Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), D – 20095 Hamburg

Klosterwall 6, Block C
D – 20095 Hamburg
Telefon: 040 - 428 54 - 40 49 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartnerin:

E-Mail*:

Az.: D42 /2017/1114

Hamburg, den 08.01.2018

Versendung von unverschlüsselten E-Mails bei Berufsgeheimnisträgern; Ihre Anfrage vom 07.11.2017

Sehr geehrter Herr ,

Prof. Caspar hat mir zuständigkeitshalber Ihre Anfrage vom 07.11.2017 zur Beantwortung übergeben. Diese betrifft die Versendung von unverschlüsselten E-Mails bei Berufsgeheimnisträgern (z.B. Apotheker, Ärzte und Rechtsanwälte). Zu dieser Frage interessiert Sie insbesondere, ob eine Pflicht für Berufsgeheimnistärger besteht und der Standpunkt des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) sowie mögliche Lösungsansätze für die Anwaltschaft.

Ihre Frage betrifft nicht originär die mandatsbezogene anwaltliche Verschwiegenheitspflicht. Vielmehr geht es darum, dass technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten nicht bzw. nicht ausreichend eingehalten werden, indem E-Mails, die personenbezogene Daten enthalten, unverschlüsselt versandt werden.

Spezialgesetzliche Regelungen zum Umgang mit personenbezogenen Daten bei der Versendung von E-Mails finden sich in den berufsrechtlichen Vorschriften BORA und BRAO nicht. § 43 a Abs. 2 BRAO und § 2 Abs. 1 BORA normieren zwar die Verschwiegenheitspflicht der Rechtsanwaltschaft als Grundpflicht, enthalten aber keine ausdrückliche Regelung zum technischen oder organisatorischen Umgang bei der Verarbeitung personenbezogener Daten.

Rechtsanwälte sind nicht-öffentliche Stellen, so dass das Bundesdatenschutzgesetz (BDSG) Anwendung findet.

Gem. § 9 BDSG haben nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Dabei bestimmt die Anlage zu § 9 Satz 1 Nr. 4 BDSG ausdrücklich:

> *„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,*
> *[…]*
> *4. 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 Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“*

Die Auswahl der zu treffenden Maßnahmen ist dabei aber durch eine Abwägung zwischen Schutzbedarf auf der einen und Aufwand auf der anderen Seite zu treffen. Kurz gesagt bedeutet dies, je höher der Schutzbedarf der Daten ist, desto höher muss auch der Aufwand sein, um die Daten entsprechend vor Zugriffen Dritter zu schützen. Dabei ist der Stand der Technik ebenso zu berücksichtigen wie der Aufwand für die Daten verarbeitende Stelle.

Die Einhaltung der technischen und organisatorischen Maßnahmen wird grundsätzlich für nicht abdingbar gehalten. Betroffene können auch nicht darin einwilligen, dass ihre Daten ohne einen ausreichenden Schutz nach dem Stand der Technik verarbeitet werden. Ein sicherer Kommunikationskanal ist deshalb nicht nur für Online-Banking, Online-Shopping und eGovernment-Dienste, sondern auch für E-Mail und alle anderen Web-basierten Anwendungen unabdingbar. Verschlüsselung ist nach wie vor die sicherste Möglichkeit, personenbezogene Daten vor Missbrauch zu schützen. Daher scheidet auch die elektronische Übertragung sensibler personenbezogener Daten ohne Verschlüsselung etwa per Mail aus, auch wenn der Betroffene explizit um die Übersendung per Mail bittet (vgl. Hamburgisches Datenschutzgesetz, Gesetzestext und Erläuterungen, HmbBfDI, 1. Aufl., 2013, S. 78).

Man unterscheidet dabei zwischen der Transportverschlüsselung (z.B. TLS) sowie der Ende-zu-Ende Verschlüsselung (z.B. S/MIME oder PGP). Aus datenschutztechnischer Sicht ist eine Ende-zu-Ende Verschlüsselung zu bevorzugen. Nach Maßgabe der Abwägung kann etwa auf die Nutzung von De-Mail zurückgegriffen werden. Die De-Mail ist ein durch Bundesgesetz geregeltes Kommunikationsverfahren, über das „auf einer elektronischen

Kommunikationsplattform“ ein „sicherer, vertraulicher und nachweisbarer Geschäftsverkehr für jedermann im Internet sichergestellt“ werden soll (§ 1 Abs. 1 De-Mail-Gesetz). De-Mail garantiert den Einsatz von Transportverschlüsselung und ist ein vom BSI zertifiziertes Verfahren. Es lässt sich zudem durch eine Ende-zu-Ende Verschlüsselung erweitern.

In diesem Zusammenhang möchte ich auch auf den 25. Tätigkeitsbericht des HmbBfDI verweisen. Unter IV.4.2 legt der HmbBfDI seinen Standpunkt zum Datenschutz in Rechtsanwaltskanzleien dar. Hier finden Sie auch weitergehende Informationen zum Thema Verschlüsselung (vgl. VI.1.1, V.13, III.1.3, II.2.4, II.1.5). Den Tätigkeitbericht können Sie unter folgendem Link abrufen: https://www.datenschutz-hamburg.de/uploads/media/25._Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf).

Vorgenanntes stellt nur die derzeit geltende Rechtslage dar. Konkret bedeutet dies, dass ein Verstoß gegen § 9 BDSG keine Ordnungswidrigkeit i.S.d. § 43 BDSG darstellt. Anders sieht es aber nach der ab Mitte dieses Jahres geltenden Datenschutzgrundverordnung (DSGVO) aus. Die Gewährleistung von Datensicherheit ist dann nicht nur gesetzlich verankert, sie stellt zudem die Bedeutung des technischen und organisatorischen Datenschutzes heraus (vgl. Art. 5 Abs. 1f und Art. 32 DSGVO). Dies wird insbesondere dadurch deutlich, dass zukünftig ein Verstoß gegen technisch-organisatorische Maßnahmen mit Geldbußen geahndet werden kann (vgl. Art. 83 DSGVO).

Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach alledem nicht nur bedenklich, sondern stellt auch ein ungeeignetes Kommunikationsmittel dar.

Für Rückfragen stehe ich Ihnen selbstverständlich jederzeit zur Verfügung.

Mit freundlichen Grüßen