RA Prof. Niko Härting, 04.03.2020

Mails, Cloud, Messenger: Was ist eigentlich erlaubt?

- Tipps und Thesen -

I. E-Mails und Berufsrecht

1. Das Thema „E-Mails und Berufsrecht“ gibt es seit fast 25 Jahren.

Lapp, BRAK-Mitt. 1997, 108, 107:

> *„Als RA oder in ähnlicher Funktion kann allerdings ohne weiteres die eigene E-Mail-Anschrift bekanntgegeben werden. Der Mandant ist Herr seiner Daten und kann entscheiden, ob er sie dem Internet übergibt. Selbst darf der RA aber nur mit ausdrücklicher Zustimmung des Mandanten das Medium nutzen. Auch dann ist Vorsicht geboten, da nicht immer nur Daten des Mandanten übermittelt werden. Wer mit sensiblen Daten anderer leichtfertig umgeht, läuft Gefahr, sich strafbar zu machen. Nur anonymisierte oder geheimhaltungsfreie Daten sollten unverschlüsselt mit E-Mail versandt werden.“*

Härting, MDR 2001, 61, 61:

> *„Immer wieder wird behauptet, dass Rechtsanwälte, die mit Mandanten per unverschlüsselter E-Mail kommunizieren, ihrer Verschwiegenheitspflicht gem. § 43a Abs. 2 Satz 1 BRAO zuwiderhandeln. Gelegentlich heißt es sogar, die Übermittlung einer unverschlüsselten E-Mail an den Mandanten erfülle den Straftatbestand des § 203 Abs. 1 Nr. 3 StGB. Diese Behauptungen beinhalten einen gravierenden Vorwurf. Erstaunlich ist, dass die Annahme einer Berufswidrigkeit und Strafbarkeit unverschlüsselter E-Mails oft nur spärlich begründet wird. Eine nähere Betrachtung zeigt, dass der Vorwurf berufswidrigen oder gar strafbaren Handelns sogar unhaltbar ist.“*

2. Die Auffassung, dass die (unverschlüsselte) anwaltliche E-Mail-Kommunikation berufswidrig oder gar strafbar ist, hat sich nie durchsetzen können.

3. Ebenso wenig hat sich die Auffassung durchgesetzt, dass Mandanten vor den Risiken der (unverschlüsselten) anwaltliche E-Mail-Kommunikation stets gewarnt werden und einwilligen müssen.

4. Fälle, in denen Anwaltsmails aufgrund fehlender Verschlüsselung in falsche Hände geraten sind, sind in den letzten 25 Jahren weder aus Deutschland noch aus anderen Ländern bekannt geworden.

5. Das Telefax ist von berufs- und strafrechtlichen Diskussionen weitgehend verschont geblieben, obwohl die Kommunikation per Telefax über dieselben Kommunikationswege erfolgt wie die Kommunikation per E-Mail.

6. Technisch ist heutzutage die Transportverschlüsselung von E-Mails durchgängiger Standard. Wenn man Verschlüsselung diskutiert, geht es meist nur noch um Ende-zu-Ende-Verschlüsselung.

7. Ende-zu-Ende-Verschlüsselungsverfahren setzen sich seit 25 Jahren am Markt nicht durch, obwohl schon sehr frühzeitig – durch Signaturgesetze – regulatorische Anreize geschaffen, technische Standards gesetzt und vor den Gefahren der unverschlüsselten Kommunikation gewarnt wurde.

8. § 2 Abs. 2 Satz 5 und 6 BORA schafft seit Beginn dieses Jahres zusätzliche berufs- und strafrechtliche Sicherheit:

> *„Zwischen Rechtsanwalt und Mandant ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist,* ***jedenfalls*** *dann erlaubt, wenn der Mandant ihr zustimmt. Von einer Zustimmung ist auszugehen, wenn der Mandant diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat, fortsetzt."*

9. Zusammenfassend:

- Kein Verbot: Weder § 203 StGB noch § 43a Abs. 2 BRAO verbieten der Anwältin die Kommunikation per E-Mail. Dies gilt auch dann, wenn E-Mails nicht verschlüsselt sind oder (wie heute üblich) unter Einsatz einer bloßen Transportverschlüsselung versendet werden.
- Kein Einwilligungserfordernis: Weder § 203 StGB noch § 43a Abs. 2 BRAO verpflichten die Anwältin, den Mandanten um Einwilligung zu bitten, wenn per E-Mail kommuniziert werden soll (ob verschlüsselt oder nicht).
- Keine Aufklärungspflicht: Weder § 203 StGB noch § 43a Abs. 2 BRAO verpflichten die Anwältin, den Mandanten über Risiken des – verschlüsselten oder unverschlüsselten – E-Mail-Verkehrs aufzuklären.

II. E-Mails und Datenschutz

1. Aus Sicht mancher Datenschützer sind Anwälte eine Berufsgruppe, die sich hinter dem Anwaltsgeheimnis verschanzen, um sich der staatlichen Aufsicht zu entziehen.

Weichert, NJW 2009, 550, 551:

> *„Zu den Kontrollverweigerern gehörten zunächst die Geheimdienste, mit dem Hinweis der Schutzbedürftigkeit der dort erfassten Personen und der Geheimhaltungsbedürftigkeit ihrer Aktionen. Strafverfolgungsbehörden und Finanzbehörden wehrten sich unberechtigerweise gegen datenschutzrechtliche Pflichten bis in die jüngste Zeit hinein mit dem Argument, die Strafprozessordnung oder die Abgabenordnung wären abschließend und ließen keinen Platz mehr für die Anwendung des BDSG bzw. der jeweiligen Landesdatenschutzgesetze (LDSG). Auch Notare meinten, sich mit dem Hinweis auf ihre besonderen Verschwiegenheitspflichten der Datenschutzkontrolle entziehen zu können, obwohl sie als öffentliche Stellen besonders dem Grundrechtsschutz verpflichtet sind und daher einer unabhängigen Kontrolle unterliegen müssen. Bleiben die Rechtsanwälte, die meinen, sich dem BDSG nicht unterwerfen zu müssen."*

2. Bis zur Geltung der DSGVO (2018) war das Verhältnis zwischen dem Anwaltsgeheimnis und dem Datenschutzrecht streitig. Vieles sprach für eine Subsidiarität des Datenschutzrechts (vgl. Härting, NJW 2015, 1248, 1249 f.). Dies bedeutete für die E-Mail-Kommunikation, dass E-Mails, die nach § 43a Abs. 2 BRAO erlaubt waren, datenschutzrechtlich nicht verboten sein konnten. Das Berufsrecht gab für uns Anwälte den Ton an.

3. Seit der Geltung der DSGVO sind Ausnahmen von datenschutzrechtlichen Verpflichtungen der Anwälte (nur) in § 29 BDSG vorgesehen. Anwälte sind danach weder zur Information noch zur Auskunft über personenbezogene Daten verpflichtet. Die Datenschutzbehörden haben zudem kein Recht auf Zutritt zur Kanzlei und auf Zugang zu Daten, die in der Kanzlei verarbeitet werden.

4. Ohne Einschränkung (auch) auf die Anwaltsarbeit anwendbar ist Art. 32 Abs. 1 DSGVO, der Maßgaben für die „Sicherheit der Verarbeitung" regelt und in lit. a auch eine Regelung zur „Verschlüsselung" trifft:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:*
>
> *die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten…"*

5. Durch Art. 32 Abs. 1 DSGVO ist die Diskussion um eine Verschlüsselung von Anwaltsmails neu entfacht – nicht zuletzt auch aufgrund der PR-Arbeit einzelner Dienstleister, die (vermeintlich) „sichere" Verfahren und Lösungen für Anwaltskanzleien anbieten.

6. Schon dem Wortlaut nach verpflichtet Art. 32 Abs. 1 DSGVO nicht zur Verschlüsselung (ebenso wenig wie Art. 32 Abs. 1 DSGVO zu der im selben Atemzug genannten Pseudonymisierung verpflichtet). Behauptungen, aus Art. 32 Abs. 1 DSGVO lasse ich eine Verschlüsselungspflicht oder ein bestimmter Verschlüsselungsstandard ableiten, sind haltlos.

7. Allerdings verpflichtet Art. 32 Abs. 1 DSGVO jede Anwältin zu Maßnahmen der Datensicherheit. Zu den zu prüfenden Maßnahmen gehören auch Verschlüsselungsverfahren. Jede Anwaltskanzlei muss sich daher mit Verschlüsselungstechnik befassen und abwägen, ob Verschlüsselungsverfahren eingesetzt werden.

8. Ganz allgemein lässt sich aus Art. 32 Abs. 1 DSGVO die weitergehende Verpflichtung ableiten, die in der Kanzlei zum Schutz von Daten getroffenen Vorkehrungen regelmäßig zu prüfen und zu dokumentieren. Die vom DAV veröffentlichte Checkliste zu Art. 32 Abs. 1 DSGVO kann dabei die Arbeit erleichtern (https://anwaltverein.de/de/praxis/datenschutz?file=files/anwaltverein.de/downloads/praxis/datenschutz/technische-und-organisatorische-massnahmen-zur-datensicherung.pdf).

9. § 2 Abs. 2 Satz 1 bis 3 BORA knüpft an Art. 32 Abs. 1 DSGVO an und betont die Maßgaben der Risikoadäquanz und Zumutbarkeit, die sich in Art. 32 Abs. 1 DSGVO finden:

> *„Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit der Vorschriften zum Schutz personenbezogener Daten deren*

Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen."

10. Zusammenfassung:

- Keine generelle Pflicht zur Ende-zu-Ende-Verschlüsselung: Art. 32 Abs. 1 DSGVO lässt sich keine Verpflichtung der Anwältin entnehmen, per E-Mail nur unter Nutzung von Ende-zu-Ende-Verschlüsselung zu kommunizieren.
- Datensicherheit ist Chefsache: Art. 32 Abs. 1 DSGVO verpflichtet die Anwältin, sich mit Maßnahmen der Datensicherheit zu befassen und solche Maßnahmen unter Abwägung der Risiken und des Sicherheitsaufwands zu treffen.
- Transportverschlüsselung sollte gewährleistet sein: Aus Art. 32 Abs. 1 DSGVO lässt sich die Pflicht ableiten, dass ein E-Mail-Provider verwendet wird, der Transportverschlüsselung gewährleistet. Dies ist bei den größeren Providern heutzutage ohnehin Standard.
- Ende-zu-Ende-Verschlüsselung auf Anfrage: Die Anwältin sollte zur Ende-zu-Ende-Verschlüsselung imstande sein. Dies darf jeder Mandant erwarten. Eine entsprechende Verpflichtung lässt sich aus Art. 32 Abs. 1 DSGVO, jedenfalls aber aus dem Mandatsvertrag ableiten.
- Keine Absenkung des Sicherheitsniveaus per Einwilligung: Art. 32 Abs. 1 DSGVO steht nicht zur Disposition der Mandanten. Sicherheitsmängel lassen sich daher nicht damit rechtfertigen, dass die Anwältin pauschal von allen Mandanten das Einverständnis mit mangelhafter Datensicherheit einholt.
- Keine Aufklärungspflichten: Aufklärungspflichten der Anwältin über Sicherheitsmängel lassen sich aus Art. 32 Abs. 1 DSGVO nicht ableiten.

III. Cloud- und Messengerdienste

1. Vor den Neuregelungen zum „Non-Legal-Outsourcing" (2017) wiederholte sich bei den Clouddiensten die berufs- und strafrechtliche Diskussion, die es seit Ende der 90er-Jahre zur unverschlüsselten E-Mail-Kommunikation gegeben hatte: Ist die Speicherung von Daten bei einem Dienstleister ein „Offenbaren" im Sinne des § 203 StGB? Verletzt die Anwältin durch eine solche Speicherung bereits ihre berufsrechtliche Verschwiegenheitspflicht?

2. § 203 Abs. 3 StGB stellt seit 2017 klar, dass die Nutzung von Clouddiensten noch kein „Offenbaren" eines Geheimnisses darstellt. Mit dem Dienstleister muss allerdings ein Vertrag nach § 43e BRAO abgeschlossen werden. Unsicherheiten bleiben bei ausländischen Dienstleistern, da § 43e Abs. 4 BRAO für ausländische Dienstleister ein Schutzniveau vorschreibt, der „der Schutz im Inland vergleichbar ist".

3. Datenschutzrechtlich bedarf es in der Regel des Abschlusses eines Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO. Bei Dienstleistern aus einem Staat außerhalb der EU können sich zudem aus den Art. 44 ff. DSGVO Besonderheiten ergeben.

4. WhatsApp setzt Ende-zu-Ende-Verschlüsselung ein, sodass sich die bei E-Mails diskutierten Fragen nicht stellen. Das Anwaltsgeheimnis wird zudem nicht dadurch verletzt, dass – wie bei WhatsApp üblich – Adressdaten von Kontakten auf WhatsApp-Server geladen werden. Mit der Übermittlung von Kontaktdaten ist keine Aussage darüber verbunden, ob eine bestimmte Person Mandantin ist.

5. Datenschutzrechtlich gibt es gegen den Einsatz von WhatsApp im Hinblick auf das Hochladen von Kontaktdaten Bedenken, denen sich allerdings durch „Containerlösungen“ und andere Schutzmaßnahmen begegnen lässt (vgl. Schirmbacher, Suchradar 79/ August2019, https://www.suchradar.de/magazin/79/messenger-dienste-unternehmenskommunikation-ist-nutzung-von-whatsapp-co-im-unternehmen).

IV. Drei Beobachtungen zum Schluss

1. Datensicherheit ist Chefsache: Unabhängig von allen rechtlichen Vorgaben erwarten Mandanten von uns, dass Informationen vor unbefugtem Zugriff geschützt sind. Wer schludert, setzt das Vertrauen der Mandanten leichtfertig aufs Spiel. Dis schadet uns allen.

2. Datensicherheit ist mehr als Verschlüsselung: Datensicherheit ist kein bloßes „IT-Thema“. Es beginnt bei der gesicherten Eingangstür und dem gesicherten Hausbriefkasten und hört bei verschließbaren Schränken und dem Sichtschutz auf dem eigenen Laptop nicht auf. Mitarbeiter brauchen klare Regeln im Umgang mit Akten – ob auf Papier oder digital. Mandantennamen eignen sich nicht zur Prahlerei. Für Mandantentelefonate sind öffentliche Verkehrsmittel der falsche Ort.

3. Die größte Sicherheitsgefahr sitzt vor dem Endgerät: Wem von uns ist es noch nicht passiert, dass eine E-Mail oder ein Fax den falschen Empfänger erreichte? Tipps und Tricks zur Vermeidung von Eingabefehlern sind ein wichtiges Thema für die Schulung von Kollegen und Mitarbeitern.

4. Der Mandant ist König: Wenn Mandanten Ende-zu-Ende-Verschlüsselung wünschen oder ganz auf E-Mails verzichten wollen, müssen wir diesen Wünschen nachkommen. Wenn sie andererseits mit uns per WhatsApp oder SnapChat kommunizieren möchten, dürfen sie von uns gleichfalls erwarten, dass wir uns auf diesen Wunsch einlassen. Es mag sinnvoll und auch angezeigt sein, auf Risiken hinzuweisen. Verweigern sollten wir uns im Zweifel nicht.