LICHT IM DATENSCHUTZRECHTLICHEN DUNKEL?

EIN ERSTER SCHRITT ZUR KLÄRUNG BEI ANWALTLICHER E-MAIL-KOMMUNIKATION

RECHTSANWALT DR. HENDRIK SCHÖTTLE*

Ob Rechtsanwältinnen und Rechtsanwälte generell nur per Ende-zu-Ende-verschlüsselter E-Mail mandatsbezogen kommunizieren dürfen oder ob eine Transportverschlüsselung ausreicht, wird seit Längerem unter datenschutz- und berufsrechtlichen Gesichtspunkten kontrovers diskutiert. Die Landesdatenschutzbeauftragten vertreten hierzu teils konträre Auffassungen, was für

* Der Autor ist Rechtsanwalt und Fachanwalt für IT-Recht in München und Mitglied des Ausschusses Datenschutzrecht der BRAK.

die anwaltliche Praxis zu Unsicherheiten führt. Das VG Mainz[1] hatte sich als erstes deutsches Gericht mit der Frage zu befassen und hält grundsätzlich eine Transportverschlüsselung für ausreichend. Der Autor erläutert die Hintergründe der Entscheidung und zeigt auf, inwieweit diese Licht ins Dunkel zu bringen vermag.

I. DER AUSGANGSFALL

Das VG Mainz beschäftigt sich als erstes deutsches Gericht mit der Frage, ob Rechtsanwälte beim Einsatz von E-Mail-Kommunikation mit ihren Mandanten grundsätzlich Ende-zu-Ende-verschlüsselt kommunizieren müssen oder ob eine Transportverschlüsselung ausreicht.

Anlass zu der Entscheidung war etwas, das für viele Rechtsanwälte vermutlich alltägliche ist: Der Kläger war als Rechtsanwalt in einer Erbschaftsangelegenheit mandatiert. Nachdem der Bruder des Mandanten auf ein postalisch übersandtes Schreiben nicht reagiert hatte, wurde er von der Kanzlei des Klägers per E-Mail kontaktiert. Daraufhin zeigte dieser beim zuständigen Landesbeauftragten für Datenschutz und Informationsfreiheit eine Datenschutzverletzung durch den Rechtsanwalt an, die er in der unverschlüsselten Übersendung eines Schreibens per E-Mail sah.

Der Landesbeauftragte erließ gegen den Rechtsanwalt eine Verwarnung wegen Verstoßes gegen Art. 5 I lit. f, II DSGVO, weil nach seiner Auffassung lediglich eine Ende-zu-Ende-verschlüsselte Kommunikation eine ausreichende Sicherheit bietet. Auf die hiergegen erhobene Anfechtungsklage hob das VG Mainz die Verwarnung auf.

II. DIE HINTERGRÜNDE DER ENTSCHEIDUNG

Bis zur Entscheidung des VG Mainz war die derzeitige Rechtslage alles andere als klar. Neben Meinungen in der Literatur, die eine Transportverschlüsselung für ausreichend erachteten und allenfalls in besonderen Fällen eine Pflicht zur Ende-zu-Ende-Verschlüsselung annahmen, sprachen sich insbesondere der sächsische Datenschutzbeauftragte im Jahr 2017 generell für eine verschlüsselte Kommunikation von Rechtsanwälten per E-Mail aus, ohne allerdings zu spezifizieren, ob eine Transportverschlüsselung oder eine Ende-zu-Ende-Verschlüsselung gemeint ist.[2] Der Hamburgische Datenschutzbeauftragte hielt in einer Stellungnahme aus dem Jahr 2018 zumindest eine Transportverschlüsselung für erforderlich, eine Ende-zu-Ende-Verschlüsselung für vorzugswürdig.[3]

Noch weiter ging die Datenschutzkonferenz in ihrer Orientierungshilfe vom März 2020,[4] welche als eine generelle Forderung nach einer Ende-zu-Ende-Verschlüsselung anwaltlicher E-Mail-Kommunikation verstanden werden kann. In die entgegengesetzte Richtung gingen schließlich Meldungen, wonach in Kreisen des EU-Ministerrats Ende 2020 ein Verbot von Ende-zu-Ende-Verschlüsselung erwogen wurde, welches die Arbeit insbesondere von Ermittlungsbehörden erleichtern sollte.

Damit lag bis zur Entscheidung des VG Mainz von einer Empfehlung zur Verwendung von Ende-zu-Ende-Verschlüsselung über die Pflicht zu ihrer Verwendung bis hin zu einem beabsichtigten Verbot derselben die gesamte Bandbreite der denkbaren Optionen auf dem Tisch.

III. DIE ENTSCHEIDUNG DES VG

Es ist erfreulich, dass das VG Mainz mit der vorliegenden Entscheidung nun ein Stück weit Licht ins Dunkel bringt. Zwar hält die Kammer eine Transportverschlüsselung für obligatorisch (Rn. 29), allerdings ist dies inzwischen heutzutage ohnehin Standard und ohne größere technische und organisatorische Implikationen umzusetzen. Anders als wohl die Datenschutzkonferenz geht das Gericht jedoch nicht pauschal von einer besonderen Schutzbedürftigkeit anwaltlicher, mandatsbezogener Kommunikation aus; vielmehr sei die Schutzbedürftigkeit im Einzelfall zu ermitteln (Rn. 34). Eine bloß schematische Betrachtungsweise verbiete sich (Rn. 35).

Bemerkenswert ist auch, dass das Gericht nicht allein die Schutzwürdigkeit der Mandatsinformationen betrachtet, sondern diese auch ins Verhältnis zum mit der Ende-zu-Ende-Verschlüsselung einhergehenden Aufwand setzt. So werden unter anderem auch Zugangsprobleme sowie Beschränkungen bei der Weiterleitung der Informationen gesehen (Rn. 36). Auch wenn das Gericht die Möglichkeit einer „kostenschonenden Implementierung" sieht, wenn etwa eine Containerverschlüsselung als Lösung gewählt wird, führe dies nicht zwingend zu einer entsprechenden Verpflichtung des Verantwortlichen (Rn. 36).

Das Gericht hält grundsätzlich die Verwendung einer Transportverschlüsselung datenschutzrechtlich auch bei Berufsgeheimnisträgern für ausreichend (Rn. 38), soweit keine Anhaltspunkte für besonders sensible Daten oder sonstige Umstände hinzutreten. Die Betonung, dass transportverschlüsselte E-Mails „wohl derzeit *noch* als (Mindest-)Stand der Technik einzustufen" sind, zeigt allerdings das Bewusstsein der entscheidenden Kammer über einen möglichen Wandel im Laufe der Zeit. Es dürfte in der Tat nicht auszuschließen sein, dass bei

[1] VG Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ, BRAK-Mitt. 2021, 104 (in diesem Heft).

[2] Sächsischer Datenschutzbeauftragter, 8. Tätigkeitsbericht v. 31.3.2017, LT-Drs. 6/10550, 138, https://www.saechsdsb.de/images/stories/sdb_inhalt/noeb/taetigkeitsberichte/8-TB-Endfassung-Version-5.pdf.

[3] Stn. des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit v. 8.10.2018, 2, https://www.datenschutzbeauftragter-info.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf.

[4] Orientierungshilfe des Arbeitskreises technische und organisatorische Datenschutzfragen mit dem Titel „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" v. 13.3.2020, https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf; s. dazu auch *Schöttle/Ludwig*, BRAK-Mitt. 2020, 308.

einer zukünftigen Verbreitung weiterer Verschlüsselungstechniken ein Gericht dann anders entscheiden würde.

Was den Umgang mit Daten angeht, die unter Art. 9 oder 10 DSGVO fallen, so scheint sich das Gericht eine Hintertür offen gehalten zu haben. Zwar heißt es, dass bei solchen Daten in jedem Fall besondere Schutzmaßnahmen zu ergreifen sind. Das gelte auch für Fälle, wenn „ein Interesse krimineller und ressourcenreicher Dritter absehbar ist" (Rn. 37). Allerdings spricht das Gericht hier lediglich von besonderen Schutzmaßnahmen bzw. einem hohen Risiko (Rn. 37), ohne explizit eine Ende-zu-Ende-Verschlüsselung zu fordern. Lägen keine Fälle von Art. 9 oder 10 DSGVO vor, sei es allenfalls sachgerecht, in Zweifelsfällen eine widerlegliche Vermutung für einen besonderen Schutzbedarf anzunehmen. Ein solcher Zweifelsfall liegt nach Auffassung der Kammer allerdings nicht vor (Rn. 37).

IV. FOLGEWIRKUNGEN UND OFFENE FRAGEN

Entspannt sich mit der Entscheidung nun die Situation für den Rechtsanwalt, der per E-Mail kommuniziert und damit ein inzwischen immerhin fünfzig Jahre altes, in allen Lebensbereichen den postalischen Brief weitestgehend verdrängt habendes Kommunikationsmittel verwendet? Leider nicht. Das Gericht entschied in dem vorliegenden Fall, dass die vom klagenden Rechtsanwalt versandten Informationen den in Art. 9 und 10 DSGVO genannten Datenkategorien nicht unterliegen und diesen auch nicht einmal nahe kamen. Allein aus diesem Grund lehnte es eine Verpflichtung einer Ende-zu-Ende-Verschlüsselung ab (Rn. 38).

Offen bleibt, wie nach Auffassung der Kammer zu entscheiden gewesen wäre, wenn es sich um sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten gehandelt hätte. Wäre in diesem Fall zwingend eine Ende-zu-Ende-Verschlüsselung erforderlich gewesen? Auch ließen die Richter ausdrücklich offen, ob die Pflichten nach Art. 32 DSGVO überhaupt disponibel sind, ob also auf einer aus datenschutzrechtlicher Sicht erforderliche Ende-zu-Ende-Verschlüsselung aufgrund einer Einwilligung der an der Kommunikation Beteiligten hätte verzichtet werden können (Rn. 42).

Sollte tatsächlich in den Fällen von Art. 9 und 10 DSGVO zwingend eine Pflicht zur Ende-zu-Ende-Verschlüsselung erforderlich und auch nicht durch Einwilligung verzichtbar sein, wären die daraus resultierenden Folgen gravierend und weder den Rechtsanwälten noch den Rechtsuchenden zu vermitteln:

Ein praktikabler Austausch von Informationen per E-Mail wäre schlichtweg nicht mehr möglich. Die technischen Voraussetzungen für eine Ende-zu-Ende-Verschlüsselung existieren bei den wenigsten E-Mail-Nutzern. Praktisch wäre also der Einsatz von Containerverschlüsselung oder eines Webportals notwendig. Jeder, der einmal ein Anliegen über ein webbasiertes Kontaktformular geschildert oder eine längere Konversation über ein solches Portal geführt hat, weiß, dass dies nicht praktikabel ist. Vollends offen bleibt, wie auf diesem Wege eine Kommunikation mit mehreren Verfahrensbeteiligten umgesetzt werden soll. Statt auf eingespielte Wege und standardisierte E-Mail-Kommunikation zu setzen, müssten sich die alle Beteiligte wahlweise entweder mit Passwort- und Schlüsselmanagement oder der Einarbeitung in jeweils von Anwalt zu Anwalt unterschiedliche Portallösungen herumschlagen. Insbesondere bei dem hohen Zeitdruck, unter dem die Beteiligten oft stehen, ist das nicht zu schaffen.

Und damit schließt sich auch der Kreis: Hoher Zeitdruck war die Begründung, mit welcher der klagende Rechtsanwalt den Versand von Informationen per E-Mail anstelle des postalischen Versands begründete. Sollte die Entscheidung des VG Mainz dazu führen, dass Rechtsanwälte im Zweifel auf E-Mail-Kommunikation verzichten müssen, dürfte darunter auch die Qualität der Rechtsberatung insbesondere bei eilbedürftigen Sachen leiden.

V. BERÜCKSICHTIGUNG DES TECHNISCH UND ORGANISATORISCH MACHBAREN

Leider wird die Diskussion um das Thema häufig ohne vertiefte Auseinandersetzung mit der verwendeten Technik geführt, vor allem ohne Berücksichtigung der Auswirkung von Forderungen eines technisch machbaren maximalen Schutzes auf die Arbeitsabläufe und organisatorischen Anforderungen der Beteiligten. Auch wenn im konkreten Fall die Pflicht einer Ende-zu-Ende-Verschlüsselung abgelehnt wurde, wäre in der Entscheidungsbegründung vertiefte Betrachtung der Risiken und Angriffsszenarien wünschenswert gewesen, denen durch eine solche Verschlüsselungstechnik tatsächlich begegnet würde. Erfreulicherweise wurden im vorliegenden Fall zumindest die technischen und organisatorischen Nachteile, die solche Maximallösungen mit sich bringen, zumindest angedeutet und die Kritik aus der Literatur daran wurde aufgegriffen.[5]

Es ist jedenfalls dem technisch versierten Beteiligten nicht vermittelbar, warum bei Verschlüsselung des gesamten Transportweges einer E-Mail allein den E-Mail-Providern, die dem strafbewehrten Telekommunikationsgeheimnis unterliegen, nicht getraut werden können soll, wenn gleichzeitig der postalische Versand von ohne weitere technische Hilfsmittel lesbaren Briefen sicher genug sein soll, welche lediglich durch einen papiernen Umschlag vor Transportbeschädigungen geschützt sind und mit dem bloßen Finger aufgerissen werden können. Allein das Paradigma „Brief war eben schon vorher da" dürfte nach gut fünfzig Jahren E-Mail bzw. mindestens zwanzig Jahren E-Mail-Nutzung in der Breite nicht mehr gelten.

[5] S. zu technisch-organisatorischen Implikationen auch *Schöttle/Ludwig*, BRAK-Mitt. 2020, 308 ff.

Überzeugend wäre es jedenfalls, allein bei einem im Einzelfall anzunehmenden, hinreichend konkreten „Interesse krimineller und ressourcenreicher Dritter“ eine Pflicht zum Einsatz von Ende-zu-Ende-Verschlüsselung oder vergleichbaren Maßnahmen anzunehmen und im Übrigen die Transportverschlüsselung genügen zu lassen.

Letztlich steht zu befürchten, dass weder der Landesdatenschutzbeauftragte noch die Richter der Kammer des VG Mainz die drastischen Auswirkungen einer Forderung nach einer Ende-zu-Ende-Verschlüsselung in ganz praktischer Hinsicht im Blick hatten. Die E-Mail ist nach vielen Studien schon seit Jahren das Kommunikationsmittel Nummer eins – es faktisch durch Forderung nach dem obligatorischen Einsatz von Verschlüsselungstechniken mit so hohen Sicherheitsstandards flankieren zu wollen, dass die Mehrheit der Rechtssuchenden daran scheitern dürfte,[6] stellt auch das in § 3 Abs. 3 BRAO statuierte Beratungs- und Vertretungsrechts des Bürgers in Frage.[7]

VI. FAZIT

Positiv ist, dass nach Auffassung des VG Mainz der Rechtsanwalt, der keine sensiblen Daten i.S.d. Art. 9 DSGVO und auch keine Daten über strafrechtliche Verurteilungen gem. Art. 10 DSGVO verarbeitet, im Regelfall davon ausgehen kann, dass der Einsatz von Transportverschlüsselung ausreicht und dass eine Ende-zu-Ende-Verschlüsselung nicht erforderlich ist.

Mit der Entscheidung ist allerdings nicht den Strafrechtlern geholfen und auch nicht den Kollegen, die sensible Daten verarbeiten. Auch wenn die Entscheidung nicht ausdrücklich in diesen Fällen eine Ende-zu-Ende-Verschlüsselung fordert, steht doch zu befürchten, dass sie am Ende so verstanden werden kann. Dies schürt Bedenken beim Einsatz von seit Jahrzehnten etablierter Kommunikationstechniken und zieht – sollte Ende-zu-Ende-Verschlüsselung tatsächlich obligatorisch sein – organisatorische Konsequenzen nach sich, welche die entscheidende Kammer vermutlich gar nicht im Blick hatte.

Das derzeitige Fehlen brauchbarer technischer Lösungen für eine Ende-zu-Ende-Verschlüsselung dürfte dazu führen, dass der Mandant im Einzelfall von einer Inanspruchnahme anwaltlicher Beratung Abstand nimmt, wenn er die technischen Anforderungen schlichtweg nicht erfüllen kann.[8] Und das kann kaum gewollt sein, ja ein solches Ergebnis mag sogar im Konflikt mit dem Beratungs- und Vertretungsrecht des Bürgers nach § 3 Abs. 3 BRAO stehen.

[6] S. zu praktischen Fragen des Einsatzes von Ende-zu-Ende-Verschlüsselung Schöttle/Ludwig, BRAK-Mitt. 2020, 308 ff (311).

[7] Welches letztlich aus Art. 2 Abs. 1 GG in Verbindung mit dem Rechtsstaatsprinzip hergeleitet wird, vgl. Brüggemann in: Weyland, BRAO, 10. Aufl. 2020, § 3 BRAO, Rn. 26.

[8] *Schöttle/Ludwig*, BRAK-Mitt. 2020, 308 ff. (314).