments an einen bestimmten Empfänger, nicht jedoch auch auf den Inhalt der übermittelten Datei. Insoweit ist nämlich allein § 416 ZPO maßgeblich, der die Beweiskraft elektronischer Dokumente auf ein Mindestmaß beschränkt und ihnen lediglich den Status sog. **Augenscheinsobjekte** beimisst, die der freien richterlichen Beweiswürdigung unterfallen. Dies hängt daran, dass elektronische Dokumente grundsätzlich jederzeit veränderbar sind und diese Veränderungen rechtssicher zunächst einmal nicht nachvollzogen werden können. Dies gilt sowohl in Bezug auf inhaltliche Änderungen als auch in Bezug auf das Alter bzw. den Erstellungszeitpunkt einer elektronischen Datei. Bei eingescannten Dokumenten stellt sich zudem das Problem der Originalität. Dennoch ist die elektronische Kommunikation standesrechtlich zugelassen.

Wie aber begegnet der Rechtsanwalt der jederzeitigen Veränderbarkeit seiner elektronischen Kommunikation und verhindert so, dass diese im Rahmen eines Prozesses nur geringen Beweiswert hat. Sich hierbei allein darauf zu verlassen, in regelmäßigen Abständen einfache Datensicherung vorzunehmen reicht jedenfalls nicht. Im Rahmen von etwaigen Streitigkeiten zwischen Anwalt und Mandant wird der Mandant sonst einfach anführen können, das Dokument sei ihm nicht in der behaupteten Form zugegangen, sondern erst nachträglich erstellt bzw. zum Zwecke der erleichterten Prozessführung um entscheidungserhebliche Punkte angereichert worden. Eine rechtssichere Lösung für die vorgenannte Problematik bietet das Verfahren der so genannten qualifiziert elektronischen Signierung mit qualifiziert elektronischen Zeitstempeln. Unter einer so genannten elektronischen Signatur versteht man mit elektronischen Informationen verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Information überprüfen kann. Sie trägt dazu bei, eine zuverlässige Identifizierung des Unterzeichners zu gewährleisten und sicher zu stellen, dass nachträgliche Veränderungen einer Datei erkannt werden können. Vereinfacht dargestellt vollzieht sich die elektronische Signatur einer Datei wie folgt:

Von der zu signierenden Datei wird unter Zuhilfenahme einer Signatursoftware ein so genannter **Hash-Wert** erzeugt. Dieser Hash-Wert stellt keine „Kopie des Originaldokumentes“ dar, das Originaldokument kann vielmehr aus dem Hash-Wert nicht reproduziert werden. Der Hash-Wert kann vielmehr als „elektronischer Fingerabdruck“ eines elektronischen Dokumentes bezeichnet werden. Dieser elektronische Fingerabdruck einer Datei ist ähnlich wie der normale Fingerabdruck Unikat. Das heißt, ein Dokument gezielt mit dem gleichen Hash-Wert herzustellen, ist – zumindest nach heutigem Stand der Technik – unmöglich. Das bedeutet, dass zwei Textdateien, die sich nur in einem Byte (ein weiteres Leerzeichen, ein Komma, ein anderes Wort) unterscheiden, vollkommen verschiedene Hash-Werte erzeugen. Der Hash-Wert sichert also die Unveränderbarkeit eines Dokumentes. Erzeugt man nun von einer elektronischen Datei den Hash-Wert muss noch die Authentizität des Dokumentes belegt werden. Hier kommt die so genannte elektronische Signatur zum Einsatz. Der Nutzer verwendet zur Unterzeichnung seines Dokumentes ein so genanntes **asymmetrisches Kryptografieverfahren**. 79

Das bekannteste **Kryptografieverfahren** ist das so genannte RSA-Verfahren. Bei diesem Verschlüsselungsverfahren wird ein Klartext, hier der Hash-Wert, unter Anwendung zweier Schlüsselpaare nach einem Algorithmus in einen geheimen Text überführt. Bei dieser Art der Verschlüsselung besitzt jeder Kommunikationspartner ein Schlüsselpaar, einen öffentlichen und einen privaten Schlüssel. Der Absender einer Datei verschlüsselt dabei die Daten mit einem öffentlichen Schlüssel eines Empfängers, der die Nachrichten dann mit seinem privaten Schlüssel entschlüsselt. Das bedeutet, dass der öffentliche Schlüssel problemlos allen Kommunikationspartnern zur Verfügung gestellt werden kann. Die beiden Schlüssel

stehen in einer mathematischen Beziehung zueinander, können aber praktisch nicht aus dem jeweils anderen abgeleitet werden. Der dermaßen verschlüsselte Hash-Wert gilt damit im Rechtssinne als durch den Signaturverwender unterzeichnet. Es kann also festgestellt werden, dass ein bestimmtes Dokument, dem ein verschlüsselter und signierter Hash-Wert eindeutig zugeordnet werden kann, von einem bestimmten Ersteller stammt, hier dem Rechtsanwalt. Noch nicht geklärt ist damit jedoch die Frage, wann der Rechtsanwalt die nunmehr unikate Dokumentation erstellt hat. Dies aber ist gerade im **Haftungsprozess** von entscheidender Bedeutung. Wie also bewerkstelligt der Anwalt, dass der Erstellungszeitpunkt seines Dokumentes rechtssicher festgehalten werden kann. Hierzu nutzt man in der EDV so genannte elektronische Zeitstempel. Der Zeitstempel versieht den Hash-Wert mit einer eindeutigen Zeitangabe. Er wird von einer Institution vergeben, die die Authentizität der Zeitinformation versichert und welche sich der Prüfung durch die Bundesnetzagentur unterzogen hat. Ein elektronischer Zeitstempel gibt also an, dass das gestempelte Dokument, in diesem Fall der Hash-Wert, spätestens zum angegebenen Zeitpunkt existiert hat. Der Hash-Wert wiederum versichert, dass das Dokument zwischenzeitlich nicht verändert wurde. Ein mit einer qualifiziert elektronischen Signatur und einem qualifizierten Zeitstempel signiertes Dokument hat gemäß § 371a ZPO den Anschein der Echtheit und wird damit beweissicher. Auch private elektronische Dokumente, die mit einer qualifiziert elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privaten Urkunden damit entsprechend Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegender Erklärung, der sich aufgrund der Prüfung nach dem Signaturgesetz ergibt, kann damit nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung nicht vom Schlüsselinhaber abgegeben oder von diesem nachträglich verändert worden ist. § 371a ZPO schafft für qualifiziert elektronische Dokumente damit eine vollkommene Urkundenanerkennung im Sinne der §§ 415 ff. ZPO und stellt das elektronische Dokument damit der Papierdokumentation gleich. Wegen der genauen zeitlichen Einordnung über den qualifiziert elektronischen Zeitstempel ist die elektronische Dokumentation der Papierakte sogar überlegen. Es empfiehlt sich daher, die über die WebAkte bereitgestellten Dokumente zuvor zu signieren und mit einem Zeitstempel zu versehen.

Schließlich sollte man sich darüber im Klaren sein, dass auch die Kommunikation über die WebAkte nicht gänzlich von der Kenntnisnahme Dritter abgeschlossen ist. So weist eConsult darauf hin, dass es **80**

> *„für den vorgesehenen Support unerlässlich [ist], dass eConsult Zugriff auf die WebAkte der Anwaltskanzlei gestattet wird. Dabei ist es nicht ausgeschlossen, dass der Support-Mitarbeiter Kenntnis von Inhalten erhält."*

Dies stellt mit Blick auf die Vorgaben des § 203 StGB ein nicht unerhebliches Problem dar, das nur über eine vorherige und konkrete Einwilligung des Mandanten in die Nutzung des Systems zu lösen ist. Ist dies geschehen, bietet die „WebAkte" indes ein Mehr an Sicherheit innerhalb der Mandantenkommunikation und ist gegenüber der einfachen und unverschlüsselten E-Mail klar im Vorteil. Es lohnt sich also, auch diese Möglichkeit in Betracht zu ziehen.

Datensynchronisation mit Team-Drive **81**

Eine ähnliche Lösung bietet die Datensynchronisation mit Team-Drive. Die Nutzung dieser Cloud-Lösung wird durch den Deutschen Anwaltverein explizit unterstützt und über eine Kooperation auch kostentechnisch interessant. Anders als die WebAkte bietet TeamDrive eine vollständige Ende-zu-Ende-Verschlüsselung der übertragenen Dokumente an, die auf dem System nicht nur übertragen, sondern auch gespeichert, synchronisiert und „geshared" werden können. Die Software TeamDrive ist mit dem Datenschutzgütesiegel des Landeszentrums für Datenschutz Schleswig Holstein ausgezeichnet und bietet daher ein besonders hohes Maß an Sicherheit. TeamDrive bietet dabei mehrere Lösungsoptionen für den Daten-

austausch. So kann entweder der TeamDrive Cloud-Service genutzt oder die Daten auf dem eigenen Server hinterlegt werden. Der DAV schreibt hierzu:[42]

„Mit TeamDrive DAV erhalten Sie eine transparente Dokumentenverwaltung und standortunabhängiges Teamwork. Modernste Verschlüsselungstechnologien, eine ausgeklügelte Netzwerk-Architektur sowie die freie Serverwahl stellen die Vertraulichkeit aller Daten sicher. Die Software ermöglicht die sichere Zusammenarbeit mit Kollegen und Mandaten über eine automatische, verschlüsselte Übertragung mit revisionssicherer Dokumentation aller Änderungen.

Alle Cloud Services von TeamDrive DAV sind in Deutschland gehostet – nach ISO 27001 samt ADV-Vertrag gemäß den Anforderungen des BDSG.

Zum TeamDrive DAV Online-Portal für DAV-Mitglieder gelangen Sie über die DAV-Onlineplattform. Für die Anmeldung benötigen Sie Ihre DAV-Mitgliedsnummer und ein Passwort. TeamDrive DAV finden Sie dort im Persönlichen Bereich unter Vorteile der Mitgliedschaft."

82

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

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: Deaktivieren Sie in jedem Fall vorkonfigurierte Gastzugänge in einem WLAN-Router.

Regel 4: Verwenden Sie keinesfalls die technisch veralteten Verschlüsselungsverfahren WEP oder WPA in einem WLAN (Wireless Local Area Network).

Regel 5: 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 6: 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 7: Bieten Sie keinesfalls Ihren Mandanten und Besuchern ein unverschlüsseltes und offenes WLAN als Service an!

Regel 8: Schulen und sensibilisieren Sie regelmäßig das Personal hinsichtlich der Gefahren der IT-Nutzung.

Regel 9: 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 10: 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.

Regel 11: Seien Sie gegenüber E-Mail-Anhängen misstrauisch. Öffnen Sie keine E-Mail-Anhänge, die nicht aus eindeutig vertrauenswürdigen Quellen stammen.

Regel 12: Lassen Sie sich nicht durch Ihnen unbekannte Anrufer oder Personen dazu animieren, im Internet Links aufzurufen, Programme oder Dateien auf Ihren Rechner zu laden oder irgendwelche Programme und Funktionen auf der Webseite auszuführen.

Regel 13: Achten Sie bei Anrufen unbekannter Personen stets auf die angezeigte Nummer bzw. achten Sie darauf, ob die Rufnummer unterdrückt wird.

42 Http://anwaltverein.de/de/mitgliedschaft/rabatte#panel-kommunikation-technik.

E. Voice-over-IP in der Anwaltskanzlei

Voice-over-IP (VoIP) verbreitet sich rasant im privaten und geschäftlichen Bereich und folglich auch im Bereich von Rechtsanwaltskanzleien. In vielen Regionen werden derzeit Telefonanschlüsse bereits zwangsweise umgestellt. Soweit der Nutzer dabei der Umstellung nicht zustimmt, wird ihm dann sein Telefonanschluss gekündigt. Die erzwungene flächendeckende Nutzung von VoIP ist voraussichtlich nur noch eine Frage der Zeit. Gleichwohl, rät das DSL-Magazin,[43] 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? Zur Beantwortung dieser Frage ist zunächst das Verständnis der VoIP-Technik erforderlich. **83**

Während die klassische Telefonie per analoger Technik oder per ISDN (Integrated Services Digital Network) eine Verbindung von Punkt zu Punkt darstellt, schickt VoIP die digitalisierten Sprachpakete über das Internet. VoIP ist dabei nicht gleich VoIP: Wie die Beauftragte für den Datenschutz und die Informationsfreiheit in einer aktuellen Broschüre[44] hervorhebt, existiert hier kein einheitlicher Standard, sondern es werden verschiedene technische Varianten „mit fließenden Übergängen" eingesetzt, die sich zum Teil erheblich unterscheiden. Nach Angaben der Bundesdatenschutzbeauftragten stellen hier SIP sowie das H.323 die „populärsten" Protokolle dar. Die Bundesdatenschutzbeauftragte hält jedoch gerade diese Protokolle „von Natur aus [für] geschwätzig und per se nicht für die vertrauliche Kommunikation geeignet". Die Sicherheit muss hier also erst durch geeignete Maßnahmen hergestellt werden, sonst drohen nicht nur die Gefahren, die generell bei der Internet-Nutzung drohen, sondern auch erhebliche weitere Probleme. **84**

Durch die Funktionsweise des digitalen Netzes, das Datenpakete verschickt, die beim Empfänger wieder zusammen gesetzt werden müssen, ist die Verbindungsqualität in keinem Fall besser, als sie in einem gut ausgebauten konventionellen Netz ist. Wir wissen also nun, dass unsere Gespräche digitalisiert, in kleine Häppchen zerlegt und als Nutzlast mittels sogenannter Datenpakete über das öffentliche Netz verschickt werden. Geradezu skandalös ist jedoch der Umstand, dass dieses von Hause aus unverschlüsselt geschieht. Bereits seit Einführung der VoIP-Telefonie wird von Datenschützern gefordert, dass entsprechende Daten bei der Übertragung verschlüsselt werden sollen. Entsprechendes würde eine Ver- und Entschlüsselungslogik im jeweiligen Endgerät erfordern. Durch die Aushandlung eines Schlüssels bei Gesprächsaufbau zwischen den Geräten wäre eine Verbindung trotz Internetnutzung abhörsicher. Der Einsatz solcher Technik ist bis heute eher die Ausnahme geblieben, weil es nur funktionieren kann, wenn beide an einem Telefonat beteiligten Anschlüsse über die entsprechende Technik verfügen. Mit einfachen Mitteln lassen sich nun 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 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 weiteren Begriffen wie „Erpressung" oder „Unfallflucht" identifiziert werden können. 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 konventionelle Telefonsystem über eine eigene externe Stromversorgung verfügt. Auch hier sollten entsprechende Vorkehrungen getroffen werden. Schließlich sind in der Vergangenheit immer wieder Netzausfälle bei VoIP-Anbietern aufgetre- **85**

43 Http://www.dsl-magazin.de/voip/sicherheit/.

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

ten. So berichten VoIP-Nutzer teilweise von fortwährenden z.T. stundenlangen Netzausfällen, einige berichten sogar über tagelange Ausfälle.[45] Soweit ein regionaler Stromausfall über mehrere Stunden nicht behoben werden kann, könnte es zukünftig zu Situationen kommen, bei welchen auch die Mobilfunknetze regional ausfallen, so dass keinerlei telefonische Kommunikation mehr möglich wäre. Der Ausbau der Kommunikationsnetze (Glasfasernetzwerke) und der Wunsch nach schnellerem Internet könnten also durchaus auch negative Seiteneffekte mit sich bringen.

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.[46] Verschlüsselungs- und Authentifizierungsverfahren sind in diesem Kontext die wohl zentralen Begriffe. Aufgrund der Variabilität des Einsatzes von VoIP können konkrete Handlungsempfehlungen leider nicht ausgesprochen werden. **86**

VoIP ist gleichwohl eine Technologie, die beim Einsatz entsprechender Sicherheitsmaßnahmen nicht nur eine ernsthafte Alternative zur klassischen Telefonie darstellt, sondern aufgrund der im Vergleich zur konventionellen Telefonie (analog/ISDN) wesentlich erweiterten Möglichkeiten sicherlich in Zukunft noch mehr an Bedeutung gewinnen wird. Eine Entscheidung für oder gegen den Einsatz von VoIP-Systemen stellt sich allerdings den Kanzleien nicht, da eine flächendeckende Zwangsumstellung von analoger Telefonie oder ISDN auf VoIP bereits in vollem Gange ist. Entsprechend sollte sich jeder Anwalt damit auseinandersetzen, wie er trotz VoIP das Mandatsgeheimnis bestmöglich schützen kann. **87**

Obwohl bereits die VoIP-Technologie als solche schon durchaus kritisch zu betrachten ist, wirft die Einführung dieser Technik weitere Probleme auf. Die Art der VoIP-Technologie erfordert, dass entsprechende Telefonanlagen nunmehr an das Internet angeschlossen sein müssen. Damit erhöht sich das Gefährdungspotential durch Angriffe auf Kommunikationsanlagen aus dem Internet signifikant. Bereits jetzt sind Telefonanlagen ein beliebtes Angriffsziel für Internetkriminelle.[47] Teilweise wird der Angriff auf solche Anlagen sehr einfach gemacht, indem bei der Installation die Standardpasswörter nicht geändert werden, unsichere Kommunikationsports nicht geschlossen werden und keine professionellen Firewalls zum Internet die Telefoneinrichtungen schützen. Das Resultat mangelnder Absicherung der Anlagen sind schnell fünf- oder gar sechsstellige Telefonrechnungen, weil ein Angreifer nach erfolgreicher Attacke auf die Telefonanlage bis zur Entdeckung des Angriffs kostenpflichtige und i.d.R. sehr kostspielige Telefonnummern im Ausland, bevorzugt im Nahen Osten, anruft. Aber auch in anderer Weise kann ein solcher Einbruch in das System gefährlich werden, wenn nämlich die Telefonanlage aus Ausgangsbasis genutzt wird, um weitere Systeme im Netzwerk der Kanzlei anzugreifen. **88**

Regel 1: Beauftragen Sie nur ausgewiesene IT-Experten mit der Umstellung auf VoIP. **89**
Regel 2: Achten Sie darauf, dass alle nichtbenötigten Ports der Telefonanlage gesperrt sind.
Regel 3: Trennen Sie unbedingt die Netze von Telefon- und IT-Technik. Bei Einsatz einer CTI-Lösung, können diese über eine Firewall kommunizieren.
Regel 4: Schalten Sie der VoIP-Telefonanlage unbedingt eine professionelle Firewall vor.
Regel 5: Achten Sie darauf, dass in die Telefonanlage regelmäßig Sicherheitsupdates eingespielt werden.

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

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

47 Siehe *Kazemi/Lenhard*, Cyberkriminalität und Cyberschutz für Rechtsanwälte und Mandanten, Deutscher Anwaltsverlag, Bonn, 2016, ISBN 978–3-8240–5776–4.

F. 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, Buchhaltungsdaten) der Kanzlei unwiederbringlich zerstört sind. **90**

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 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. Nun wird der eine oder andere Leser denken: „Kein Problem – meine Mitarbeiter wechseln ja jeden Tag die Sicherungsbänder“. **91**

Genau hier liegt häufig das Problem. Das tägliche Wechseln von Bändern wiegt uns 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. Ein 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 **92**

Datensicherung besteht 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. 93

Wie sollte nun in der Kanzlei eine Datensicherung erfolgen? 94

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.

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. 95

Eine weitere Problematik im Zusammenhang mit Datensicherungen zeigt sich insbesondere durch eine gegenwärtig massive Bedrohung von IT-Systemen durch Verschlüsselungsviren. Diese sind teilweise in der Lage, alle verknüpften Netzlaufwerke ebenfalls zu verschlüsseln. Aus diesen Gründen müssen Datensicherungen unbedingt als externe Datensicherung gelagert werden. Üblicherweise kann dies zusätzlich zu sogenannten **Online-Sicherungen** erfolgen.

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. 96

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.

G. Warum Sie die Datenträger in Ihrer Kanzlei verschlüsseln sollten

War dieses Kapitel ursprünglich dem Thema Verschlüsselung von Notebook-Festplatten gewidmet, so zeigte ein entsprechender Fall, dass bestimmte Umstände nicht nur im Zusammenhang mit einem Notebook auftreten können. 97

Wie das Swiss IT-Magazine bereits in seiner Ausgabe 2005/19[48] 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? 98

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. 99

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.[49] 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, 100

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

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

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.

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. **101**

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. **102**

Bei der Auswahl eines Verschlüsselungssystems ist jedoch Vorsicht geboten. Einige am Markt präsente Systeme gaukeln dem Nutzer nur die Sicherheit vor. So wurden in der Vergangenheit USB-Sticks als sicher angepriesen, deren Verschlüsselung sich bereits nach wenigen Sekunden als untauglich erwies, Daten vor den Augen technisch versierter Hacker zu verbergen. Aber ebenso untauglich ist eine Festplattenverschlüsselung, bei deren Einsatz sich US-amerikanische Unternehmen den Wiederherstellungsschlüssel übertragen, der eigentlich und ausschließlich im Tresor des Nutzers liegen sollte um einen Festplatteninhalt trotz eines vergessenen Passworts wiederherzustellen. Die Logik, die sich dahinter verbirgt, ist schwer bis gar nicht nachzuvollziehen, denn einfacher wäre es für den Benutzer, direkt das Passwort in einem Tresor oder Bankschließfach zu hinterlegen. Soweit also ein Festplattenverschlüsselungsverfahren zum Einsatz kommt, sollte es nach Möglichkeit kein System sein, das mitteilungsbedürftig ist, „nach Hause telefoniert“ oder Dritten die Möglichkeit bietet, die Daten Ihrer Kanzlei zu entschlüsseln. **103**

Regel 1: Verschlüsseln Sie Daten oder Festplatten aller mobilen Geräte, die Sie außerhalb der Kanzlei verwenden. **104**

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.

Regel 4: Nutzen Sie keine Verschlüsselungsverfahren, die Informationen oder gar sogenannte Wiederherstellungsschlüssel an den Software-Hersteller übermitteln.

Anzeige

Cloud-Dienste und Geheimnisträger – Voraussetzungen für die Nutzung

Ein Gastbeitrag von Dr. Hubert Jäger - CTO der Uniscon GmbH sowie maßgeblicher Akteur bei der Definition und Entwicklung des Datenschutzzertifikats Trusted Cloud Datenschutzprofil.

Angehörige von Berufsgruppen, die einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, lagern IT-Dienstleistungen an externe Spezialisten aus, zunehmend auch an innovative IT-Angebote im Internet (Cloud-Dienste). In diesem Fall muss hinreichender Datenschutz gewährleistet sein. Falls eine Kanzlei, die einen Dienst verwenden will, diesen im Rahmen einer Auftragsdatenverarbeitung beauftragt, ist sie als Auftraggeber gesetzlich verpflichtet, sich von der Ordnungsgemäßheit der technischen und organisatorischen Maßnahmen des Cloud-Anbieters zu überzeugen. Eine sinnvolle Überprüfung der technischen Systeme erfordert jedoch Qualifikation wie auch zusätzliche Ressourcen.

Datenschutz-Zertifizierung - berücksichtigt die DS-GVO

Eine Kanzlei kann mithilfe der Datenschutz-Zertifizierung nach dem Trusted Cloud Datenschutzprofil (TCDP) Aufwand vermeiden: Das TCDP wurde im Auftrag des Bundesministeriums für Wirtschaft und Energie unter Mitarbeit der maßgeblichen Interessenvertreter entwickelt. Dazu zählen Datenschutzaufsichtsbehörden, Vertreter der Privatwirtschaft, Verbände und Normungsstellen mit Erfahrung im IT-Bereich. Es umfasst die datenschutzrechtlichen Anforderungen des BDSG, außerdem wurden bereits die Anforderungen der DS-GVO berücksichtigt.

Da die Anforderungen an die technisch-organisatorischen Maßnahmen ein individueller Maßstab sind und sich nach dem Schutzbedarf richten, liegt im Kern des TCDP ein Schutzklassenkonzept: Der Schutzbedarf wird aus den verwendeten Datenarten und dem Verwendungskontext ermittelt. Wenn eine Kanzlei einen IT-Dienst auswählt, der gemäß der Anforderungen einer Schutzklasse zertifiziert wurde, die dem Schutzbedarf der Daten entspricht, darf sie die gesetzliche Kontrollpflicht als erfüllt erachten. Rechtsanwaltskanzleien können durchgängig von der Schutzbedarfsklasse 3 ausgehen. Die Stiftung Datenschutz stellt einen Rechner zur Verfügung, mit dem Sie Ihren Schutzbedarf leicht bestimmen können.
Zum Schutzbedarfsrechner

Geheimnisschutz für Inhalte UND Metadaten

Die Beauftragung externer Dienstleister kann als eine unbefugte Offenbarung von Berufsgeheimnissen angesehen werden, die nach § 203 StGB strafbar ist, sofern der Dienstleister Zugriff auf die Berufsgeheimnisse erlangen kann. Eine Ende-zu-Ende-Verschlüsselung der Geheimnisse kann dies weitgehend verhindern, sofern die Verbindungsdaten keine Berufsgeheimnisse preisgeben. Bei einem für Anwaltskanzleien typischen Datenaustausch mit der Mandantschaft stellen die Verbindungsdaten i.d.R. Berufsgeheimnisse dar. Sie müssen vor dem Zugriff durch den Dienstleister bewahrt werden (Metadatenschutz).

Cloud-Dienst iDGARD erfüllt die Anforderungen der Schutzklasse 3

IT-Security Spezialist Uniscon GmbH aus München bietet den Cloud-Dienst iDGARD zum vertraulichen Austausch von Dokumenten und Nachrichten für Anwälte an. Der Dienst wurde bereits in der Schutzklasse 3 nach TCDP zertifiziert, schützt Inhalte und Metadaten und ist somit für den Einsatz in Kanzleien geeignet.

iDGARD

zertifiziert nach TCDP 0.9 Schutzklasse III TUVIT-5527.16 www.tuvit.de bis 31.03.2018

- Sicherer Dokumentenversand & Empfang
- Rückstandsfreies Löschen von Dokumenten
- Hohe Sicherheit bei der Anmeldung: Login Card, SMS
- Verbreitungsschutz durch Wasserzeichen, Journal, etc.

Testen Sie iDGARD 30 Tage kostenlos - kein Abo

Wir bieten Ihnen die Möglichkeit, iDGARD 30 Tage kostenfrei zu testen. Starten Sie Ihren Test unter **https://www.idgard.de/business-registrierung** und geben Sie den Bonus Code **30tage-dav** ein.

H. 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. 105

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 immer wieder gab es zum Teil recht schwerwiegende Vorfälle im Zusammenhang mit Cloud-Computing. 106

Wie funktioniert nun eine solche Cloud? 107

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 sind 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. Die Vorteile der Cloud können Sie trotzdem nutzen, soweit Sie auf Ihren mobilen Geräten den entsprechenden 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. Einige Anbieter bieten auch bereits die separate Dateiverschlüsselung an, so dass die Daten nicht nur über verschlüsselte Kanäle in die Cloud übertragen werden, sondern bereits in der Kanzlei verschlüsselt werden und nach der verschlüsselten Übertragung zusätzlich auf verschlüsselten Festplatten abgelegt werden.

108 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 diverse Ausspähskandale hinlänglich bekannt sein dürfte, zählen zu diesen „datenschutzrechtlichen Entwicklungsländern" auch die Vereinigten Staaten von Amerika. Nicht zuletzt wurde diesem Umstand durch das Urteil des EuGH vom 6.10.2015 Rechnung getragen.[50] 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.

109 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.

110 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 in Hinblick auf Fremdzugriffe sicher ist, sondern auch hinsichtlich der Verfügbarkeit der Daten. Bei dem v.g. Anbieter kam es bzgl. 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.

50 EuGH Rechtssache C-362/14, Urt. v. 6.10.2015.

Notwendigkeit ADV-Vertrag 111

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 ein datenschutzrelevanter Vorgang verbunden. Das Verhältnis zum Cloud-Anbieter ist als Auftragsdatenverarbeitung im Sinne des § 11 BDSG zu qualifizieren.[51]

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.[52] 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.[53] 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.[54] Eine am 10.2.2014 vom BSI herausgegebene technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen"[55] 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 Themen- 112

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

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

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

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

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

gebiets überfordert, so dass empfohlen wird, vor Einsatz von erweiterten Cloud-Lösungen einen unabhängigen Datenschutzexperten zu konsultieren.

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 arbeiten, wenn der Webservice nicht erreichbar ist (z.B. DSL-Störung), und was bedeutet ein Datenverlust beim Anbieter des Dienstes für meine Kanzlei? **113**

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. **114**

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. Das heißt, dass man die Vorteile einer Cloud nutzen kann, ohne gleichzeitig die damit verbundenen Nachteile in Kauf nehmen zu müssen. So bietet zum Beispiel, das saarländische Unternehmen 1A-Archiv GmbH ein Online-Archivsystem als Compliance-Lösung an, also eine in sich geschlossene Lösung, bei der Hard- und Software eng aufeinander abgestimmt sind. Das System kann sowohl als internes Datenarchiv in Kanzleien genutzt werden, als auch von außerhalb per sicherem Zugriff verfügbar gemacht werden. **115**

Wer hierbei Redundanz benötigt, der kann zwei Systeme per Kabel verbinden und diesen mit einem Mausklick mitteilen, dass eine Spiegelung der Daten gewünscht ist. Neuerdings können dabei sogar die Daten des Archivs mit einer kanzleieigenen Datenbank im Rechenzentrum des Unternehmens synchronisiert werden. Bei solchen Lösungen kann dann ebenfalls von überall auf Daten zugegriffen werden kann, ohne dass jedoch die Daten in einer Cloud gespeichert werden. Die Kanzlei hat mit einer derartigen Lösung die volle Kontrolle über Ihre Daten und muss nicht befürchten, dass diese in datenschutzrechtliche Entwicklungsländer transferiert werden.

„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 wird. 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 Doku- **116**

mente erstellt, bearbeitet und archiviert sowie beliebig viele digitale Akten angelegt werden.[56] Auf Wunsch werden die an die Cloud übertragenen Daten Ende-zu-Ende und mindestens gemäß AES 256 verschlüsselt.

Finger weg von der iCloud im anwaltlichen Berufsalltag

Dringend abzuraten ist jedoch von der Nutzung der sog. Apple iCloud.[57] 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.[58] 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.: **117**

> *„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 angemessener Weise 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. **118**

Kritisch zu sehen, sind momentan auch diverse Cloud-Zertifizierungen, die zum Teil eher einer politischen oder geschäftsmodell-getriebenen Augenwischerei gleichen, als dass Sie wirklich in der Lage wären, eine Garantie für die Sicherheit bestimmter Cloud-Systeme darzustellen. Im Rahmen der Recherchen zu der vorliegenden Auflage wurde daher eine solche Cloud-Zertifizierung näher betrachtet. Dabei war u.a. nicht in Erfahrung zu bringen, wie sich ein sachverständiger Prüfer qualifizieren kann, um als Auditor für die entsprechende Zertifizierung anerkannt zu werden. Erstaunlicherweise war an anderer Stelle festzustellen, dass eine staatliche Institution auf Ihrer Webseite gleich an eine bestimmte Firma verweist. Offensichtlich hat man vielerorts in jüngster Zeit Zertifizierungen als lukrative Einnahmequelle für sich entdeckt. Diese Entwicklung hat jetzt auch den Bereich des Cloud-Computing erreicht. **119**

Unter Ausblendung monetärer Faktoren ist es nicht nachvollziehbar, wieso für eine Cloud eine der etablierten Zertifizierungsmaßnahmen wie die des „Unabhängigen Landeszentrums für Datenschutz Schles-

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

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

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

wig-Holstein“ (kurz: ULD Datenschutzgütesiegel) oder die Zertifizierung durch das „Europäische Datenschutzsiegel“ (EuroPriSe) nicht ausreichend sein sollten und daher immer neue Zertifizierungen aus dem Hut gezaubert werden.

Soweit Sie sich für die Nutzung von Cloud-Computing entscheiden, sollten Sie folgende Regeln[59] beachten: **120**

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.

59 Ausführlich zum Cloud-Computing auch der Leitfaden Cloud-Computing der BITCOM, abrufbar unter: https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Cloud-Computing.html.

Mehr Sicherheit durch IT-Outsourcing

ANZEIGE

Software und IT aus der DATEV-Cloud

Gerade im Hinblick auf berufsständische Verschwiegenheitspflichten spielen bei Anwälten Datenschutz und Datensicherheit eine große Rolle. Hinzu kommt, dass Mobilität auch bei Anwälten immer mehr an Bedeutung gewinnt. Von unterwegs aus Kanzlei-E-Mails aufrufen, Termine checken oder schnell mal eine Information in einer Mandantenakte nachschauen – mobile Endgeräte wie Notebooks, Tablets oder Smartphones machen die anwaltliche Arbeit von unterwegs aus in vieler Hinsicht einfacher.

Werden vertrauliche Daten nicht physisch auf dem mobilen Endgerät, sondern sicher über die Cloud im Kanzleinetzwerk abgelegt, verhindern Sie bei Verlust des Geräts, dass die sensiblen Daten in unbefugte Hände gelangen. Gleichzeitig bietet die externe Datenlagerung den bestmöglichen Schutz vor Datenverlust bei Ausfall der PC-Systeme, bei Brand oder Wasserschaden. Mit den Angeboten von DATEV führen Sie Ihre Kanzlei in eine sichere digitale Zukunft.

Kanzleisoftware aus der Cloud

Mit der Kanzleisoftware DATEV Anwalt classic pro erledigen Sie Ihre gesamte Kanzleiorganisation von A wie Aktenverwaltung bis Z wie Zwangsvollstreckung. Doch mit einer leistungsfähigen Software allein ist es nicht getan – Kanzleiorganisation fängt bereits bei der IT an. Um Ihre Software zum Laufen zu bringen, muss auch die entsprechende Infrastruktur vorhanden sein. Eine Lösung ist es, Ihre Kanzleisoftware sowie das IT-Management auszulagern. Das heißt, Software, Daten und Server stehen in einem gesicherten Rechenzentrum und Sie greifen online über eine verschlüsselte Leitung auf Ihre Systeme zu. Das Arbeiten funktioniert wie vorher auch, mit dem Unterschied, dass die Daten sicher in einem externen Rechenzentrum lagern. Ein Zugriff ist von überall möglich – ob in der Kanzlei, im Home-Office oder von unterwegs aus. Sie benötigen lediglich einen Internetzugang. Das erleichtert Ihren Arbeitsalltag ungemein und bringt Sie einen großen Schritt voran in Richtung Digitalisierung. Ihre Kanzleisoftware ist stets auf dem aktuellen Stand und um Wartung, Betrieb und Installationen kümmern sich erfahrene Experten.

Eine Cloud – viele Möglichkeiten

DATEV bietet verschiedene Lösungen, das Software- und IT-Management in die DATEV-Cloud auszulagern – ganz nach Ihrem eigenen Bedarf.

www.datev.de/cloud-sourcing

Keine Kostenfalle

Viele Kanzleiinhaber glauben, dass die Kosten bei IT-Outsourcing weitaus höher sind als der Nutzen – verglichen mit einer Inhouse-Lösung. Was die meisten aber nicht im Blick haben, ist die mit der Auslagerung verbundene Optimierung der Kostenstrukturen. Denn Investitionen in neue Hardware sind kostspielig und stehen regelmäßig alle paar Jahre an, ganz zu schweigen von den versteckten Kosten für Strom und Kühlung. Hinzu kommen der Zeitaufwand und das erforderliche Know-how für Installationen, Updates, Wartung und Betrieb der IT-Systeme. IT-Outsourcing entlastet Sie hier umfassend, denn statt eigene Hardware zu kaufen, mieten Sie Serverplätze im Rechenzentrum.

Sicher in der Cloud

IT-Outsourcing bedeutet aber auch, seine Hard- und Software außer Haus – und damit in kanzleifremde Hände zu geben. Das erfordert eine vertrauensvolle Beziehung zum Outsourcing-Partner. Denn es wird nicht einfach nur der Standort der Server verlagert, sondern es geht vor allem um die Daten von Mandanten: Vertrauliche Informationen, die vertraulich bleiben müssen. Denn als Rechtsanwalt unterliegen Sie der berufsrechtlichen Verschwiegenheitspflicht. Deshalb heißt es: Augen auf bei der Wahl des IT-Outsourcing-Partners! In Sachen Datenschutz und -sicherheit ist DATEV seit 50 Jahren ein verlässlicher Partner und bietet mehr Erfahrung und Sicherheit als jeder andere Anbieter in diesem Bereich. Das nach ISO 27001 zertifizierte DATEV-Rechenzentrum mit Standort in Deutschland ist der physische Ort der DATEV-Cloud und die sichere Basis und zentrale Datendrehscheibe für die Outsourcing-Lösungen von DATEV. Vertrauen Sie daher auf die langjährige Erfahrung und Kompetenz von DATEV, wenn es um das Thema Sicherheit geht.

Mehr Infos unter:
www.datev.de/anwalt
Kontakt: anwalt@datev.de

DATEV eG
90329 Nürnberg
Telefon +49 911 319-0
Telefax +49 911 147-43342
E-Mail info@datev.de
Internet www.datev.de
Paumgartnerstraße 6–14

I. Betriebssystem und Datenschutz

Wie bereits in vorhergehenden Kapiteln hinlänglich dargelegt wurde und ohnehin jedem interessierten Juristen bekannt ist, ist der Anwalt bzw. die Anwaltskanzlei hinsichtlich der Verarbeitung personenbezogener Daten verantwortliche Stelle im Sinne des § 3(7) BDSG. Als solche bzw. als datenverarbeitende Stelle, wie es der Wortlaut des § 9BDSG nennt, sind organisatorische und technische Maßnahmen zu treffen, „*die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten*". In diesem Zusammenhang denkt man zumeist an ein Antivirenprogramm, ein funktionierendes Backup oder aber an eine sogenannte Firewall. Jedoch zählt auch ein Betriebssystem zu den technischen Maßnahmen, welche üblicherweise einen angemessenen Schutz gegen unbefugte Zugriffe leisten sollen. Was nun im Einzelnen gegen die Nutzung einiger Cloud-Lösungen spricht (siehe Kapitel H, Rdn 105 ff.), gilt auch für Betriebssysteme. Auf Betriebssysteme muss sich der Anwender, also in unserem Fall der Anwalt, ebenso verlassen können, wie auf die eingesetzte Kanzleisoftware. Mehr noch muss das Betriebssystem als besonders zuverlässig und sicher gelten. Ist nämlich das Betriebssystem mit diversen technischen Unzulänglichkeiten behaftet, die geeignet sind, Angreifern einen Zugriff auf die Dateiebene oder sogar auf die Applikationsebene zu verschaffen, so wird hier unter Umständen der Schutz durch andere, sogar weitreichende Sicherungsmaßnahmen mitunter ausgehebelt. Daher ist es stets erforderlich, Betriebssystemaktualisierungen, die der Sicherheit des Systems dienen, zu installieren. Soweit Sie z.B. ein Windows-Betriebssystem einsetzen und zu der Gruppe der Windows-Benutzer dürfte aktuell ein großer Teil der Leser zählen, so ist es i.d.R. unverzichtbar sogenannte wichtige Updates einzuspielen. Entsprechendes kann unter den Menüpunkten „Systemsteuerung – Windows-Updates" eines Windows-Betriebssystems eingestellt werden, so dass wichtige Updates auch automatisch installiert werden. An eben dieser Stelle kann auch ein Modus ausgewählt werden, der neben wichtigen Updates auch empfohlene Updates automatisch einspielt. Diejenigen, die diese Konfigurationen auf Systemen der Versionen Windows 7 oder Windows 8.x vorgenommen haben, dürften sich irgendwann zumindest gewundert haben, dass Ihr Rechner Ihnen ein kostenloses Update auf Windows 10 angeboten hat. Eben diese Vorgehensweise des Softwareunternehmens ist vielfach in die Kritik geraten. 121

Zwischenzeitlich ist es ruhiger geworden um die Diskussion der Aktualisierung von Windows 7 oder Windows 8.1. auf die neuere Version Windows 10. Zwar kann man das neuere Betriebssystem durchaus als robust und zuverlässig ansehen, jedoch trifft diese Einschätzung auch auf die Vorgängerversionen zu, für die erst in den Jahren 2020 bzw. 2023 der erweiterte Support enden wird. Speziell in einer Kanzlei, ist es nicht nachvollziehbar, wieso man vorzeitig einen Versionswechsel durchführen soll, zumal der Wechsel eines Betriebssystems oder einer Betriebssystemversion immer Kompatibilitätsprobleme zwischen Betriebssystem und Anwendungssoftware mit sich bringen kann. Eine goldene Regel in der Informatik lautet deswegen: „**Never change a running system!**" 122

Anders sieht es aus, wenn ein Rechner ersetzt werden muss, da neue Geräte in der Regel nicht mehr mit älteren Betriebssystemen verkauft werden. Es ist zwar immer noch möglich, neue Rechner mit Windows 7 oder Windows 8.1 als Betriebssystem zu erwerben, das dürfte aber eher die Ausnahme sein. 123

Neuere Betriebssysteme sind sehr mitteilungsbedürftig 124

Die eigentliche Problematik neuerer Betriebssysteme – und hier wird ganz bewusst der Plural gewählt – liegt darin, dass sie es dem kleinen Außerirdischen mit dem roten Leuchtfinger nur allzu gerne gleich tun und nach Hause telefonieren. Letzteres ist mittlerweile die in der Informatik gängige Beschreibung für Systeme, die Daten sammeln und an Herstellerunternehmen oder Server im Internet senden.

Einen Eindruck, was z.B. das System Windows 10 alles seinem Hersteller mitzuteilen gedenkt, erhalten Sie, wenn Sie z.B. das kostenlose Werkzeug des Berliner Unternehmens O&O Software GmbH mit dem

bezeichnenden Namen „O&O ShutUp 10“[60] herunter laden und auf einem Rechner mit dem Betriebssystem Windows 10 starten.

Es ist nichts außergewöhnliches, dass Benutzer zunächst einmal schockiert sind, was alles von einem Betriebssystem an seinen Hersteller übermittelt wird.

Noch kritischer als die bloße Übermittlung von Daten ist die Kombination mit der Nutzung von Cloud-Diensten eines entsprechenden Betriebssystemanbieters. 125

Je nach eingesetztem Betriebssystem steht zu befürchten, dass Telemetriedaten, Biometrische Daten (Fingerabdruck, Gesichtserkennung), Sprachprofile (Spracherkennung oder Nutzung eines sprachbasierten Assistenzsystems), Daten zur Handschriftenerkennung und vieles mehr zumeist an Server in den USA übermittelt werden.

Es ist daher keine leere Floskel darauf hinzuweisen, dass manche US-Amerikanischen Unternehmen bereits heute mehr von uns wissen, als wir selbst. In diesem Zusammenhang kann man nur das Marktplatzprinzip begrüßen, welches uns die EU-DSGVO bringen wird.

Ein Typus von Daten wurde bislang in diesem Kapitel noch nicht angesprochen. Es geht dabei um Geodaten. Viele mobile Geräte verfügen heute über ein GPS[61]-Modul. Während in der Literatur häufig zu lesen ist, dass GPS-Systeme auf ca. 100 m genau einen Standort lokalisieren können, muss davon ausgegangen werden, dass diese mittlerweile so ausgereift sind, dass der Standort auf Meter genau trianguliert werden kann. Ansonsten wären keine GPS-gesteuerten Hilfssysteme für Blinde oder Sehbehinderte einsetzbar. Was einerseits von großem Nutzen ist, kann aber andererseits zum Problem werden. Durch die Mitteilungsbedürftigkeit einiger Betriebssysteme oder darauf installierter Programme, sogenannter Apps, können mittlerweile sehr exakte Bewegungsprofile erstellt werden. Es braucht also nicht mehr unbedingt die Kennung der Mobilfunkzelle, um ein Bewegungsprofil zu erstellen, da die Geräte mitunter sehr viel genauere GPS-Daten zur Verfügung stellen können. 126

Wo liegt hier aber das Problem für den Anwalt? 127

Stellen Sie sich eine Konstellation vor, in der ein Mandant Ihre Unterstützung benötigt, weil er selbst nicht in Erscheinung treten darf. Das wäre durchaus vorstellbar, wenn es sich um einen sogenannten Whistleblower handeln würde, der größere Schwierigkeiten zu erwarten hätte, wenn seine Identität bekannt werden würde. Je nach „Branche“ könnte ein Bekanntwerden seiner Identität dazu beitragen, seine wirtschaftliche Existenz zu bedrohen oder sogar eine Gefahr für Leib und Leben darstellen.

Dieser Mandant nutzt in unserem imaginären Szenario ein Smartphone, auf dem er irgendeine kostenlose App installiert hat, die zwar keine Geodaten benötigt, aber diese an einen Server in den USA sendet. Niemand weiß, was mit den dort erstellten Profilen alles angerichtet wird. Eines ist jedoch sicher: Es sind keine humanitären Motive, die US-Unternehmen dazu bewegen, exzessiv Daten sammeln. Vielmehr geht es i.d.R. ausschließlich um monetäre Gründe. Wer also dem Datensammler für das Bewegungsprofil des Mandanten ausreichend gute „Gründe“ liefert, also einen bestimmten Preis bezahlt, wird auch das Bewegungsprofil erhalten.

Eine Speicherung von Geodaten wäre ebenso sinnlos wie die Speicherung irgendwelcher Daten, wenn damit nicht gearbeitet würde oder bestimmte Zwecke verfolgt würden.

Das heißt, dass es mit heutigen Mitteln bereits möglich ist, herauszufinden, wer in einer Kanzlei ein und ausgeht. Vorausgesetzt, er hat das GPS-Modul seines Smartphones oder Tabletts aktiviert.

Regel 1: Installieren Sie regelmäßig Updates, die Sicherheitslücken im Betriebssystem schließen. 128

60 Https://www.oo-software.com/de/shutup10.
61 Global Positioning System.

Regel 2: Wechseln Sie nie ohne triftigen Grund (z.B. Support-Abkündigung, techn. Probleme) das Betriebssystem. „Never change a running system"
Regel 3: Falls ein Betriebssystemwechsel ansteht, klären Sie mit dem Hersteller Ihrer Kanzlei-Software Fragen der Kompatibilität.
Regel 4: Lassen Sie neue Betriebssysteme nur von Sicherheitsexperten installieren und konfigurieren.
Regel 5: Treffen Sie Sie Sicherheitsvorkehrungen, damit Ihre Systeme keine Daten ungewollt übermitteln.
Regel 6: Weisen Sie ggf. Ihre Mandanten darauf hin, dass Bewegungsprofile durch die Nutzung von Smartphones und Tablettrechnern möglich sind.

J. 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,[62] die zur „Einstimmung" vorangestellt werden soll: 129

Muss eine Kanzlei die persönlichen Daten eines ausgeschiedenen Arbeitnehmers von ihrer Homepage löschen? 130

Das Landesarbeitsgericht Hessen sagt: Ja!

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[63] hatte der Verfügungsklägerin zunächst Recht gegeben, die Verfügungsbeklagten haben Berufung zum Landesarbeitsgericht eingelegt. 131

Das Landesarbeitsgericht Hessen hat der Verfügungsklägerin, wie auch das Arbeitsgericht Frankfurt zuvor Recht gegeben. 132

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 Ver- 133

62 Hessisches LAG, Urt. v. 24.1.2012 – 19 SaGa 1480/11.
63 ArbG Frankfurt, Urt. v. 5.10.2011 – 13 Ga 160/11.

fügungsklägerin hervorheben, ergebe sich, dass konkret mit dem Bild der Verfügungsklägerin geworben werde.

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. **134**

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 Angestellten 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. **135**

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

Was ist Beschäftigtendatenschutz? **136**

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.

So bestehen beispielsweise keine expliziten arbeitsrechtlichen Bestimmungen für den Umgang mit betrieblichen Informations- 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. **137**

Der Bundesgesetzgeber hat – nachdem bereits seit langem von verschiedenen Stellen die Schaffung eines bereichsspezifischen Arbeitnehmerdatenschutzgesetzes gefordert wurde[64] – auch bedingt durch die Vielzahl verschiedener Datenschutzskandale bei Großunternehmen im Jahre 2009[65] mit § 32 BDSG erstmals eine spezifische Regelung zum Arbeitnehmerdatenschutz geschaffen. Gleichzeitig wurde eine Arbeitsgruppe eingerichtet, die den Entwurf für ein umfassendes Arbeitnehmerdatenschutzgesetz erarbeiten sollte.[66] **138**

§ 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. **139**

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

§ 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. 140

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. 141

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.[67] 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.[68] 142

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. 143

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 144

67 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.

68 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.

und bereichsspezifischen Vorschriften" des BDSG grundsätzlich nicht.[69] Somit können vor allem die Erlaubnistatbestände des § 28 BDSG, insbesondere die in § 28 Abs. 1 S. Nr. 2 und 3 BDSG genannten,[70] auch hier herangezogen werden.

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

146 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.

147 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.

148 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.

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

150 *Übersicht über datenschutzrechtliche Rechtsgrundlagen im Beschäftigungsverhältnis*

- **§ 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.

69 BT-Drucks 16/13657, S. 20; z.T. a.A. *Gola*, in: Gola/Schomerus (Hrsg.), BDSG, 10. Aufl. 2010, § 32 Rn 2.
70 *Erfurth*, NJOZ 2009, 2914, 2922; *Polenz*, DuD 2009, 561, 563; *Schmidt*, RDV 2009, 193, 198.

Datenschutz im Bewerbungsverfahren 151

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

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. 152

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". 153

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. 154

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. 155

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. 156

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[71] 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.[72] 157

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

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

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.[73] 158

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 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. 159

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.[74] 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.[75] 160

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.[76] 161

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. 162

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. 163

73 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.

74 *Rolf/Rötting,* RDV 2009, 263, 266; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437; *Oberwetter*, BB 2008, 1562, 1564.

75 *Simitis*, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, § 28 Rn 189.

76 *Forst*, NZA 2010, 427, 432; *Rolf/Rötting*, RDV 2009, 263, 266 f.; *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2437.

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 hochzuladen 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. **164**

Die Datenerhebung aus derartigen berufsorientierten Netzwerken ist ohne Einwilligung des Betroffenen nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG zulässig. **165**

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. **166**

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. **167**

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. **168**

Nicht berücksichtigte Bewerber

Die weitere Speicherung personenbezogener Daten von abgewiesenen Bewerbern ist in aller Regel nicht mehr erforderlich.[77] Das allgemeine Persönlichkeitsrecht schließt das Recht ein, darüber zu bestimmen, **169**

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

ob der Arbeitgeber die im Bewerbungsverfahren erfragten persönlichen Daten aufbewahren darf oder ob deren Vernichtung verlangt werden kann.

Datenschutz im Rahmen bestehender Beschäftigungsverhältnisse 170

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.

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. 171

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. 172

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.[78] 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.[79] 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.[80] 173

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,[81] 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.[82] Darüber hinaus können im Rahmen der Einwilligung die technischen und organisa- 174

78 *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.

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

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

81 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.

82 *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.

torischen 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.[83]

175 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, weil nach herrschender Auffassung insbesondere auch eine konkludente Gestattung der privaten Nutzung von E-Mail und Internet im Arbeitsverhältnis in Betracht kommt.[84] 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.

176 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.

177 *Merke!*

- 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.

178 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.[85] Dies gilt sowohl für die äußeren Verbindungsdaten als auch für die Inhaltsdaten einer dienstlichen E-Mail.

179 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.

180 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

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

84 *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.

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

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.

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 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. **181**

Arbeitnehmerdaten im Internetauftritt des Unternehmens

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. **182**

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. **183**

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:[86] 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 zurzeit 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 „zurzeit im Krankenstand" war von dem Landesdatenschutzbeauftragten[87] – zu Recht – als besonderes personenbezogenes (Gesundheits-)Datum eingestuft worden.[88] Seine Veröffentlichung war dementsprechend nicht zulässig. **184**

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. **185**

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

186 *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
- Nur mit Einwilligung des Betroffenen zulässig:
- Bekanntgabe der Privatanschrift
- Private Erreichbarkeit per Telefon
- Fotos
- Staatsangehörigkeit
- Angaben zur Konfession
- Gewerkschaftszugehörigkeit

K. Die EU-Datenschutzgrundverordnung

187 **Die DSGVO kommt – Was sich 2018 in der Anwaltskanzlei in Sachen Datenschutz ändern wird oder zumindest ändern könnte….!**

188 **Datenschutzrecht 2015 & 2016**

Das Datenschutz-Jahr 2016 war vornehmlich durch weitreichende Änderungen auf europäischer Ebene geprägt. So hatte der EuGH noch Ende 2015 die Bestimmungen zum „sicheren Hafen" (Safe Habor) umgestoßen und den Datentransfer zwischen der EU und den USA auf Grundlage der hierzu bestehenden Sondervorschriften (Entscheidung 2000/520/EG der Kommission vom 26.7.2000) nicht nur in Frage gestellt, sondern die Übermittlung personenbezogener Daten auf Grundlage der Entscheidung 2000/520/EG zukünftig untersagt. Die Entscheidung war mehr als ein Sturm im Wasserglas und führte insbesondere bei internationalen (Groß-)Konzernen zu Aufregung. Für den im Datenschutzrecht beratenden Rechtsanwalt sicherlich ein Geschenk aus Luxemburg, für die betroffenen Unternehmen jedoch eine Hiobsbotschaft, auf die man gerne verzichtet hätte. Doch mit der Safe-Habor-Entscheidung[89] war es in Sachen Datenschutzrecht Ende 2015 nicht getan: Am 15.12.2015 endeten die sog. **Trilogverhandlungen** über eine Europäische Datenschutzgrundverordnung (DSGVO) mit einer Einigung. Am 14.4.2016 passierte die DSGVO das EU-Parlament, am 4.5.2016 erfolgte ihre Veröffentlichung im Amtsblatt der Europäischen Union.[90] 20 Tage später, am 25.5.2016, trat die Verordnung offiziell in Kraft (Art. 99 Abs. 1 DSGVO). Ab dem 25.5.2018 (Art. 99 Abs. 2 DSGVO) finden die dort niedergelegten Datenschutzvorgaben in den Mitgliedstaaten unmittelbar Anwendung.

89 EuGH, Urt. v. 6.10.2015 – C-362/14, abrufbar unter: http://openjur.de/u/859036.html.

90 Amtsblatt EU L 119/1 v. 4.5.2016, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE.

Die DSGVO 189

Die DSGVO bringt zum Teil weitreichende Änderungen des Datenschutzrechts mit sich und zwingt in vielen Bereichen zu einem (datenschutz-)rechtlichen Umdenken im Rechtsverständnis und vor allem der Rechtsanwendung. Als EU-Verordnung tritt die DSGVO an die Stelle nationaler Datenschutz-Gesetzte. Nicht nur das BDSG als zentrales Datenschutzgesetz, sondern auch die zahlreichen, in Deutschland beispielsweise im Bereich des Sozial- und Versicherungsrechts, vorzufindenden sondergesetzlichen Regelungen werden ab dem 25.5.2018 nur noch **bedingt anwendbar** sein.

Als Leser dürfen Sie über unsere vorstehende Formulierung zu Recht verwundert sein: Warum sprechen wir an dieser Stelle im Zusammenhang mit einer EU-Verordnung nicht von genereller Unanwendbarkeit nationalstaatlicher Gesetzgebung, sondern (bewusst) von bedingter Anwendbarkeit? Eigentlich, dies ist Ihnen zuzugestehen, kann es doch eine bedingte Anwendbarkeit vor dem Hintergrund der Zwecksetzung einer EU-Verordnung, die bekannter Maßen einen einheitlichen und im Gegensatz zur Richtliniengesetzgebung unmittelbar anwendbaren europäischen Rechtsrahmen schaffen und etablieren will, gar nicht geben. Mit dieser Zielsetzung war die EU auch ursprünglich angetreten; wie so oft, scheiterte eine Vollharmonisierung schlussendlich an nationalstaatlichen Einzelinteressen, so dass die DSGVO eine **Kompromisslösung** darstellt, die als „**Verordnung light**" bezeichnet werden kann. 190

Tatsächlich sieht die DSGVO in zahlreichen Kernbereichen die sog. **Öffnungsklausel** vor, die es dem nationalen Gesetzgeber gestattet, von den Vorgaben der DSGVO auf nationaler Ebene abzuweichen und hier nicht nur strengere, sondern grundsätzlich auch hinter dem Schutzniveau der DSGVO zurückbleibende nationale Sonderwege zu beschreiten. 191

> *Ein Beispiel:*
>
> Die DSGVO (Art. 37) sieht – anders als § 4f BDSG – keine grundsätzliche Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten ab einer bestimmten Mitarbeiterzahl vor, sondern stellt auf die Kategorien der verarbeiteten Daten und/oder die Tätigkeit des Verantwortlichen ab. Gem. Art. 37 Abs. 4 DSGVO kann nach dem Recht der Mitgliedstaaten vorgeschrieben werden, dass abweichend hiervon gleichwohl ein Datenschutzbeauftragter zu bestellen ist.

Aus hiesiger Sicht steht zu erwarten, dass in Deutschland von dieser Öffnungsklausel Gebrauch gemacht und die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten bei Erreichen einer bestimmten Mitarbeiterzahl aufrechterhalten wird. Ob insoweit die Neun-Personen-Grenze des § 4f Abs. 1 BDSG bestehen bleibt oder – was wünschenswert wäre – die Mindestbeschäftigtenzahl angehoben wird, bleibt abzuwarten. Anfang September ist jedenfalls ein erster Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) aufgrund heftiger Auseinandersetzungen zwischen BMI, BMJ und BfDI schnell wieder zurückgenommen worden.[91] Hier war explizit offen gelassen worden, ob von der Öffnungsklausel in Art. 37 Abs. 4 DSGVO überhaupt Gebrauch gemacht werden soll.

Die Auseinandersetzungen um das DSAnpUG-EU sind der Grund dafür, warum wir an dieser Stelle und im Rahmen der vorliegenden Neuauflage unseres Werkes noch davon absehen, Ihnen eine Broschüre zum Datenschutz- und zur Datensicherheit in der Anwaltskanzlei unter Geltung der DSVGO zu präsentieren. In Bezug auf die Öffnungsklauseln ist aktuell noch zu vieles im Fluss und unausgereift. Es ist zwar davon auszugehen, dass die Bundesregierung noch vor der Bundestagswahl wesentliche Umsetzungsmaßnahmen in Bezug auf die Öffnungsklauseln der DSGVO vollziehen wird; aktuell ist dies indes noch nicht geschehen. Wir gehen davon aus, dass die vierte Auflage der vorliegenden Broschüre im Jahre 2017 bundesdeutsche Umsetzungsmaßnahmen in Bezug auf die Öffnungsklauseln der DSGVO wird berücksichtigen können. 192

91 Hierzu: https://netzpolitik.org//wp-upload/2016/09/Referentenentwurf_DSAnpUG_EU.pdf.

Problemlagen aus Sicht der Rechtsanwaltschaft 193

Bereits heute zeichnen sich jedoch eine Reihe von Problemlagen ab, die mit dem Wirksamwerden der DSGVO auch für den Rechtsanwalt Bedeutung erlangen werden. Zuerst gilt es hier darauf hinzuweisen, dass die DSGVO keine Regelung enthält, die mit § 1 Abs. 3 BDSG vergleichbar ist (hierzu oben Abschnitt A. Rdn 13 ff.) und die Frage des (partiellen) Vorrangs berufs- und strafrechtlicher Regelungen unter Geltung der DSVGO einer erneuten Diskussion bedarf.

Kein genereller Vorrang des Berufs- und Standesrechts mehr – DSGVO als Befugnisnorm für Offenbarungshandlungen nach § 203 StGB? 194

Dies hat unmittelbare Auswirkungen auf die anwaltliche Tätigkeit als solche. So wird die Frage des Verhältnisses datenschutzrechtlicher Erlaubnistatbestände zu § 203 StGB näher zu beleuchten und zu beantworten sein, ob die in der DSGVO normierten Vorgaben zum Umgang mit personenbezogenen Daten als Befugnisnormen im Sinne des § 203 StGB zu behandeln sind. Eine Bejahung dieser Fragestellung könnte die Etablierung von Outsourcing-Maßnahmen in der Rechtsanwaltskanzlei erheblich erleichtern. Bislang gilt, dass die Vorgaben zur Auftragsdatenverarbeitung in § 11 BDSG nicht dazu führen können, dass ein „unbefugtes" Offenbaren im Sinne des § 203 StGB zu verneinen wäre. Maßgeblich ist dieser Umstand indes auf den Anwendungsvorrang des § 203 StGB bzw. der berufsrechtlichen Regelungen zur anwaltlichen Verschwiegenheit zurückzuführen. Einen derartigen generellen Vorrang kennt die DSGVO wie beschrieben nicht. Fraglich ist also, ob die rechtmäßige Einschaltung eines Auftragsverarbeiters (Art. 28 DSGVO), der als Teil des „Verantwortlichen" behandelt und nur auf Weisung des Verantwortlichen tätig wird, weiterhin ausnahmslos der Einwilligung durch den Betroffenen (Mandanten) bedarf oder eine solche Einschaltung auch einwilligungslos erfolgen kann, solange und soweit der Auftragsverarbeiter nur die in Art. 28 DSGVO normierten Garantien einhält und die an ihn gestellten Pflichtanforderungen gegenüber dem Verantwortlichen (Rechtsanwalt) erfüllt. Fakt ist jedenfalls, der Auftragsverarbeiter ist nicht „Dritter" (Art. 4 Nr. 10 DSGVO) im Sinne der DSGVO und agiert damit nicht „außerhalb des Verantwortlichen". Er könnte insoweit den „berufsmäßigen Gehilfen" des Rechtsanwaltes gegenüber denen ein „unbefugtes Offenbaren" nach absolut h.M. ausscheidet, gleichzustellen sein. Die DSGVO würde insoweit das vollenden, was die Satzungsversammlung der BRAK mit der zum 1.7.2015 in Kraft getretenen Neuregelung des § 2 BORA (hierzu bereits unter: A. Rdn 9) angestoßen hat und mangels entsprechender Rechtsetzungsbefugnis nicht vollenden konnte. Nämlich die Grenzen der anwaltlichen Verschwiegenheitspflichten zugunsten „sozialadäquater" Verhaltensweisen zu erweitern und das non-legal Outsourcing „entpönalisieren".

Neue Informationspflichten gegenüber dem Mandanten? 195

Weiterhin werden die Regelungen zu Auskunftspflichten und Informationsrechten in Art. 13 bis 15 DSGVO einer näheren Betrachtung in Bezug auf ihre Auswirkungen für die anwaltliche Berufsausübung zu unterziehen sein. Nach dem erklärten Willen des europäischen Gesetzgebers soll jede betroffene Person ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken seine personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann (Erwägungsgrund 63 der DSGVO). Korrespondierend hierzu normiert Art. 13 DSGVO umfangreiche Informationspflichten des Verantwortlichen gegenüber dem Betroffenen bei der erstmaligen Erhebung von personenbezogenen Daten beim Betroffenen selbst (Direkterhebung). Die hier normierten Verpflichtungen gehen z.T. weit über die bisherigen Vorgaben im BDSG hinaus. Zwar sieht Art. 13 Abs. 4 DSGVO die Möglichkeit eines Absehens von der Informationsverpflichtung vor, diese soll indes nur dann greifen, wenn und soweit die betroffene Person bereits über die in Art. 13 DSGVO geregelten (Pflicht-)Informationen verfügt. Dies wird mit Blick auf die allgemeinen Informationspflichten des Art. 13 Abs. 1 DSGVO; mit Blick

auf die in Art. 13 Abs. 2 DSGVO geregelten weitergehenden Informationen, dürfte sich indes auch im Anwalt-Mandanten-Verhältnis zukünftig eine Informationsverpflichtung auf Seiten des Rechtsanwalts ergeben. So ist der Betroffene (Mandant) bei erstmaliger Erhebung personenbezogener Daten (in der Regel bei Mandatsbegründung) über die Dauer, für die die personenbezogenen Daten gespeichert werden, jedenfalls aber über die Kriterien für die Festlegung dieser Dauer zu informieren; ebenso sind Informationen zu Auskunfts-, Beschwerde-, Löschungs- und Widerrufsrechten zu geben. Insbesondere die Auskunftsrechte (Art. 15 DSGVO) sind hier interessant. So soll der Betroffene ein Recht auf Auskunft über seine eigenen personenbezogenen Daten haben, was die Übermittlung von in der Anwaltsakte gespeicherten Daten umfasst. Das Auskunftsrecht gilt insoweit absolut und ohne Einschränkung. Die Auskunft ist grundsätzlich binnen Monatsfrist zu erteilen und sie darf nicht von der Erstattung der Kosten für Abschriften/Ausdrucke abhängig gemacht werden (Art. 14 Abs. 3 DSGVO). Vor dem Hintergrund, dass die DSGVO – wie beschrieben – keine Ausnahme zugunsten bereichsspezifischer Normen vorsieht, dürfte das Recht auf eine kostenfreie Erstkopie auch auf die Einsichtnahme in die Anwaltsakten zu erstrecken sein. Ob daher – wie aktuell – auch zukünftig Zurückbehaltungsrechte bei offenen Honoraren geltend gemacht, oder die im RVG für die Anfertigung von Kopien normierte Auslagenerstattung vom Mandanten gefordert werden kann, ist fraglich.

Recht auf Datenübertragbarkeit – „Anwalt gib mir Deine Dateien“ 196

Gänzlich neu und bislang unbekannt ist das in Art. 20 DSGVO normierte „**Recht auf Datenübertragbarkeit**“. Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, gewährt die DSGVO der betroffenen Person das Recht, personenbezogene Daten, die sie einem Verantwortlichen zur Verfügung gestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Das Recht auf Datenübertragbarkeit greift dort, wo die Verarbeitung auf einer **Einwilligung** gemäß Art. 9 Abs. 2 lit. a) DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b) DSGVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Dies dürfte im Anwalt-Mandanten-Verhältnis grundsätzlich der Fall sein, so dass es durchaus möglich erscheint, dass sich aus dem Anwaltsvertrag beispielsweise im Falle des Beraterwechsels zukünftig ein „Recht auf Datenübertragbarkeit“ zugunsten des Mandanten ergeben könnte. In diesem Fall würde man nicht nur das Mandat verlieren, sondern müsste auch für die Übertragbarkeit der gespeicherten Mandatsinformationen an den neuen Kollegen Sorge tragen.

Weiterhin keine Auskunftspflichten gegenüber Gegnern, aber was ist mit den Aufsichtsbehörden? 197

Aufatmen können wir im Hinblick auf Auskunftsansprüche der Gegenseite. Hier normieren Art. 14 Abs. 5 lit. d und Art. 15 Abs. 5 lit. d DSGVO in erfreulicher Deutlichkeit, dass die in Art. 14 und Art. 15 DSGVO geregelten Informationspflichten und Auskunftsrechte der DSGVO im Anwalt-Gegner-Verhältnis keine Anwendung finden.

Es bleibt zu hoffen, dass der Bundesgesetzgeber auch von der in Art. 90 DSGVO bestehenden Möglichkeit Gebrauch machen wird, die Befugnisse der Aufsichtsbehörden gegenüber Rechtsanwälten als dem Berufsgeheimnis unterliegenden Verantwortlichen zu beschränken. Dabei sollte er klarstellen, dass unter Geltung der DSGVO generell weder Auskunftspflichten noch Betretungsrechte der Aufsichtsbehörden gegenüber Rechtsanwälten bestehen. 198

Neue Anforderungen an Hard- und Software 199

Die DSGVO normiert in Art. 25 eine generelle Verpflichtung zum „**Datenschutz durch Technikgestaltung**“ und fordert vom Verantwortlichen die Etablierung geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen

der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Dies wird neue Anforderungen an die Daten- und Systemsicherheit in der Rechtsanwaltskanzlei nach sich ziehen und die in diesem Werk seit der ersten Auflage geforderten Datensicherheitsmaßnahmen zur Pflichtaufgabe in der Kanzlei erheben. So ist u.a. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Software), die im Zusammenhang mit der Verarbeitung personenbezogener Daten zum Einsatz kommen, sicherzustellen. Ebenso sind personenbezogene Daten und der Zugang zu ihnen verfügbar zu halten und dafür Sorge zu tragen, dass diese auch bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Art. 32 DSGVO). Dies erfordert konsequentere Sicherheitsmaßnahmen und -konzepte, als sie bislang in den meisten Rechtsanwaltskanzleien vorzufinden sind. Ob sämtliche am Markt angebotenen Softwarelösungen die vorgenannten Kriterien erfüllen, ist ebenso fraglich. Auch hier wird sich in den kommenden eineinhalb Jahren Handlungsbedarf ergeben.

Pflicht zur Datenschutzfolgenabschätzung 200

Partiell aufatmen dürften wir, was die in Art. 35 DSGVO normierte Verpflichtung zur Erarbeitung einer sog. **Datenschutz-Folgenabschätzung** angeht. Diese soll nach Erwägungsgrund 91 der DSGVO für die Verarbeitung personenbezogener Daten von Mandanten durch einen einzelnen Rechtsanwalt, jedenfalls keine Anwendung finden. Erwägungsgrund 91 spricht explizit vom „**einzelnen Rechtsanwalt**“, so dass sich eine Verpflichtung zur Anfertigung einer Datenschutz-Folgenabschätzung u.U. für Rechtsanwaltszusammenschlüsse ergeben könnte. Auch hier bleibt zu hoffen, dass der Gesetzgeber von der Öffnungsklausel Gebrauch macht und Rechtsanwälte generell und mit Blick auf die strikten Vorgaben des Berufs- und Standesrechts generell von der Verpflichtung zur Erstellung einer Datenschutz-Folgenabschätzung freistellen wird.

Zusammenfassung 201

Die DSGVO bringt also eine Menge Veränderungen mit sich. Diese Veränderungen könnten, wenn der Gesetzgeber hier nicht über entsprechende Öffnungsklauseln reagiert, auch auf die anwaltliche Berufsausübung erhebliche Auswirkungen entfalten. Da bislang noch nicht abzusehen ist, wo sich der Gesetzgeber für die Einführung von nationalstaatlichen Sondervorgaben entscheidet, bleibt zu hoffen, dass DAV und BRAK sich hier in Stellung bringen und den Gesetzgeber auf die Notwendigkeit der Schaffung von Sondervorschriften für die Rechtsanwaltschaft aufmerksam machen. Spätestens in der 4. Auflage dieses Werkes, Ende 2017 werden wir Ihnen hierzu hoffentlich ausführlicher und konkreter berichten können.

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.

Begriff	Erläuterung
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).
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).

Begriff	Erläuterung
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.
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.

Begriff	Erläuterung
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.
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.

Begriff	Erläuterung
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.
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).

Begriff	Erläuterung
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.
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.

Begriff	Erläuterung
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).
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).

Die EU-Datenschutz-Grundverordnung kommt – jetzt informieren!

Die Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis

Von RA Dr. Robert Kazemi
1. Auflage 2017, ca. 400 Seiten,
gebunden, ca. 139,00 €
ISBN 978-3-8240-1450-7
Erscheint Februar 2017

Die EU-Datenschutz-Grundverordnung hat das EU-Parlament am 14.4.2016 ohne Ablehnung und Änderungen in der konsolidierten Fassung des EU-Ministerrates passiert. Damit ist es amtlich: **Ab 1. Januar 2018 gilt in Europa ein neues Datenschutzgesetz.**

Auf 200 Seiten verpflichtet der neue Verordnungstext die Unternehmen, klare Regeln beim Umgang mit Daten zu befolgen. **Verstöße haben drastische Folgen**. Bis zu 20 Millionen Euro oder bis zu **4 Prozent des weltweiten Konzernumsatzes** können die Bußgelder betragen, wobei jeweils der höhere Wert gilt.

Damit ist die neue EU-Datenschutz-Grundverordnung ein wirkungsvolles Instrument, das den **Beratungsbedarf rasant steigen** lassen wird – sowohl **bei mittelständischen Unternehmen wie bei großen Konzernen**.

Profitieren Sie rechtzeitig von dieser Entwicklung und verschaffen Sie sich mit dem **Werk zur EU-Datenschutz-Grundverordnung** von RA Dr. Robert Kazemi einen **klaren Wettbewerbsvorteil**.

„Die Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis" bietet Ihnen eine **komprimierte Darstellung der neuen Rechtslage** – inklusive einer **Gegenüberstellung** der alten und neuen Gesetzeslage.

Sie erhalten umfassende und **sofort nutzbare Informationen** zu allen Inhalten des neuen Gesetzes. Darunter:

- Von **welchen Grundsätzen** geht die neue Verordnung aus?
- Welche **Datenfallen** lauern **im Vertrieb**, welche bei der Datennutzung und -verarbeitung im **Marketing**?
- **Welche Rechte haben Kunden** hinsichtlich Information, Löschung und Berichtigung?
- Welche Folgen haben **Verstöße**?

Gehen Sie gemeinsam mit Ihren Mandanten **auf Nummer sicher** – denn nur Unternehmen, die Datenbestände und Datenverarbeitungsprozesse **rechtzeitig nach den neuen Vorgaben analysieren und umstellen**, sind auf der sicheren Seite.

Der **Autor Rechtsanwalt Dr. Robert Kazemi** arbeitet seit Jahren auf dem Gebiet des Datenschutzrechts. Er ist **Autor des Fachbuches** „Das neue Datenschutzrecht in der anwaltlichen Beratung" sowie **zahlreicher weiterer Publikationen** zum Thema.

Bestellen Sie jetzt Ihre Lagerexemplare:
Telefon: 0228 91911-34 · Fax 0288 91911-24

perfekt beraten

DeutscherAnwaltVerlag

Impressum

Autoren

Dr. Robert Kazemi
Rechtsanwalt, Bonn
kanzlei@medi-ip.de

Dr. Thomas H. Lenhard
Sachverständiger für IT und Datenschutz, Rodalben
dr.lenhard@it-planung.com

DeutscherAnwaltVerlag

Rochusstr. 2–4
53123 Bonn

Hinweis:

Die Ausführungen in diesem Werk 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. Herausgeber, Autoren und Verlag übernehmen keinerlei Haftung für die Richtigkeit und Vollständigkeit der in diesem Buch enthaltenen Ausführungen.

Hinweise zum Urheberrecht:

Die Inhalte dieser eBroschüre wurden mit erheblichem Aufwand recherchiert und bearbeitet. Sie sind für den Bezieher zur ausschließlichen Verwendung zu internen Zwecken bestimmt.

Dementsprechend gilt Folgendes:

- Die schriftliche Verbreitung oder Veröffentlichung (auch in elektronischer Form) der Informationen aus dieser eBroschüre darf nur unter vorheriger schriftlicher Zustimmung durch die Deutscher Anwaltverlag & Institut der Anwaltschaft GmbH erfolgen. In einem solchen Fall ist der Deutsche Anwaltverlag als Quelle zu benennen.
- Unter „Informationen" sind alle inhaltlichen Informationen sowie bildliche oder tabellarische Darstellungen von Informationen aus dieser eBroschüre zu verstehen.
- Jegliche Vervielfältigung der mit dieser eBroschüre überlassenen Daten, insbesondere das Kopieren auf Datenträger sowie das Bereitstellen und/oder Übertragen per Datenfernübertragung ist untersagt. Ausgenommen hiervon sind die mit der Nutzung einhergehenden, unabdingbaren flüchtigen Vervielfältigungen sowie das Herunterladen oder Ausdrucken der Daten zum ausschließlichen persönlichen Gebrauch. Vom Vervielfältigungsverbot ausgenommen ist ferner die Erstellung einer Sicherheitskopie, soweit dies für die Sicherung künftiger Benutzungen dieser eBroschüre zum ausschließlich persönlichen Gebrauch notwendig ist. Sicherungskopien dürfen nur als solche verwendet werden.
- Es ist nicht gestattet, diese eBroschüre im Rahmen einer gewerblichen Tätigkeit Dritten zur Verfügung zu stellen, sonst zugänglich zu machen, zu verbreiten und/oder öffentlich wiederzugeben.