BUNDESRECHTSANWALTSKAMMER

# Stellungnahme Nr. 47/2020
# September 2020

## zur Orientierungshilfe der Datenschutzkonferenz (Arbeitskreis „Technische und organisatorische Datenschutzfragen“) „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ vom 13.03.2020


**Mitglieder des Ausschusses Datenschutzrecht**

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RA Dr. Wulf Kamlah
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.

RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK Berlin

**Verteiler:** Bundesministerium für Justiz und Verbraucherschutz
Bundesministerium des Innern
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat im März 2020 eine Orientierungshilfe zu „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (gegen die Stimme des Freistaates Bayern) beschlossen. Verfügbar ist der Text der Orientierungshilfe u. a. unter datenschutzkonferenz-online.de.

Der Text berührt auch die Verarbeitung personenbezogener Daten durch Rechtsanwältinnen und Rechtsanwälte. Allein dieser Aspekt ist Gegenstand der vorliegenden Stellungnahme.

1. Zu begrüßen ist das Grundanliegen der Orientierungshilfe: In einem lange umstrittenen Bereich soll die Auffassung der Datenschutz-Aufsichtsbehörden klar kommuniziert werden.

   Für „typische Verarbeitungssituationen“ wird „ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail“ betrachtet, welche Maßnahmen zur Risikominderung erforderlich sind (Orientierungshilfe, Ziffer 1).

2. Richtig und für die Praxis äußerst wichtig ist die Aussage zum „Normalfall“:

   „In Verarbeitungssituationen mit normalen Risiken wird … bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht.“ (Orientierungshilfe, Ziffer 2). Damit ist ein jahrelanger Meinungsstreit beendet, in dessen Verlauf immer wieder auch die falsche, nicht praxistaugliche Meinung vertreten wurde, jegliche Übermittlung personenbezogener Daten per E-Mail (im Ergebnis also: jede E-Mail) bedürfe zwingend einer Ende-zu-Ende-Verschlüsselung.

   Unzweifelhaft richtig ist auch die weitere Feststellung (a.a.O., Ziff. 4.1.2), dass bei E-Mail-Verkehr mit hohem Datenschutz-Risiko qualifizierte Transportverschlüsselung oder Ende-zu-Ende-Verschlüsselung einzusetzen sind. Der Datenschutz-Mindeststandard kann je nach besonderen Umständen des Einzelfalles abweichen (a.a.O., Ziffer 4.2.2).

3. Nützlich und lobenswert stellt die Orientierungshilfe (insbesondere Ziffer 5) komprimiert die Sicherungs-Stufen nach aktuellem Stand der Technik dar. Dies entspricht dem gesetzlichen Aufklärungs- und Beratungsauftrag der Datenschutz-Aufsichtsbehörden.

4. <u>Entschieden abzulehnen sind jedoch die Aussagen unter Ziffer 4.2.3 der Orientierungshilfe. Die Datenschutz-Aufsichtsbehörden überschreiten dort ihren Zuständigkeitsbereich, greifen in fremde Kompetenzen ein und stellen unklare, nicht erfüllbare Anforderungen:</u>

   a) Unter der Überschrift „Versand von E-Mail-Nachrichten mit geheim zu haltenden Inhalten bei hohen Risiken" wird behauptet:

      „Verantwortliche, die aufgrund von § 203 StGB zur Geheimhaltung von Kommunikationsinhalten verpflichtet sind, müssen über die unter 4.2.1 bzw. 4.2.2 aufgeführten Anforderungen hinaus durch Verschlüsselung sicherstellen, dass nur Stellen eine Entschlüsselung vornehmen können, an die die Inhalte der Nachrichten offenbart werden dürfen.“

b) § 203 StGB ist keine datenschutzrechtliche Vorschrift. Die Datenschutz-Aufsichtsbehörden scheinen zu verkennen, dass Berufsgeheimnisse sich nicht nur auf personenbezogene Daten beziehen und andererseits nicht jede Verarbeitung personenbezogener Daten durch Berufsgeheimnisträger (z. B. durch Rechtsanwälte) dem Berufsgeheimnis unterfällt.

Der Schutz von Berufsgeheimnissen ist strafrechtlich und berufsrechtlich sichergestellt. Er wird dementsprechend durch Gerichte, Strafverfolgungsbehörden und Berufskammern vollzogen. Datenschutz-Aufsichtsbehörden sind insoweit nicht beteiligt.

Ob und wann bei Informationen, die dem Berufsgeheimnis unterliegen, mit Blick auf die berufsrechtliche Verschwiegenheitspflicht durchschnittliche oder hohe Risiken anzunehmen sind, ist deshalb ebenso wenig durch die Datenschutz-Aufsichtsbehörden zu beurteilen wie die Frage, welche Schutzmaßnahmen (auch mit Blick auf anfallende Implementierungskosten) angemessen erscheinen. Das Berufsgeheimnis dient dem Schutz der betroffenen Mandanten und der Funktion der Rechtspflege. Mandanten sollen nicht dadurch an der Inanspruchnahme anwaltlicher Unterstützung gehindert werden, dass sie dabei einen Vertraulichkeitsbruch zu befürchten hätten. Wo der Mandant aber gar keine Vertraulichkeit wünscht und auf diese verzichtet, kann er durch Offenbarungen von Mandatsinhalten auch nicht von der Inanspruchnahme anwaltlicher Unterstützung abgehalten oder sonst in seinen Interessen beeinträchtigt und insbesondere nicht in seinen Persönlichkeitsrechten verletzt werden. Es steht daher in berufsrechtlicher Hinsicht allein dem Mandanten zu, über den Grad der Schutzbedürftigkeit zu entscheiden und notfalls auch auf einen Schutz der Vertraulichkeit zu verzichten. Insoweit infolge eines solchen Verzichts berufsrechtlich keine Vertraulichkeit geboten ist und für den Anwalt keine Pflicht zur Verschwiegenheit besteht, kann in datenschutzrechtlicher Hinsicht auch nicht unter Berufung auf die vermeintlich berufsrechtlich gebotene Vertraulichkeit etwas Gegenteiliges hergeleitet werden.

Dies gilt umso mehr für solche Mandatskommunikationen, bei denen der Personenbezug und die mit der Datenverarbeitung für die beteiligten Personen einhergehenden Risiken als gering einzustufen sind. Erstellt beispielsweise ein Rechtsanwalt ein Gutachten zu den rechtlichen Implikationen des Brexits für den Geschäftsbetrieb einer GmbH, werden darin regelmäßig nur wenige und nicht überdurchschnittlich schützenswerte personenbezogene Daten zu finden sein. Die sich aus einem solchen Gutachten etwaig ergebende Information, dass ein namentlich genannter Mitarbeiter für das entsprechende Unternehmen tätig ist und dass dieses nun den bevorstehenden Brexit zu bewältigen hat, dürfte nach datenschutzrechtlichen Kriterien nicht als überdurchschnittlich schützenswert einzustufen sein. Zwar kann sich – dem Wunsch der Mandantin entsprechend – aus dem Berufsrecht ein höherer Schutzbedarf ergeben. Die Einschätzung dieser berufsrechtlichen Frage obliegt jedoch allein den Berufskammern und Gerichten – nicht aber den Datenschutzbehörden.

Mit der GmbH genießt zudem im Beispielsfall wie in unzähligen anderen Fällen eine juristische Person den Schutz des Berufsgeheimnisses und keine natürliche Person, welche den Schutz des Datenschutzrechts für sich in Anspruch nehmen könnte. Die offenbar seitens der Datenschutzbehörden bestehende Annahme, dass bei Bestehen eines Berufsgeheimnisses zwangsläufig personenbezogene Daten verarbeitet würden und dass dabei regelmäßig besondere Risiken für personenbezogene Daten bestünden, trifft auch insoweit nicht zu.

Mandatskommunikationen mit umfangreichem Personenbezug, besonderen Kategorien personenbezogener Daten oder sonstigen besonderen Risiken sind in datenschutzrechtlicher Hinsicht freilich anders zu beurteilen. Maßstab für die Datenschutzaufsicht muss und darf insoweit aber aus den genannten Gründen nur das Datenschutzrecht sein. Die Einhaltung des

Berufsrechts wird demgegenüber entsprechend der hierfür einschlägigen Normen und Schutzzwecke unabhängig von datenschutzrechtlichen Erwägungen durch die Berufskammern und Gerichte sichergestellt.

c) Darüber hinaus ist diese Passage der Orientierungshilfe unklar und nicht umsetzbar.

Sie verlangt „über die unter 4.2.1 bzw. 4.2.2 aufgeführten Anforderungen hinaus“ (damit auch noch hinausgehend über eine Ende-zu-Ende-Verschlüsselung) „durch Verschlüsselung sicherzustellen, dass nur Stellen eine Entschlüsselung vornehmen können, an die die Inhalte der Nachrichten offenbart werden dürfen“.

Es ist aber gerade Sinn und Zweck einer jeden Nachrichten-Verschlüsselung, dass sie nur von den vorgesehenen Kommunikationsteilnehmern (also nicht von unbefugten Dritten) entschlüsselt werden kann. Mit anderen Worten: Wenn eine E-Mail ordnungsgemäß Ende-zu-Ende-verschlüsselt wird, dann kann sie nur vom Empfänger entschlüsselt werden. Andernfalls sind die Verschlüsselungsmaßnahmen mangelhaft.

Bei Ende-zu-Ende-Verschlüsselung kann und muss also nicht durch zusätzliche Maßnahmen sichergestellt werden, dass nur der vorgesehene Nachrichten-Adressat die Entschlüsselung vornehmen kann.

Kompetenz-Überschreitungen der Datenschutz-Aufsichtsbehörden zu Lasten der Berufsgeheimnisträger und der dortigen Aufsichtsbehörden sind ein wiederkehrendes Problem. Zuletzt behauptete z. B. die Berliner Beauftragte für Datenschutz und Informationsfreiheit in ihrer Stellungnahme „zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen“, Version 1.1 vom 22. Mai 2020, Berufsgeheimnisträger dürften „nur Dienstleister einsetzen, die bei einem Vertraulichkeitsbruch strafrechtlich belangt werden können“ (a.a.O., S. 2). Dies ist inhaltlich falsch und von der Datenschutz-Aufsicht überhaupt nicht zu beurteilen.

Grundsätzlich ist die Orientierungshilfe zu begrüßen. Sie kann die Erfüllung der Datenschutz-Anforderungen bei E-Mail-Kommunikationen auch für die Anwaltschaft erleichtern und unterstützen.

Ziffer 4.2.3 der Orientierungshilfe gibt jedoch – einmal mehr – Anlass, die Datenschutz-Aufsichtsbehörden daran zu erinnern, dass sie für den Schutz von Berufsgeheimnissen und die berufsrechtliche Aufsicht nicht zuständig sind.

* * *