Mag. Markus Dörfler, LL.M.
Rechtsanwalt
IT-Recht Datenschutzrecht Immaterialgüterrecht

155/09/31/md/1785-1.doc

Stand: 9.12.2015

Autoreninfo: Von Mag. Markus Dörfler, LL.M. Der Autor ist Rechtsanwalt in Wien und auf IT-Recht, Immaterialgüterrecht und Datenschutzrecht spezialisiert. Neben seiner Tätigkeit als Vortragender auf der FH(BFI) für IT-Recht, ist er Mitherausgeber des Fachbuchs “Rechtsberatung Internet” des WEKA-Verlags.

Die E-Mail: Verletzung von Ansehen und Ehre des Standes?

In den letzten Jahren hat sich der Anwaltsberuf drastisch verändert: er wurde schneller! Der Brief wurde durch das Fax abgelöst, dieses durch die E-Mail. Zugegebener Maßen scheint das im ersten Moment nicht viel mit dem Standesrecht der Rechtsanwälte zu tun zu haben, tatsächlich befinden sich die Rechtsanwälte durch die allumfassende Erreichbarkeit und schnelle Kommunikation auf einem standesrechtlich gefährlichen Terrain.

Zur Erinnerung: „*Der Rechtsanwalt ist zur Verschwiegenheit über die ihm anvertrauten Angelegenheiten und die ihm sonst in seiner beruflichen Eigenschaft bekanntgewordenen Tatsachen, deren Geheimhaltung im Interesse seiner Partei gelegen ist, verpflichtet.[…]*“[1] Schon der OGH hat im Jahr 2002 festgehalten, dass „*die Verschwiegenheitsverpflichtung des Rechtsanwaltes gemäß § 9 Abs 2 RAO […] eine Norm [ist], die eine unabdingbare Voraussetzung für die Ausübung des Rechtsanwaltsberufes darstellt, sie ist zentrales Element der Berufsausübung der Rechtsanwaltschaft. […]*“[2]

Das Gut der Verschwiegenheit wird von den Rechtsanwälten – zu Recht – hochgehalten, jedoch permanent unbewusst stückchenweise abgetragen und relativiert.

Die den Rechtsanwälten auferlegte Verschwiegenheitspflicht betrifft naturgemäß nicht nur verbale Äußerungen, sondern auch den Schriftverkehr mit den Mandanten. Dies ist mit einer der Gründe, warum Rechtsanwälte ihren Mandanten keine Postkarten senden, sondern (verschlossene) Briefe[3]. Der technische Fortschritt und die damit verbundene Beschleunigung der Kommunikation führt jedoch dazu, dass – aus Gründen der Einfachheit – in der heutigen Zeit nahezu ausschließlich elektronische *Post*karten gesendet werden (anstelle von elektronischen Briefen).

---

[1] § 9 Abs 2 RAO.
[2] OGH vom 02.09.2002 zu 4 Bkd 1/02.
[3] Auf den grundrechtlichen Schutz des Brief- und Fernmeldegeheimnisses wird hier nicht näher eingegangen.

Mariahilfer Strasse 20
A-1070 Wien

RLB NÖ-Wien BIC: RLNWATWW
IBAN: AT40 32000 00011518016

Tel.: +43 1 521 75 - 0
Fax: +43 1 521 75 - 37

UID: ATU66953923
DVR 4007303

office@it-rechtsanwalt.at
www.it-rechtsanwalt.at

RLB NÖ-Wien BIC: RLNWATWW
Anderkonto IBAN: AT11 32000 00011522224

Die E-Mail

Technisch gesehen werden bei einer E-Mail Absender, Empfänger, Betreff und der Inhalt der E-Mail aufgrund eines speziellen Protokolls[4] über das Internet von einem Server zu nächsten geleitet, bis die E-Mail beim Server des Empfängers einlangt und in das Postfach des Empfängers einsortiert wird. Dieser kann die E-Mail anschließend mit seinem Benutzernamen und Passwort lesen.

Im Rahmen dieser (normalen) E-Mail, welche faktisch den Standardfall darstellt, gibt es weder einen Schutz vor dem Verändern der E-Mail, noch vor dem (unbefugten) Lesen mit Ausnahme des Benutzernamens und des Passwortes. Da dieses jedoch am Endgerät hinterlegt ist (und damit niemals eingegeben werden muss) ist der Zugriff auf das E-Mailpostfach unbeschränkt möglich, sofern ein Zugriff auf das Endgerät möglich ist.

Ferner bedeutet das, dass jedermann, der Zugriff zum Netzwerk hat, über das die E-Mail geleitet wird, den Inhalt der E-Mail lesen kann. Dies beinhaltet (oft) sogar lokale Netzwerke von Rechtsanwaltskanzleien. Mit anderen Worten: Jeder Server im Internet, über den die E-Mail geleitet wird, kann den Inhalt mitlesen, ohne eine Sicherheitsvorkehrung umgehen zu müssen. Da der Weg im Internet faktisch nicht nachvollziehbar ist, können das neben den jeweiligen Internetprovidern, auch staatlichen Behörden und Kriminelle (Hacker) sein. Die hier Genannten sind darüber hinaus in der Lage, den Inhalt der E-Mail nach Belieben zu manipulieren, ohne, dass dies für den Empfänger nachvollziehbar wäre.

Aus diesem Grund ist das Pendant zur E-Mail auch die Postkarte und nicht (wie oftmals fälschlich angenommen) der Brief. Der Informationsgehalt wird von A nach B Transportiert und jeder, der mit dem Transport befasst ist, kann die Information lesen.

Das praktische, weil schnelle Kommunikationsmedium „E-Mail“ wird in den letzten Jahren verstärkt durch das Smartphone ergänzt, welches den Abruf und das Versenden von E-Mails jederzeit und überall ermöglicht. Der Rechtsanwalt hat daher zu jederzeit und überall Zugriff auf die gesamte E-Mail-Kommunikation mit seinen Mandanten – und damit auf sämtliche Informationen, welche der Verschwiegenheitsverpflichtung des § 9 Abs 2 RAO unterliegt.

Verschlüsselung

Um Dritten die Möglichkeit zu nehmen, einerseits den Inhalt einer E-Mail zu lesen (Verschlüsselung) und andererseits den Inhalt zu manipulieren (Signierung) gibt es zahlreiche Verfahren. Geläufige Produkte dazu sind PGP[5], welches auch kostenlos zur Verfügung gestellt wird, sowie die von A-Trust (kommerziell) angebotenen Produkte. A-Trust bietet dabei auch qualifizierte Zertifikate an, welche eine qualifizierte digitale Sig-

[4] SMTP (Simple Mail Transfer Protocol) gemäß der RFC 821 vom August 1982, aktualisiert mit der RFC 5321 vom Oktober 2008.
[5] Pretty Good Privacy.

natur nach dem Österreichischen Signaturgesetz umfassen.

Voraussetzung für die Verschlüsselung von E-Mails ist, dass der Empfänger über dieselben (technischen) Voraussetzungen wie der Sender verfügt. Nur so kann dieser eine E-Mail entschlüsseln bzw. die Integrität prüfen.

Die technische Hürde liegt hierbei weniger bei den Rechtsanwälten, da diese mit der Einführung der Ausweiskarte mit elektronischer Anwaltssignatur[6] über ein entsprechendes Zertifikat von A-Trust verfügen, sondern üblicherweise bei den Mandanten, welche über keine der genannten technischen Einrichtungen verfügen.

Um diese technische Hürde leichter meistern zu können, hat der österreichische Rechtanwaltskammertag gemeinsam mit der Notariatskammer und der Wirtschaftskammer Österreich das TrustNetz.at geschaffen. Das Trustnetz stellt dabei eine Verknüpfung des Elektronischen Rechtsverkehrs (ERV) mit der sogenannten E-Zustellung dar.

Bei der E-Zustellung (www.e-zustellung.at) werden Postsendungen verschlüsselt und signiert dem Empfänger in sein zugewiesenes Postfach übermittelt (gleich wie bei einer verschlüsselten und signierten E-Mail). Neben der wesentlich einfacheren Handhabung, ist der wesentliche Unterschied zur E-Mail, dass die Zustellung mit einem Zustellnachweis erfolgt (wie einem eingeschriebenen Brief), sodass der Sender auch Kenntnis über den Eingang des Schriftstückes beim Empfänger erlangt. Die E-Zustellung steht dabei jedem offen, einzige Voraussetzung für den Empfang ist eine kostenlose Anmeldung (lediglich bei der Übersendung der Nachrichten fallen Kosten an).

Aufgrund der Verknüpfung der E-Zustellung mit dem ERV über das TrustNetz hat der Rechtsanwalt die Möglichkeit, **ohne Änderung** seiner bestehenden Infrastruktur (die Teilnahme am ERV ist für Rechtsanwälte verpflichtend[7]) mit seinen Mandanten verschlüsselt und signiert zu kommunizieren.

Rechtliche Konsequents

Die Tatsache, dass ein Dritter im Falle von unverschlüsselten E-Mails ohne größeren Aufwand Kenntnis vom Inhalt einer Rechtsanwalt-Klient-Kommunikation erlangen kann, steht in einem großen Spannungsverhältnis zur anwaltlichen Verschwiegenheitspflicht. Selbst wenn man jene Fälle ignoriert, in denen sich Kriminelle Zugang zu E-Mail-Postfächern verschaffen, bleiben die Fälle, in denen die mit dem Transport der E-Mail betrauten Unternehmen Kenntnis des Inhaltes (faktisch) erlangen.

---

[6] Richtlinie gemäß § 37 Abs 1 Z 1a RAO über Ausweisekarten mit elektronischer Anwaltssignatur (Ausweis-RL) vom 3.10.2006.
[7] § 9 Abs 1a RAO.

Unbestritten rechtlich unzulässig[8] (und daher wohl jedenfalls die Standesregeln der Rechtsanwälte verletzend) ist die Nutzung von E-Mail-Diensten, welche im EU-Ausland ansässig sind (beispielsweise die USA), oder die Datenspeicherung in der EU nicht garantieren, sowie jene E-Mail-Dienste, die bis zuletzt durch das Safe-Harbour-Abkommen zulässig waren[9].

Zur E-Mailnutzung und anwaltliche Verschwiegenheit hat *Mosig* bereits 2001[10] ausführlich und nachvollziehbar dargelegt, dass jener Schutz, der Briefen zukommt[11], nicht auf E-Mails anwendbar ist. Andere Rechtsnormen (etwa § 119 StGB) schützen dabei jedes Stadium des E-Mail-Transportes[12]. In weiterer Folge führt *Mosig* aus, dass es für den „*nicht unbeträchtlichen Arbeits- und auch Kostenaufwand*“[13] keine sachliche Rechtfertigung für die Nutzung von kryptografischen Verfahren gibt, da mit entsprechender krimineller Energie sowohl Briefe, als auch E-Mail durch unbefugte Dritte gelesen werden können.[14] Er zieht daraus den Schluss, dass die E-Mail-Nutzung durch die Verpflichtung, kryptographische Verfahren zu nutzen, ungerechtfertigt diskriminiert würde, sodass die Nutzung von unverschlüsselter E-Mail-Kommunikation keine Verletzung der anwaltlichen Verschwiegenheitspflicht darstellt.

In Anbetracht des technischen Fortschritts kann die Frage, ob dieser Schluss damals korrekt war, unbeantwortet bleiben. Die Art der Kommunikation zwischen Rechtsanwälten und ihren Mandanten hat sich in den letzten 14 Jahren stark gewandelt, sodass jedenfalls eine neue Beurteilung notwendig ist. War im Jahr 2001 die Nutzung des E-Mail-Dienstes eher die Ausnahme, stellt diese heute den Regelfall dar. Wie bereits ausgeführt, werden ferner E-Mails mit Hilfe von Smartphones überall gelesen, was in die Beurteilung ebenso einfließen muss.

§ 9 Abs 2 RAO liefert keinerlei Anhaltspunkte zur Frage, welche Maßnahmen im Zusammenhang mit der Versendung von E-Mails ergriffen werden müssen, sodass auf die allgemeinen Regeln des Datenschutzgesetzes zurückgegriffen werden muss. § 14 Abs 1 DSG 2000 sieht dabei vor, dass der Auftraggeber (im konkreten Fall: der Rechtsanwalt) für alle „*Organisationseinheiten Maßnahmen zur Gewährleistung der Datensicherheit zu treffen [hat]. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust ge-*

---

[8] Siehe dazu: §§ 12 DSG 2000.

[9] Dieses Abkommen hat der EuGH jedoch mit 6.9.2015 für ungültig erklärte. Siehe dazu auch Österreichisches Anwaltsblatt 2015, 586.

[10] *Mosig,* Die E-Mail-Nutzung im Lichte der anwaltlichen Verschwiegenheitspflicht, AnwBl 2001, 440.

[11] Etwa § 118 StGB.

[12] Heute: §§ 118a ff StGB.

[13] *Mosig* aaO.

[14] Die von *Mosig* aufgeworfene Frage, ob die private Verwendung von kryptographischen Verfahren überhaupt zulässig ist, ist mittlerweile unbestritten.

schützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.“

Der Gesetzgeber hat somit ein dynamische System geschaffen, welches ein Gleichgewicht zwischen der Art verarbeiteten Daten, dem Umfang und dem Zweck der Verwendung einerseits und den technischen Möglichkeiten sowie der wirtschaftliche Vertretbarkeit andererseits schaffen soll. Rechtsanwälte verarbeiten teilweise sensible Daten im Sinne des § 4 Z 2 DSG 2000[15], darüber hinaus strafrechtlich relevante Daten[16]. Ferner wird aufgrund der besonderen, in § 9 Abs 2 RAO normierten Verschwiegenheitsverpflichtung der Rechtsanwälte auch hier ein besonders hohes Sicherheitsniveau angenommen.

In Abwägung der Sensibilität der Daten einerseits und der technischen Möglichkeiten andererseits, ist der Schluss zu ziehen, dass Übersendung von E-Mails an Mandanten gesichert erfolgen muss.

Dieser Schluss wird durch die aktuellen technischen Gegebenheiten gestützt. Die Kommunikation zwischen dem Mandanten und seinem Rechtsanwalt kann gesichert erfolgen, ohne, dass der Rechtsanwalt seine technischen Gegebenheiten anpassen muss – diese sind durch die Teilnahme am elektronischen Rechtsverkehr (ERV) gegeben. Einzige Voraussetzung ist die kostenlose Anmeldung des Mandanten am Trustnetz. Die genannten Punkte „technische Möglichkeiten“ und „wirtschaftliche Vertretbarkeit“ sind damit von vornherein gegeben.

Sollte der Mandant weder die technischen Voraussetzungen für eine verschlüsselte Übermittlung mitbringen, noch bei der E-Zustellung angemeldet sein oder auch gar keine gesicherte Kommunikation wünschen, kann dieser seinen Rechtsanwalt aktiv von der Verschwiegenheitspflicht entbinden. Welche rechtliche Qualität diese Entbindung im Zusammenhang mit E-Mail-Kommunikation hat, kann dahingestellt bleiben.[17]

Wesentlich ist jedoch, dass die Verletzung der Verschwiegenheitsverpflichtung im Sinne des § 9 Abs 2 RAO auch fahrlässig begangen werden kann[18]. Der Rechtsanwalt wird daher seinen Mandanten wohl jedenfalls auf die Gefahr einer unverschlüsselten Kommunikation hinweisen müssen.

Zuletzt ist die Frage, ob bei Endgeräten (insbesondere Smartphones) Sicherheitsmaßnahmen ergriffen werden müssen, leicht zu beantworten. § 14 DSG sieht vor, dass Datensicherheitsmaßen derart zu ergreifen sind, dass – unter anderem – „*die Daten Unbefugten nicht zugänglich sind.*“ Dies soll durch „*Zugriffsberechtigung auf Daten und*

---

[15] etwa bei Verkehrsunfällen: Gesundheitsdaten,

[16] Diese stellen zwar keine „sensiblen Daten“ im Sinne des § 4 Z 2 DSG 2000 dar, „*werden aber hinsichtlich ihrer Schutzwürdigkeit in die Näher dieser Daten gerückt.*“ (*Jahnel* in *Handbuch Datenschutzrecht* (2010) Rz 4/63.

[17] Siehe dazu schon *Mosig* aaO.

[18] OGH vom 02.09.2002 zu 4 Bkd 1/02.

Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte“[19] erfolgen. Schon aus diesen Gründen ist ein (mit Sicherheitsmaßnahme ausgestatteter) Sperrbildschirm für Computer und Smartphones obligatorisch. Wenn sich schon aus den „allgemeinen“ datenschutzrechtlichen Grundsätzen die Pflicht zur Ergreifung von Datensicherheitsmaßnahmen ergeben, müssen diese umso mehr für Rechtsanwälte gelten, um dem hohen Anspruch des § 9 Abs 2 RAO zu genügen.

Zusammenfassung und Ausblick

Die Änderung des Kommunikationsverhaltens macht auch von der Kommunikation zwischen dem Rechtsanwalt und seinem Mandanten nicht halt. Um die Interessen der Mandanten zu wahren und dem hohen Vertrauen gerecht zu werden, dass die Mandanten in die Rechtsanwälte haben, sind die Rechtsanwälte in der E-Mail-Kommunikation mit ihren Mandanten verpflichtet, gewisse Mindeststandards einzuhalten.

Für ein – standesrechtlich – korrektes Verhalten soll der jeweilige Rechtsanwalt seinen Mandanten zumindest das Trustnet anbieten, zumal jeder Rechtsanwalt in Österreich bereits an diesem teilnimmt. Sollte der Mandant dieses Angebot nicht annehmen (die Praxis hat gezeigt, dass mehr als 99% der Mandanten eine Verschlüsselung ablehnen[20]), sollte der Mandant über die Risiken der unverschlüsselten Versendung von E-Mail aufgeklärt werden. Dies ist durch einen entsprechenden Passus in der Mandatsvereinbarung leicht möglich.

Dennoch wäre es wünschenswert, dass die Nutzung des Trustnet – zumindest in naher Zukunft – zum Standard wird. Durch diese aktuelle Entwicklung wird erfreulicherweise auch technisch unversierten Nutzern eine sichere Kommunikation mit dem Rechtsanwalt ihres Vertrauens ermöglicht.

---

[19] § 14 Abs 1 Z 5 DSG 2000.

[20] In der Kanzlei des Autors dieses Beitrags gibt es lediglich **einen** Mandanten, der dieses Angebot wahrnimmt.