RECHTSANWALTSKAMMER
FRANKFURT AM MAIN

50. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten – Hinweise zum Datenschutz –

zusammengefasst
vom Referenten der Rechtsanwaltskammer Frankfurt am Main
Rechtsanwalt Dr. Marc Zastrow

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat nach Art. 59 DS-GVO i.V.m. § 15 HDSIG seinen 50. Tätigkeitsbericht Datenschutz für 2021 nebst 4. Tätigkeitsbericht Informationsfreiheit vorgelegt:

Aus anwaltlicher Sicht sind insbesondere folgende Themen von Interesse:

Interessenkonflikte bei Datenschutzbeauftragten

Unter Nr. 11.4 (S.140 ff.) teilt der Hessische Datenschutzbeauftragte mit, dass die Vereinbarkeit der Tätigkeit als Datenschutzbeauftragter mit anderen Tätigkeiten im Unternehmen immer wieder Gegenstand von Anfragen oder Beschwerden bei ihm ist und beschreibt einige relevante Konstellationen. Auch Anwaltskanzleien müssen bei Vorliegen der Voraussetzungen des Art. 37 DS-GVO oder des § 38 BDSG ein(n) Datenschutzbeauftragte(n) benennen. Nach § 38 Abs.1 BDSG müssen Kanzleien stets eine(n) Datenschutzbeauftragte(n) benennen, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Da unabhängig davon alle Kanzleien zur Einhaltung des Datenschutzrechts verpflichtet sind, kann es sich auch bei fehlender Verpflichtung zur Benennung einer/s Datenschutzbeauftragten empfehlen, freiwillig eine(n) Datenschutzbeauftragte(n) zu benennen.

Nach Art.37 Abs.7 DS-GVO sind die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und diese Daten sind dem Hessischen Datenschutzbeauftragten als Aufsichtsbehörde mitzuteilen. Der Hessische Datenschutzbeauftragte bittet darum, hierfür das Online-Meldeformular zu verwenden und von schriftlichen Meldungen abzusehen.
Nach Art. 38 Abs. 6 DS-GVO kann der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen, die Verantwortlichen haben jedoch sicherzustellen, dass diese nicht zu einem Interessenkonflikt führen. Der Hessische Datenschutzbeauftragte weist auf den engen Zusammenhang mit dem in Art. 38 Abs. 3 S. 1 DS-GVO bestimmten Erfordernis einer unabhängigen Tätigkeit des Datenschutzbeauftragten hin. Weiter führt er aus (S. 141 f.):

„Interessenkonflikte können sich regelmäßig aus der Stellung im Unternehmen ergeben (Inhaber, Mitglieder der Geschäftsführung oder des Vorstandes). Diese Personen sind originär für die Rechtmäßigkeit der Datenverarbeitung beim Verantwortlichen oder beim Auftragsverarbeiter verantwortlich und können sich nicht wirksam selbst kontrollieren (siehe auch Art. 38 Abs. 3 Satz 3 DS-GVO, nach dem der Datenschutzbeauftragte unmittelbar der höchsten Managementebene berichtet). Ferner ist in der Regel die Benennung von Leitungspersonen nicht zulässig: Dies gilt insbesondere für die Leitung der Personalabteilung (aufgrund der damit einhergehenden Verantwortung für den Umgang mit Beschäftigtendaten), die Leitung der IT-Abteilung (wegen der mit dieser Funktion

einhergehenden Verantwortung für die technisch-organisatorischen Maßnahmen) sowie die Leitung der Marketing- oder Vertriebsabteilung (wegen der Verantwortung für den Umgang mit Kundendaten). Auch ist eine Benennung bei hierarchisch nachgeordneten Positionen wie etwa Beschäftigte der IT- (insbesondere mit Administratorenrechten) oder Personal-Abteilung regelmäßig unzulässig, sofern diese in der Lage sind, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen. Des Weiteren ist die Benennung eines Datenschutzbeauftragten regelmäßig unzulässig, sofern dieser ein besonderes wirtschaftliches Interesse an dem Unternehmenserfolg hat (etwa Gesellschafter sowie Familienangehörige der Geschäftsleitung)."

Auch die Benennung von IT-Sicherheitsbeauftragten und Compliance-Beauftragten erachtet der Hessische Datenschutzbeauftragte als kritisch. Außerdem weist er darauf hin, dass auch bei externen Datenschutzbeauftragten Interessenkonflikte auftreten können, beispielsweise wenn diese gleichzeitig mit IT-Dienstleistungen beauftragt sind.

Auskunftsanspruch versus Tipping-Off-Verbot

Nach § 47 Abs. 1 GwG dürfen Verpflichtete im Sinne des GwG, zu welchen unter den Voraussetzungen des § 2 Abs. 1 Nr. 10 GwG auch Rechtsanwältinnen und Rechtsanwälte gehören, den Vertragspartner (also die Mandantschaft) nicht von einer beabsichtigten oder erstatteten Verdachtsmeldung nach § 43 GwG, einem daraufhin eingeleiteten Ermittlungsverfahren oder einem Auskunftsverlangen der FIU nach § 30 Abs. 3 GwG in Kenntnis setzen. Hierbei ist allerdings die Einschränkung der Melde- bzw. Auskunftspflicht für Rechtsanwältinnen und Rechtsanwälte nach §§ 30 Abs. 3 S. 3 und 4, 43 Abs. 2 GwG zu beachten. Der Hessische Datenschutzbeauftragte hat unter Nr.14.2 (S. 162 ff.) im Hinblick auf Banken klargestellt, dass die grundsätzliche Pflicht, auf Antrag nach Art. 15 DS-GVO Auskunft zu den verarbeiteten Daten zu erteilen, durch dieses sogenannte Tipping-Off-Verbot eingeschränkt ist (§ 47 GwG i.V.m. Art. 23 Abs. 1 lit e DS-GVO und § 29 Abs. 1 S. 2 BDSG); die Auskunft muss also so beschränkt werden, dass die Mandantschaft nichts von einer gegen sie erstatteten Verdachtsanzeige etc. erfährt.

Fehlversand von Kundenanschreiben

Wie der Hessische Datenschutzbeauftragte unter Nr. 14.3 (S. 166 ff.) ausführt, gehört der Fehlversand von Kundenanschreiben zu den häufigsten gemeldeten Datenschutzverstößen, löst allerdings nicht immer eine Meldepflicht nach Art. 33 DS-GVO aus. In jedem Einzelfall ist eine Risikobewertung vorzunehmen, bei Unsicherheit sollte beim Hessischen Datenschutzbeauftragten nachgefragt werden. Meldepflichtige Datenschutzpannen können sich sowohl durch eine fehlerhafte Adressierung von Schreiben als auch durch die Beifügung falscher Anlagen bzw. Seiten ergeben. Nach Art. 33 Abs. 1 DS-GVO muss der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Die 72-Stunden-Frist verlängert sich nicht, soweit sie auf ein Wochenende fällt (S. 197 ff.). Beim Fehlversand von Unterlagen sind im Rahmen der Risikobeurteilung insbesondere Inhalt und Empfänger des Schreibens sowie betroffene Person zu berücksichtigen. Zu einer Meldepflicht aufgrund des Inhalts führen beispielsweise Anschriftendaten, Vermögensaufstellungen und Gesundheitsdaten. Melde

sich der Empfänger selbst, händigt die zu Unrecht erhaltenen Unterlagen aus und bestätigt idealerweise zusätzlich, keine Kopien gefertigt zu haben, könne der Verzicht auf eine Meldung durchaus gut zu vertreten sein.

Rechnungen aus der Apotheke per E-Mail ?

Unter Nr. 17.2 (S. 184 ff.) führt der Hessische Datenschutzbeauftragte aus, dass bei der Übermittlung von Apothekenrechnungen per E-Mail zum Schutz der hier betroffenen Gesundheitsdaten eine Inhaltverschlüsselung („Ende-zu-Ende-Verschlüsselung“) erforderlich ist. Nach Art. 5 Abs. 1 lit. f DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die deren angemessene Sicherheit gewährleistet („Integrität und Vertraulichkeit“). Art. 32 DS-GVO verlangt von den Verantwortlichen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei Rechnungen von Apotheken sind die nach Art. 9 Abs. 1 DS-GVO besonders geschützten Gesundheitsdaten betroffen, so dass eine Transportverschlüsselung nach Auffassung des Hessischen Datenschutzbeauftragten nicht ausreichend ist.

Hierzu folgende ergänzende Hinweise:
Nach Urteil des VG Mainz vom 17.12.2020 – 1 K 778/19.MZ (BRAK-Mitteilungen 2021, 104 ff.; vgl. hierzu auch den Aufsatz von Schöttle in BRAK-Mitteilungen 2021, 77 ff.) ist ein angemessenes Schutzniveau im Sinne des Art. 32 Abs. 1 DS-GVO auch bei Rechtsanwälten und anderen Berufsgeheimnisträgern grundsätzlich durch Nutzung einer (obligatorischen) Transportverschlüsselung anzunehmen, soweit nicht im Einzelfall – wie bei Daten nach Art. 9 Abs. 1 oder Straftaten nach Art. 10 DS-GVO - besondere Anhaltspunkte für einen erhöhten Schutzbedarf bestehen.

Im Hinblick auf die anwaltliche Verschwiegenheitspflicht ist auch darauf hinzuweisen, dass nach § 2 Abs. 2 S. 5 und 6 BORA zwischen Rechtsanwalt und Mandant die Nutzung eines mit Risiken für die Vertraulichkeit verbundenen elektronischen Kommunikationsweges jedenfalls dann erlaubt ist, wenn der Mandant zustimmt oder diesen Kommunikationsweg vorschlägt oder beginnt und nach Hinweis des Rechtsanwalts auf die Risiken fortsetzt. Nach § 10 Abs. 1 RVG kann der Rechtsanwalt die Vergütung allerdings nur aufgrund einer von ihm unterzeichneten Berechnung einfordern. Für Anwaltsrechnungen besteht also ein Schriftformerfordernis, sofern die Mandantschaft nicht auf eine schriftliche Rechnung verzichtet (Gerold / Schmidt, RVG § 10 Rn. 23).

Diskretion in Arztpraxis

Unter Nr. 17.3 (S. 187 ff.) weist der Hessische Datenschutzbeauftragte darauf hin, dass Arztpraxen die Wahrung der nötigen Diskretion in ihren Räumlichkeiten sicherstellen müssen und vertrauliche Gespräche am Praxisempfang grundsätzlich nicht im Wartezimmer hörbar sein dürfen. In diesem Zusammenhang weist er nicht nur auf das Gebot der Vertraulichkeit nach Art. 5 Abs. 1 lit. f DS-GVO, sondern auch auf die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB hin. Das gilt für Anwaltskanzleien entsprechend (vgl. § 203 Abs. 1 Nr. 3 StGB).

Angriffe auf Exchange-Schwachstellen in Rechtsanwaltskanzleien

Dieser eine Vielzahl von Anwaltskanzleien betreffende Beitrag unter Nr. 18.3 III. (S. 227 f.) wird nachfolgend im Wortlaut wiedergegeben:

„Auch hessische Rechtsanwaltskanzleien waren Ziele von Angriffen, die Schwachstellen der Exchange-Server-Software ausnutzten. Rechtsanwaltskanzleien müssen als datenschutzrechtlich Verantwortliche gemäß Art. 24 DS-GVO i.V.m. Art. 32 DS-GVO die Sicherheit der Verarbeitung der ihnen anvertrauten Daten gewährleisten und müssen sich daher proaktiv und ernsthaft mit dem Thema der Informationssicherheit auseinandersetzen.

Rechtsanwaltskanzleien in Hessen waren ebenfalls von der Ausnutzung der Sicherheitslücken in Microsofts Exchange-Server-Software betroffen. Meine Behörde hat sich hierzu frühzeitig an die hessischen Rechtsanwaltskammern gewendet und über die Problematik informiert. Die Rechtsanwaltskammer Frankfurt am Main hat daraufhin eine Warnung und Hinweise zu Abhilfemaßnahmen des BSI auf ihrer Internetseite veröffentlicht. In der Folge wurden mir zahlreiche Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO gemeldet.

Rechtsanwaltskanzleien müssen als datenschutzrechtlich Verantwortliche gemäß Art. 32 DS-GVO für die Sicherheit der Verarbeitung personenbezogener Daten Sorge tragen. Hierzu gehören „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Nach dem Bekanntwerden von Sicherheitslücken in der elektronischen Datenverarbeitung muss eine unverzügliche Untersuchung und Absicherung potenziell betroffener Systeme erfolgen. Dies setzt voraus, dass der Verantwortliche sich entweder selbst oder durch beauftragte Dienstleister bereits im Vorfeld aktiv über Entwicklungen im Bereich der IT-Sicherheit informiert. Der unbestimmte Rechtsbegriff des „Stands der Technik“ unterliegt einem stetigen Wandel, den der Verantwortliche verfolgen muss. Nachdem die Bedrohung durch die Installation der vom Hersteller bereitgestellten Sicherheitsupdates und durch ergänzende Maßnahmen zunächst abgewendet zu sein schien, erreichten mich Ende des Jahres 2021 immer noch Meldungen über das Ausnutzen vorhandener oder neu aufgetretener Sicherheitslücken in der Exchange-Server-Software. Häufig wurden die kompromittierten Server zum Versand von E-Mails mit Hyperlinks verwendet, die Schadsoftware nachladen und dadurch weitere Systeme der Nachrichtenempfänger infizieren können. Hierbei sind praktisch in allen Fällen personenbezogene Daten betroffen, da die versandten E-Mails regelmäßig Metadaten und Nachrichteninhalte der gespeicherten Korrespondenz enthalten, um beim Empfänger den Anschein der Echtheit zu erwecken. Die nachgeladene Schadsoftware kann wiederum eine Verschlüsselung der Zielsysteme vornehmen, um im Anschluss Lösegeld für die verschlüsselten Daten zu erpressen. Ein solcher Vorfall beeinträchtigt die Verfügbarkeit personenbezogener Daten und kann gravierende Folgen für den laufenden Geschäftsbetrieb von Rechtsanwaltskanzleien haben.

Zu beachten ist außerdem, dass gemäß Art. 34 Abs. 1 DS-GVO eine Benachrichtigung betroffener Personen über die Verletzung des Schutzes personenbezogener Daten erforderlich ist, wenn hohe Risiken für deren Rechte und Freiheiten nicht ausgeschlossen werden können. Dies liegt bei einem Abfluss von personenbezogenen Daten, die einem Berufsgeheimnisträger anvertraut sind, besonders nahe. Benachrichtigungen wurden von

den Verantwortlichen zumeist proaktiv vorgenommen. In einzelnen Fällen erfolgte dies erst nach einem Hinweis meiner Behörde. Gemäß Art. 34 Abs. 3 lit.c DS-GVO kann die Benachrichtigung auch durch öffentliche Bekanntmachung, wie einem Hinweis auf der Internetseite des Verantwortlichen, erfolgen, wenn sie ansonsten mit unverhältnismäßigem Aufwand verbunden wäre.

Die beschriebenen Vorfälle zeigen eindrucksvoll, dass Rechtsanwälte und Notare, die Informationstechnologie zur beruflichen Kommunikation nutzen, sich ernsthaft und kontinuierlich mit der Absicherung und Instandhaltung ihrer Systeme auseinandersetzen müssen. In der vernetzten Welt ist jedes über das Internet erreichbare System ein potenzielles Ziel für Cyberattacken. Dies gilt ohne Rücksicht auf Standort, Größe, Rechtsform oder etwaige Eigenschaft des Verantwortlichen als Berufsgeheimnisträger."

Orientierungshilfe der DSK-Konferenz „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail"

Im Anhang I. 3 hat der Hessische Datenschutzbeauftragte auf S. 255 ff. unter anderem die Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 (Stand: 16. Juni 2021) zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail veröffentlicht, die auch auf der Website des Hessischen Datenschutzbeauftragten unmittelbar abrufbar ist:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/DSK101_orientierungshilfe_e_mail_verschluesselung.pdf

4. Tätigkeitsbericht des Hessischen Informationsfreiheitsbeauftragten:

„voraussetzungsloser" Informationszugang und kommunaler Satzungsvorbehalt
Der Hessische Beauftragte für Datenschutz und Informationsfreiheit macht unter Nr. 2 (S. 269 ff.) des Informationsfreiheitsberichts deutlich, dass die Informationsansprüche nach §§ 80 ff. HDSIG gerade nicht von einer eigenen Betroffenheit oder Belastung abhängen. Dem dort geschilderten Fall lag die Beschwerde eines Rechtsanwalts zugrunde, der einen Mandanten in einer Straßenverkehrsangelegenheit (Geschwindigkeitsverstoß) vertrat und rügte, dass ihm die Einsicht in Unterlagen zu Probemessungen (Radaranlagen) in der Stadt Kassel nicht gewährt worden sei. Letztlich blieb die Beschwerde erfolglos, da die Geltung des kommunalen Informationsfreiheitsrechts in Hessen nach § 81 Abs. 1 Nr. 7 HDSIG unter Satzungsvorbehalt steht und die Informationsfreiheitssatzung der Stadt Kassel nur den Selbstverwaltungsbereich betraf, nicht aber den Bereich der übertragenen Verwaltungsaufgaben, um den es hier ging. Dessen ungeachtet zeigt der Fall, dass die Informationsbeschaffung nach §§ 80 ff. HDSIG in geeigneten Fällen auch dann in Betracht zu ziehen ist, wenn diese nicht Zweck der Mandatierung ist, aber hierdurch für die Bearbeitung des konkreten Mandats nützliche Informationen zu erwarten sind.