E-Mail Verkehr mit Mandanten kann bei deren Einwilligung auch unverschlüsselt zulässig sein

Eine Entgegnung auf die Stellungnahme des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Prof. Dr. Caspar

Der Hanseatischen Rechtsanwaltskammer liegt ein Schreiben des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 08.01.2018 vor, welches sich mit der Frage der Verpflichtung von Rechtsanwälten zur Verschlüsselung von E-Mails befasst. Darin wird die Auffassung vertreten, die elektronische Übertragung sensibler personenbezogener Daten ohne Verschlüsselung per E-Mail scheide selbst dann aus, wenn der Betroffene explizit um die Übersendung per E-Mail bitte. Der HmbBfDI weist in diesem Zusammenhang ferner darauf hin, dass der in der unverschlüsselten E-Mail-Kommunikation liegende Verstoß gegen § 9 BDSG keine Ordnungswidrigkeit im Sinne des § 43 BDSG darstelle. Anders sehe dies allerdings nach der ab dem 25.05.2018 unmittelbar geltenden Datenschutzgrundverordnung (Verordnung (EU) 2016/679 – „DSGVO“) aus. Die Gewährleistung von Datenschutz sei dann nicht nur gesetzlich verankert, sie stelle zudem die Bedeutung des technischen und organisatorischen Datenschutzes heraus. Dies werde insbesondere dadurch deutlich, dass zukünftig ein Verstoß gegen technisch-organisatorische Maßnahmen mit Geldbußen geahndet werden könne (Artikel 5 Abs. 1 f), 32, 83 DSGVO. Anmerkung: Nach Art. 84 Abs. 4 lit. a) DSGVO beträgt der Bußgeldrahmen bei Verstößen gegen Art. 32 DSGVO bis zu 10 Mio. Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist).

Der HmbBfDI kommt insoweit zu dem Ergebnis, die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthielten, sei insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterlägen, nicht nur „bedenklich“, sondern stelle auch ein „ungeeignetes Kommunikationsmittel“ dar.

Auf die Ausführungen des HmbBfDI ist Folgendes anzumerken:

1. Berufsrecht

Der Rechtsanwalt ist zur strikten Verschwiegenheit verpflichtet (§§ 203 StGB, § 43 a Abs. 2 BRAO, § 2 BORA) und zugleich berechtigt (s. insbes. § 53 Abs. 1 Nrn. 2 u. 3 StPO, § 2 BORA). Die Verschwiegenheit ist, ebenso wie die berufliche Unabhängigkeit und das Verbot der Vertretung widerstreitender Interessen, Grundpflicht und zugleich „Core Value“ des Anwalts.

Schon berufsrechtlich gebietet es die Verschwiegenheitspflicht dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, jedoch soweit sie risikoadäquat und für den Anwaltsberuf zumutbar sind (§ 2 Abs. 7 Satz 1 BORA). Technische Maßnahmen sind hierzu ausreichend, soweit sie im Fall der Anwendbarkeit des Datenschutzrechts dessen Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen, § 2 Abs. 7 Satz 2 und 3 BORA. Nach § 2 Abs. 3 lit. c) BORA ist ein Verstoß gegen die Verschwiegenheitspflicht des Anwalts nicht gegeben, soweit das Verhalten des Rechtsanwalts im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz).

Die - auch unverschlüsselte - elektronische Kommunikation per E-Mail zwischen Anwalt und Mandant ist seit langem üblich und hat die traditionelle Kommunikation per Brief weitestgehend ersetzt. Den meisten Mandanten dürfte auch bewusst sein, dass diese Kommunikation über weltweit verteilte Server stets die Gefahr birgt, dass andere Personen darauf zugreifen können. In weiten Bereichen dürfte daher die unverschlüsselte elektronische Kommunikation noch als „sozialadäquat“ zu beurteilen sein. Berufsrechtlich schließt die Einwilligung des Mandanten in die unverschlüsselte Kommunikation und den Austausch seiner personenbezogenen Daten einen Verstoß gegen die Verschwiegenheitsverpflichtung ohnehin aus (§ 2 Abs. 3 lit. a) BORA).

2. Datenschutzrecht

Nichts anderes dürfte auch nach datenschutzrechtlichen Bestimmungen gelten (die auch berufsrechtlich unberührt bleiben, § 2 Abs. 8 BORA):

a) Nach gegenwärtiger Rechtslage sind bei automatisierter Verarbeitung oder Nutzung personenbezogener Daten Maßnahmen zu treffen,

> „die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
> …..
> zu gewährleisten, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten

durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle), …“

Eine danach zu treffende Maßnahme ist „insbesondere“ die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (vgl. Anlage zu § 9 Satz 1 BDSG, dort Satz 2 Nr. 4 und Satz 2).

Der HmbBfDI weist in seinem Schreiben vom 08.01.2018 selbst darauf hin, dass die Auswahl der zu treffenden Maßnahmen durch eine Abwägung zwischen Schutzbedarf auf der einen und Aufwand auf der anderen Seite zu treffen sei. Kurz gesagt bedeute dies, so führt er aus, je höher der Schutzbedarf der Daten sei, desto höher müsse auch der Aufwand sein, um die Daten entsprechend vor Zugriffen Dritter zu schützen. Dabei sei der Stand der Technik ebenso zu berücksichtigen wie der Aufwand für die datenverarbeitende Stelle. Bereits hieraus wird deutlich, dass durchaus danach zu differenzieren ist, welchen Inhalt die per E-Mail ausgetauschte Kommunikation hat und wie hoch der Schutzbedarf auch durch den Mandanten selbst eingeschätzt wird.

b) Nichts anderes gilt im Anwendungsbereich des vom HmbBfDI angeführten Artikel 32 DSGVO. Die Verschlüsselung ist nach Artikel 32 Abs. 1 lit. a) DSGVO eine Maßnahme, die der Verantwortliche und der Auftrags(daten)verarbeiter zu nutzen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, jedoch „unter Berücksichtigung der 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“. Artikel 32 DSGVO erfordert folglich eine Verhältnismäßigkeitsprüfung. Nicht jede E-Mail wird daher verschlüsselt übermittelt werden müssen.

c) Nicht einheitlich zu beantworten ist im Übrigen die Frage, welche Art der Verschlüsselung gewählt werden muss, wenn eine solche erforderlich ist. Der HmbBfDI selbst führt insoweit aus, zu unterscheiden sei zwischen der Transportverschlüsselung, (z.B. TLS) sowie der Ende-zu-Ende Verschlüsselung, (z.B. S/MIME oder PGP). Aus datenschutzrechtlicher Sicht sei eine Ende-zu-Ende Verschlüsselung „zu bevorzugen“. Nach Maßgabe der Abwägung könne etwa auf die Nutzung von DE-Mail zurückgegriffen werden, die DE-Mail garantiere den Einsatz von Transportverschlüsselung und sei ein vom BSI zertifiziertes Verfahren, welches sich zudem durch eine Ende-zu-Ende-Verschlüsslung erweitern ließe.

In der Praxis dürfte ein Versand jeglicher Kommunikation per DE-Mail schon aus Kostengründen kaum in Betracht kommen. Eine Ende-zu-Ende Verschlüsselung soll indes das

besondere elektronische Anwaltspostfach ermöglichen, sobald dessen Einsatzfähigkeit wiederhergestellt ist. Hierüber wird nicht nur wieder mit Gerichten und anderen Kammermitgliedern kommuniziert werden können. Vielmehr wird auch eine Kommunikation mit Inhabern von EGVP-Bürgerpostfächern ermöglicht (s. bereits beA-Newsletter 26/2017 v. 29.06.2017). Bis dahin - oder soweit der Mandant über kein EGVP-Bürgerpostfach verfügt - wird es in Anbetracht der gebotenen Verhältnismäßigkeitsprüfung in vielen Fällen ausreichend sein, passwortgeschützte Korrespondenz als E-Mail-Anhang zu versenden, insbesondere wenn die Korrespondenz in ein passwortgeschütztes „Zip"-Archiv verpackt wird.

d) Entgegenzutreten ist im Übrigen nicht nur berufsrechtlich der Auffassung des HmbBfDI, auf eine Verschlüsselung könne selbst dann nicht verzichtet werden, wenn der Mandant einwillige. Jedenfalls soweit allein personenbezogene Daten des Mandanten übermittelt werden, wird eine den Anforderungen des Art. 7 DSGVO gerecht werdende Einwilligung auch die unverschlüsselte Kommunikation ermöglichen. Eine solche Einwilligung ist jederzeit widerruflich; auf das Widerrufsrecht ist hinzuweisen.

3. Konsequenzen und Grundsätzliches zum Datenschutz

a) Nach Auffassung der Hanseatischen Rechtsanwaltskammer wird nicht jede unverschlüsselte E-Mail eines Anwalts den Vorwurf einer Verletzung gegen die ab dem 25.05.2018 geltende Bestimmung des Artikels 32 DSGVO begründen können. Gleichwohl darf kein Missverständnis aufkommen: Schon aus der anwaltlichen Verschwiegenheitsverpflichtung resultiert die Verpflichtung, sich mit den Möglichkeiten der Verschlüsselung elektronischer Korrespondenz vertraut zu machen, technischen Sachverstand hinzuzuziehen und hinreichende Maßnahmen zum Schutze der personenbezogenen Daten der Mandanten und etwaiger Dritter zu treffen. Dem Wunsch des Mandanten, elektronisch Korrespondenz ausschließlich verschlüsselt zu führen, ist selbstverständlich zu entsprechen. In jedem Fall sind sichere alternative Kommunikationswege anzubieten.

b) Erinnert sei daran, dass die Hanseatische Rechtsanwaltskammer seit jeher gegenüber dem HmbBDfI die Auffassung vertreten hat, dass

- die Aufsicht über den Datenschutz bei Rechtsanwälten nicht in den Händen der Landesdatenschutzbeauftragten liegt, weil dies einen mit dem Gesetz nicht zu vereinbarenden, besonders schwerwiegenden Eingriff in die anwaltliche Selbstverwaltung gleichkommt,

- Rechtsanwälte bei der Erfüllung ihrer Aufträge und Mandate nicht nur durch das Gesetz in § 203, sondern auch durch die Berufsordnung auf die strikte und kompromisslose Beachtung der ihnen anvertrauten Geheimnisse verpflichtet sind, was gänzlich ausschließt, dass derjenige, der einen freien Beruf als Rechtsanwalt ausübt, der staatlichen Kontrolle oder der Bevormundung in diesem Bereich ausgesetzt wäre,

- das Bundesverfassungsgericht nichts anderes festgestellt hat, wenn es ausgeführte, dass der Schutz der anwaltlichen Berufsausübung von staatlicher Kontrolle und Bevormundung nicht nur den individuellen Belangen des Rechtsanwalts und seines Mandanten diene, sondern vor allem auch dem öffentlichen Interesse an einer wirksamen und geordneten Rechtspflege Rechnung trage (vgl. 1. Senat vom 15.03.2007, BvR 1887/06 und 2. Senat vom 30.04.2007, 2 BvR 2151/06),

und schließlich

- entscheidend ist, dass für die Berufsaufsicht, welche den gesamten Pflichtenkreis des Rechtsanwalts umfasst, ausschließlich die zuständige Rechtsanwaltskammer zuständig ist, und zwar für alle diese Mitglieder, die in ihrem Bezirk der Verkammerung unterworfen sind.

Die Hanseatische Rechtsanwaltskammer schließt sich daher auch nachdrücklich der Forderung der Bundesrechtsanwaltskammer nach Einführung eines Datenschutzbeauftragten für die Rechtsanwaltschaft an, der für alle Mitglieder der Rechtsanwaltskammern die datenschutzrechtliche Kontrollstelle entsprechend den europarechtlichen Vorgaben ist (BRAK-Stellungnahme Nr. 41/2016). Nur dies wäre ein akzeptabler Weg, den seit langem zwischen Datenschutzbehörden und Rechtsanwaltskammern bestehenden Zuständigkeitsstreit über die Datenschutzaufsicht zu beenden.

c) Erinnert sei weiter daran, dass sich aus den datenschutzrechtlichen Kontrollbefugnissen der Landesdatenschutzbeauftragten in keinem Fall eine gesetzliche Befugnis oder gar Verpflichtung des Rechtsanwaltes zur Weitergabe mandatsbezogener Informationen an die Datenschutzbehörde ergibt. Gibt der Rechtsanwalt gleichwohl mandatsbezogene Informationen preis, so handelt er bei der Weitergabe von derartigen Informationen „unbefugt“ im

Sinne des § 203 StGB, also rechtswidrig (vgl. Kammergericht, Beschluss vom 20.08.2010, 1 Ws (B) 51/07 – 2 Ss 23/07).

Nach Auffassung der Hanseatischen Rechtsanwaltskammer ändert die DSGVO hieran nichts. Im Gegenteil: Der deutsche Gesetzgeber hat von der Möglichkeit des Art. 90 DSGVO Gebrauch gemacht, in der Neufassung des Bundesdatenschutzgesetzes (Art. 1 des „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)“ besondere Regelungen zum Schutze von Berufsgeheimnisträgern zu treffen, die zum 25.05.2018 und damit zeitgleich mit der Geltung der DSGVO in Kraft treten. So ist in § 29 Abs. 3 BDSG n.F. bestimmt, dass die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Abs. 1 lit. e) und f) der DSGVO gegenüber den in § 203 Absatz 1, 2a und 3 StGB genannten Personen oder deren Auftragsverarbeitern nicht bestehen, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde. Ferner sind Rechtsanwälte in weitem Umfang von Informationspflichten nach den Art. 13 und 14 DSGVO befreit (§ 29 Abs. 2 BDSG n.F; Art. 14 Abs. 5 lit. 5 DSGVO). Für entsprechende Ausnahmen hat sich die BRAK im Gesetzgebungsverfahren erfolgreich eingesetzt.

Rechtsanwalt Dr. Christian Lemke,
Präsident der Hanseatischen Rechtsanwaltskammer