*Jan Marcel Stammkötter**

Datenschutzverletzungen und Datenpannenmanagement bei Berufsgeheimnisträgern am Beispiel der Anwaltschaft

Vorsorge ist besser als Nachsorge? – Eine wissenschaftliche Auseinandersetzung mit der Melde- und Dokumentationspflicht aus Art. 33 Abs. 1, 5 DSGVO unter Berücksichtigung reaktiver sowie präventiver Aspekte

A. Einleitung

Die Technisierung und Digitalisierung des alltäglichen Lebens schreitet schnellen Fußes voran. Angefangen im privaten Bereich erstreckt sich dieser Wandel nach und nach auch auf die Berufswelt – diese wird sichtbar digitaler: Seit kurzer Zeit werden Prozesse, die früher analog angelegt waren, mit Erfolg digitalisiert. Beschleunigt durch die Corona-Pandemie werden Meetings und Fortbildungsveranstaltungen, aber zunehmend auch ganze Tagungen und Messen in den digitalen Raum verlegt.

Dieser Wandel macht auch keinen Halt vor Justiz und Anwaltschaft. Mit der Technisierung des beruflichen Alltags gehen vielfältige Vorteile einher, zum Beispiel durch die digitale Aktenbearbeitung, die durch den Einsatz diverser Videokonferenzlösungen vereinfachte und ortsunabhängige Besprechungsmöglichkeit mit dem Mandanten, die Durchführung von Gerichtsverhandlungen per Videokonferenz sowie die vereinfachte und rechtssichere Kommunikation über Postfächer wie dem besonderen elektronischen Anwaltspostfach. Überzeugen auf einen ersten Blick die Vorteile dieser neuen digitalen Kommunikations- und Arbeitsmittel insb. hinsichtlich Schnelligkeit und Komfort, so dürfen der Datenschutz und die Datensicherheit nicht aus dem Blick geraten, denn die im Jahre 2018 in Kraft getretene Datenschutzgrundverordnung schließt die Anwaltschaft nicht aus dem persönlichen Anwendungsbereich der Verordnung aus. Somit gilt diese, wenn auch mit Einschränkungen durch den nationalen Gesetzgeber, mangels Bereichsausnahme auch für die Berufsgruppe der Rechtsanwälte.

Bedingt durch die zunehmende Digitalisierung steigt nach übereinstimmender Angabe von Bundeskriminalamt und BSI[1] die Gefahr externer Cyberangriffe. Diese

* Der Verfasser ist Diplom-Jurist und Mitarbeiter in einer auf das Wirtschaftsrecht spezialisierten Kanzlei in Bielefeld sowie Student des LL.M.-Studiengangs „IT und Recht“ an der Universität des Saarlandes. Bei dem Beitrag handelt es sich um eine Studienarbeit, welche im Wintersemester 2021/22 im Modul Datenschutzrecht bei Prof. Dr.-Ing. Christoph Sorge verfasst wurde

zielen vermehrt auf das sog. „Big Game“[2], folglich auf große und wirtschaftlich besonders relevante Unternehmen, ab. Somit muss überall dort, wo personenbezogene Daten verarbeitet werden, ein besonderer Fokus auf die Sicherheit der Verarbeitung gelegt werden. Kommt es entgegen aller Bemühungen zu einer Datenpanne, so ist ein schnelles und umsichtiges Handeln erforderlich, um den drohenden Schaden, begünstigt durch die häufig einhergehende große mediale Aufmerksamkeit[3], einzudämmen bzw. abzuwenden.

B. Datenpannen

Um in dieser Arbeit die rechtlichen Folgen und den richtigen Umgang mit Datenpannen analysieren zu können, muss zunächst erörtert werden, wann eine Datenpanne vorliegt.

I. Über das Vorliegen einer Datenpanne

Das Vorliegen einer Datenpanne bzw. einer Datenschutzverletzung, ist in Art. 4 Nr. 12 DSGVO legaldefiniert. Hiernach ist eine Datenpanne gegeben, wenn eine unbeabsichtigte oder unrechtmäßige Datenverarbeitung zur Vernichtung, Veränderung, Verlust, Offenlegung bzw. zum unbefugten Zugang zu personenbezogenen Daten, die Gegenstand des Verarbeitungsvorganges sind, führt. Es wird einerseits hervorgehoben, dass es auf einen bestimmten Verschuldensmaßstab nicht ankommt, sodass sowohl Vorsatz als auch Fahrlässigkeit vorwerfbar sind.[4] Andererseits wird durch die Bezugnahme auf die Schutzziele der Integrität, Vertraulichkeit und Verfügbarkeit, abgeleitet aus den Grundsätzen der Datenverarbeitung gem. Art. 5 Abs. 1 lit. f) DSGVO, hervorgehoben, dass es hinsichtlich der Frage, ob eine Datenpanne vorliegt, nicht um die datenschutzrechtliche Zulässigkeit der Datenverarbeitung, sondern um die Datensicherheit, welche durch Art. 32 Abs. 1 DSGVO näher konkretisiert wird, geht.[5]

Datenpannen können in vielerlei Hinsicht auftreten. Mit Fokus auf die Rechtsanwaltschaft haben sich beispielhaft folgende Szenarien[6] herausgebildet, welche als

---

1 BKA, BLB Cybercrime 20, S. 3, 9ff.; BSI, Lagebericht IT-S. 2021, S. 9, 11ff., 87.

2 BKA, BLB Cybercrime 20, S. 29; BSI, Lagebericht IT-S. 2021, S. 12; Maisch, Cybergefahren, S. 1.

3 Fuhlrott, Data Incident Management, NZA 2019, 649, 649; so z.B. Hall, Cyberangriff DLA, S. 1; Sehl, KG weiter offline, LTO.

4 Schild in BeckOK-DS, Art. 4 Rn. 135; Ernst in Paal/Pauly, Art. 4 Rn. 95.

5 Klabunde in Ehmann/Selmayr, DS-GVO, Art.4 Rn. 56, 58.

6 Beispiele nach dem Foliensatz von RAin Carola Sieling, welche jedoch aufgrund gleichgelagerter Problemfelder von Unternehmen auf Anwaltskanzleien übertragen werden können.

Datenpannen einzustufen sind: Werden personenbezogene Daten fehlversendet (z.B. Fehlversand einer E-Mail / Nachricht per beA), so handelt es sich um eine Verletzung des Schutzziels der Vertraulichkeit, mithin um einen unbefugten Zugang zu personenbezogenen Daten. Ein Cyberangriff, sofern dieser mit einer Datenveränderung in Form der Verschlüsselung (sog. Ransomware) oder gar Löschung einhergeht, bedeutet eine Verletzung des Schutzziels der Verfügbarkeit. Entgegen der Auffassung der Referentin sind jedoch das Speichern von Informationen auf einem nicht zulässigen Medium[7] (z.B. Speichern beruflicher Daten auf einem privaten Datenträger) sowie die Nutzung unzulässiger Kanäle für den Austausch personenbezogener Daten nicht als Datenpanne zu charakterisieren. Vielmehr handelt es sich hierbei um eine Verletzung interner Anweisungen bzw. Compliance-Regeln der betreffenden Kanzlei, sodass vorliegend die datenschutzrechtliche Zulässigkeit der Speicherung bzw. Nutzung des Kommunikationskanals problematisch ist. Mangels einer Schutzzielverletzung des an sich berechtigten Mitarbeiters scheidet das Vorliegen einer Datenpanne bereits auf tatbestandlicher Ebene aus.

II. (Rechts-) Folgen einer Datenpanne

Die Folgen einer Datenpanne können Anwaltskanzleien sehr weitreichend auf rechtlicher, aber auch auf wirtschaftlicher Ebene treffen.

Auf rechtlicher Ebene kann zunächst seitens der örtlich und sachlich zuständigen Aufsichtsbehörde nahezu der gesamte Maßnahmenkatalog an Untersuchungs- und Abhilfebefugnissen des Art. 58 Abs. 1, 2 DSGVO durchgesetzt werden.

Streitig ist hierbei jedoch die rechtliche Würdigung des aus § 29 Abs. 3 BDSG[8] folgenden Spannungsverhältnisses zwischen der effektiven Durchsetzung der Datenschutzaufsicht einerseits und der Wahrung des Berufsgeheimnisses andererseits.[9] Diese Regelung wurde auf Grundlage der Öffnungsklausel des Art. 90 Abs. 1 S. 1 DSGVO durch den nationalen Gesetzgeber eingeführt und untersagt den Aufsichtsbehörden, die Untersuchungsbefugnisse aus Art. 58 Abs. 1 lit. e), f) DSGVO gegenüber Berufsgeheimnisträgern einschließlich derer Beschäftigten und Auftragsverarbeitern auszuüben, soweit dies zu einer Verletzung der standesrechtlichen Geheimhaltungs- und Verschwiegenheitspflichten[10] führen würde. Nach

---

7 s. Sieling, Vortrag Datenpannen, Folie 11, Beispiel Nr. 8.

8 Hingewiesen sei darauf, dass sich der Verweis in § 29 Abs. 3 S. 1 BDSG auf den Wortlaut des § 203 StGB-aF. bezieht, welcher durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen v. 09.11.2017 geändert wurde.

9 s. u.a. Herbst in Kühling/Buchner, DS-GVO BDSG, § 29 Rn. 28.

10 Die standesrechtliche Verschwiegenheitspflicht der Anwaltschaft ergibt sich aus § 43a Abs. 2

einer Ansicht wird vertreten, dass die Ausnahme aufgrund einer zu weitreichenden Privilegierung der genannten Geheimnisträger, die letztlich dazu führe, dass sich dieser Personenkreis einer datenschutzaufsichtsbehördlichen Kontrolle entziehen könne[11], verfassungs- und unionsrechtswidrig sei.[12] Jene Vertreter, die überwiegend dem Lager der Leiter der Aufsichtsbehörden der Länder entstammen[13], verkennen jedoch einerseits, dass den Aufsichtsbehörden ausschließlich die Ausübung der beiden genannten Befugnisse untersagt wird, soweit deren Ausübung zu einer Verletzung der Geheimhaltungspflichten führen würde. Es handelt sich somit um eine Beschneidung weniger Befugnisse mit einem engen Anwendungsbereich. Andererseits wird die verfassungsrechtliche Dimension der Geheimhaltungspflicht der Berufsgeheimnisträger verkannt, welche das besondere Vertrauensverhältnis zwischen Berufsgeheimnisträger und Mandant vor staatlicher Einflussnahme schützt.[14] Nach anderer Ansicht überwiege im Rahmen einer Abwägung aufgrund des verfassungsrechtlich besonders geschützten Ranges der standesrechtlichen Verschwiegenheitspflicht die Wahrung des Berufsgeheimnisses, sodass die Regelung des § 29 Abs. 3 BDSG weder verfassungs- noch unionsrechtswidrig sei.[15] Aufgrund der hohen verfassungsrechtlichen Bedeutung des Berufsgeheimnisses sowie dem Umstand, dass die aufsichtsbehördlichen Untersuchungsbefugnisse nur in einem überschaubaren Umfang eingeschränkt werden, ist es vorzugswürdig, das Spannungsverhältnis zugunsten des anwaltlichen Berufsgeheimnisses aufzulösen. Mithin überzeugt die erstgenannte Ansicht nicht.

Weiterhin möglich ist die Verhängung von Bußgeldern gegen die Verantwortlichen gem. Art. 83 Abs. 5 lit. a) DSGVO wegen einer Verletzung der Grundsätze der Datenverarbeitung aus Art. 5 Abs. 1 DSGVO. Zudem trifft den Verantwortlichen im Falle einer Datenpanne eine zivilrechtliche Schadensersatzpflicht nach Art. 82 Abs. 1 DSGVO. Die Sanktionierung einer Datenschutzverletzung durch einen Berufsgeheimnisträger oder einer ihm gleichgestellten Person i.S.d. § 203 Abs. 1, 4 StGB kann sich letztlich bis in den strafrechtlich relevanten Bereich auf eine Strafbarkeit gem. § 42 Abs. 1 BDSG sowie § 203 Abs. 1 Nr. 3 StGB erstrecken.

BRAO, konkretisiert durch § 2 Abs. 1, 2 S. 1 BORA.

11 Eßer in Auernhammer DSGVO/BDSG, § 29 Rn. 29.

12 Kugelmann in HK DS-GVO/BDSG, § 29 Rn. 67, 70; Herbst in Kühling/Buchner, DS-GVO BDSG, § 29 Rn.28; Wiechert, DANA 2018, 76, 79; Wiechert, DuD 2017, 538, 543; Weichert/Spaeing/Hülsmann, StN DVD BDSG-RegE, S. 12.

13 Prof. Dr. Dieter Kugelmann ist LfDI RLP, Dr. Stefan Brink ist LfDI BW.

14 BVerfG, Beschl. v. 12.04.2005, Az. 2 BvR 1027/02, Rn. 94, 95; BT-Drs. 18/11325, S. 101.

15 s. hierzu u.a. Gräber/Nolden in Paal/Pauly, DS-GVO BDSG, § 29 Rn. 19; ebenso Gräger in Plath, DSGVO/BDSG, § 29 Rn. 15; ebenso Lapp in Gola/Heckmann, BDSG, § 29 Rn. 26.

Neben den rechtlichen Folgen einer Datenschutzverletzung ist stets zu beachten, dass die Datenpanne sich auch in direkter wirtschaftlicher Hinsicht negativ auswirken kann. Wegen des besonderen Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant kann es insbesondere zu einer Störung bzw. einem Verlust des Vertrauens seitens des Mandanten kommen, der zu einer Kündigung des Mandatsverhältnisses führt. Hiermit wäre eine Umsatzeinbuße verbunden. Ferner kann es bereits durch die Datenpanne selbst, aber auch durch eine fehlende Transparenz hinsichtlich des Auftretens einer Datenpanne zu einer Reputationseinbuße bzw. gar zu einem Reputationsverlust kommen, welche sich ebenfalls – bedingt durch ausbleibende Mandatierungen - negativ auf die Finanzen der Kanzlei auswirken können.[16]

C. Datenpannenmanagement

I. Vom richtigen Umgang mit Datenpannen – Melde- & Dokumentationspflichten

Zu untersuchen ist sodann, welche Pflichten sich hinsichtlich der Behandlung von Datenschutzverletzungen aus der DSGVO ergeben und wie diese Datenpannen möglichst verhindert werden können.

1. Dokumentationspflicht gem. Art. 33 Abs. 5 DSGVO

Eine Dokumentationspflicht bzgl. aller Datenschutzverletzungen, unabhängig davon, ob diese meldepflichtig sind, ergibt sich aus Art. 33 Abs. 5 DSGVO. Hierbei handelt es sich um eine Konkretisierung des allgemeinen Grundsatzes der Rechenschaftspflicht aus Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO welche das Ziel verfolgt, den Aufsichtsbehörden eine Überprüfung, ob die Vorgaben des Art. 33 DSGVO eingehalten wurden, zu ermöglichen. Ferner dient sie der Bestimmung, ob die Ergreifung weiterer Maßnahmen erforderlich ist.

Formale Anforderungen werden an die Dokumentation nicht gestellt, sodass auch eine elektronische Dokumentation statthaft ist.[17] Inhaltlich erstreckt sich die Dokumentationspflicht auf die Mindestangaben aus Art. 33 Abs. 3 DSGVO mit Ausnahme der Kontaktdaten des Datenschutzbeauftragten. Nicht überzeugend erscheint es hingegen, den Inhalt der Risikoprognose über die Meldepflichtigkeit einer Datenpanne in die Dokumentationspflicht miteinzubeziehen[18], hierzu besteht bereits dem

[16] So auch Sieling, Vortrag Datenpannen, Folie 9.

[17] Laue in Laue/Kremer, DSR betr. Praxis, § 7 Rn. 53.

[18] so gefordert von Jandt in Kühling/Buchner, DS-GVO BDSG, Art. 33 Rn. 26; zutr. a.A. neben vielen weiteren Reif in Gola, DS-GVO, Art. 33 Rn. 40; Grages in Plath, DSGVO/BDSG, Art. 33 Rn. 17.

Wortlaut nach keine rechtliche Verpflichtung. Im Sinne einer Absicherung der eigenen Entscheidung wird jedoch seitens des Europäischen Datenschutzausschusses (EDSA) empfohlen, der Dokumentation eine Begründung über die Verneinung der Meldepflichtigkeit beizufügen.[19]

Eine Dokumentation ist – um die Kontrolle der Einhaltung der Meldepflichten seitens der Aufsichtsbehörden zu ermöglichen - fortzuführen, auch wenn sich die Annahme einer Datenpanne im laufenden Prüfungsverfahren nicht bewahrheitet. Eine Verpflichtung des Verantwortlichen, der Aufsichtsbehörde die Dokumentation unaufgefordert zu übermitteln, ist jedoch nicht aus Art. 33 Abs. 5 DSGVO abzuleiten.[20] Dies ergibt sich aus einem Umkehrschluss aus Art. 58 Abs. 1 lit. a), e) DSGVO, wonach die Aufsichtsbehörde den Verantwortlichen anweist, ihr die Daten zur Verfügung zu stellen. Hinsichtlich Berufsgeheimnisträgern gilt es, die vorab näher beschriebenen Einschränkungen aus § 29 Abs. 3 BDSG zu wahren.

2. Meldepflicht gem. Art. 33 Abs. 1 DSGVO

Bei Vorliegen einer Datenschutzverletzung ist die in Art. 33 Abs. 1 DSGVO normierte Meldepflicht von zentraler Bedeutung. Hiernach ist der Verantwortliche grundsätzlich dazu verpflichtet, der nach Art. 55 DSGVO zuständigen Aufsichtsbehörde diese Datenpanne unverzüglich zu melden.

Mit einer Datenschutzverletzung gehen nicht nur die vorab beschriebenen Risiken für die datenverarbeitende Kanzlei einher - vielmehr kann eine Datenpanne auch zu einem Schaden physischer, materieller oder immaterieller Art[21] auf Seiten des betroffenen Mandanten führen. Intention des Gesetzgebers war es, mithilfe der Meldepflicht einen transparenten Umgang mit Datenpannen seitens der Verarbeiter herbeizuführen, sodass die Aufsichtsbehörde auf fundierter Tatsachengrundlage entscheiden und ggf. weitere erforderliche Maßnahmen veranlassen kann. Weiterhin werden die Verantwortlichen durch die Meldepflicht veranlasst, zeitnah auf Datenschutzverletzungen zu reagieren. Hierdurch sollen Folgeschäden auf Seiten der Betroffenen möglichst verhindert, zumindest aber minimiert werden können.[22]

Das Entstehen der grundsätzlichen Meldepflicht setzt das Vorliegen einer Datenpanne i.S.d. Art. 4 Nr. 12 DSGVO sowie die Kenntnisnahme des Verantwortlichen

---

19 Artikel-29-Datenschutzgruppe, WP 250, S. 32.

20 So auch Martini in Paal/Pauly, DS-GVO BDSG, Art. 33 Rn. 54, 58a.

21 Vgl. Erwägungsgrund 85; ebenso Sieling, Vortrag Datenpannen, Folie 15.

22 Hladjk in Ehmann/Selmayr, DS-GVO, Art. 33 Rn. 2; ebenso Schultze-Melling in Taeger/Gabel, DS-GVO – BDSG – TTDSG, Art. 33 Rn. 3; Laue in Spindler/Schuster, Recht d. elektr. Medien, Art. 33 Rn. 4.

hierüber voraus. Wann eine Datenpanne vorliegt, richtet sich nach den vorab unter B. beschriebenen Kriterien.

a) Ausnahmen von der Meldepflicht

Eine uneingeschränkte Meldepflicht für Datenpannen besteht indes nicht. Nach dem risikobasierten Ansatz der DSGVO[23] besteht die zuvor genannte Meldepflicht nicht, wenn die konkrete Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt, vgl. Art. 33 Abs. 1 S. 1 DSGVO. Ob ein solches Risiko besteht, bedarf einer umfassenden Analyse bzw. Prognose im Einzelfall. Im Rahmen der Risikoprognose ist somit zu ermitteln, welche Folgen möglicherweise durch die konkrete Datenschutzverletzung eintreten können und wie hoch die Wahrscheinlichkeit dafür ist, dass die Folge tatsächlich eintritt. Die Risikoevaluierung setzt sich somit zusammen aus der Evaluierung der Schwere des möglichen Schadens sowie dessen Eintrittswahrscheinlichkeit.[24] Da bei Vorliegen einer Datenschutzverletzung ein Risiko für die Rechte und Freiheiten Betroffener niemals gänzlich auszuschließen ist, ist die Formulierung „[…] nicht zu einem Risiko […]" dem Telos des Art. 33 Abs. 1 S. 1 DSGVO nach, namentlich der Minimierung bzw. gar Verhinderung von aus der Datenpanne resultierender Folgeschäden auf Seiten des Betroffenen sowie die Schaffung eines Mindestmaßes an Transparenz, dahingehend auszulegen, dass es sich um ein geringes bzw. geringfügiges Risiko handeln muss. Somit wird in der DSGVO zwischen den Risikostufen „geringes Risiko", „Risiko" sowie „hohes Risiko" differenziert.[25] Drohende Schäden, die aus einer Datenschutzverletzung resultieren können, sind hierbei gem. EG 85 insbesondere Diskriminierungen, Identitätsdiebstahl und Identitätsbetrug, aber auch ein Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen. Betrachtet man eingangs genannte Fallbeispiele, so stellt sich die Frage des Ausgangs einer Risikoprognose für den Fall des Verlustes eines verschlüsselten Datenträgers eines Rechtsanwalts (Bsp.: Diebstahl eines Smartphones / Notebooks auf der Bahnreise zum auswärtigen Gerichtstermin), auf dem fallrelevante personenbezogene Daten gespeichert sind. Sofern die Verschlüsselung auf dem aktuellen Stand der Technik erfolgt, läge zwar objektiv eine Datenschutzverletzung in Form eines Verlusts von Daten vor. Durch die Verschlüsselung auf dem aktuellen Stand der Technik wäre es einem Dritten

---

23 Martini in Paal/Pauly, DS-GVO/BDSG, Art. 33 Rn. 21; Brink in BeckOK DSR, Art. 33 Rn. 34.

24 vgl. DSK, Kurzpapier Nr. 18, S. 5 „Risikomatrix".

25 Paal, Meldepflicht DSV, ZD 2020, 119, 121; Brink in BeckOK-DSR, Art. 33 Rn. 35; Schultze-Melling in Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 33 Rn. 22; DSK, Kurzpapier Nr. 18, S. 5 „Risikomatrix".

allerdings nicht möglich, diese verschlüsselten Daten einzusehen. Demnach ist die Schwere des möglichen Schadens als überschaubar im Sinne der DSK-Risikomatrix anzusehen, die Eintrittswahrscheinlichkeit hingegen wäre vorliegend als geringfügig einzustufen. Mithin wäre ein geringes Risiko gegeben, sodass der Ausnahmetatbestand greifen und die Meldepflichtigkeit entfallen würde.

Die Beurteilung, ob ein (hohes) Risiko gegeben ist oder ob lediglich ein geringes Risiko besteht, obliegt dem Verantwortlichen. Aufgrund des Umstands, dass der Aufsichtsbehörde nach Art. 58 Abs. 1 lit. a) DSGVO ein Recht auf Überprüfung zusteht, empfiehlt es sich einerseits, die Beurteilung sorgfältig und gewissenhaft durchzuführen. Andererseits sollte der Verantwortliche die Risikoprognose schriftlich fixieren, um diese im Fall einer aufsichtsbehördlichen Kontrolle dem Grundsatz der Rechenschaft aus Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO entsprechend nachweisen zu können.

b) Inhalt, Form und Frist der Meldung

Die Mindestangaben der Meldung richten sich nach Art. 33 Abs. 3 DSGVO. Hiernach ist zunächst eine möglichst detaillierte Beschreibung der Art der Verletzung unter Angabe der Ursache und Kategorien der betroffenen Daten erforderlich. Sodann sind gem. Art. 33 Abs. 3 lit. b) DSGVO die Kontaktdaten des Datenschutzbeauftragten anzugeben. Weiterhin sind die wahrscheinlichen Folgen der Datenpanne für den Betroffenen sowie die vom Verantwortlichen ergriffenen Abhilfemaßnahmen anzugeben. Eine bestimmte Form ist für die Meldung einer Datenschutzverletzung an die zuständige Aufsichtsbehörde nicht vorgesehen, sodass auch hier eine elektronische Übermittlung statthaft ist.[26] Um eine möglichst zeitnahe, fristgemäße Meldung zu ermöglichen, halten die Aufsichtsbehörden hierzu Webformulare bereit.[27]

Dem Wortlaut des Art. 33 Abs. 1 S. 1 DSGVO nach entsteht die Meldefrist im Zeitpunkt der Kenntnisnahme des Verantwortlichen von der Datenschutzverletzung. Eine sichere Kenntnis von einer Datenpanne wird hierbei nach vorzugswürdiger überwiegender Ansicht nicht vorausgesetzt, ausreichend sei eine hinreichende Wahrscheinlichkeit einer Datenschutzverletzung.[28] Somit muss eine hinreichende

---

26 Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 33 Rn. 21.

27 Übersicht der Webformulare mit Links s. Peintinger in BeckOF IT-D-Recht, Formular 2.4, Anm. 1.

28 Martini in Paal/Pauly, DS-GVO, Art.33 Rn. 18; Schreibauer in Auernhammer, DSGVO/BDSG, Art. 33 Rn. 13; Art 29 Gruppe, WP 250; Grages in Plath, DSGVO/BDSG, Art. 33 Rn. 3; Paal, ZD 2020, 119, 121.

Tatsachengrundlage bestehen, der Verantwortliche muss die Datenschutzverletzung hingegen nicht unmittelbar als solche rechtlich einordnen können. Den Verantwortlichen trifft eine Ermittlungspflicht, er muss somit die maßgeblichen, fallrelevanten Umstände aufklären. Als Folge dessen ist gem. Art. 33 Abs. 4 DSGVO eine schrittweise Bereitstellung der Informationen statthaft, sofern nicht alle melderelevanten Informationen zeitgleich zur Verfügung gestellt werden können. Entzieht sich der Verantwortliche allerdings durch bewusste Untätigkeit der Kenntnisnahme einer möglichen Datenschutzverletzung mit dem Ziel, die Entstehung einer Meldepflicht zu verhindern, so erfolgt eine Fiktion der Kenntnisnahme.[29] In diesem Fall ist der Verantwortliche so zu stellen, als hätte dieser die Umstände zur Kenntnis genommen. Von einer solchen bewussten Verweigerung der Kenntnisnahme ist am Beispiel von kritischen Schwachstellen wie zuletzt „Log4j"[30] insbesondere dann auszugehen, wenn der Verantwortliche – obwohl über einschlägige Fachmedien hinaus bereits über die entsprechende Schwachstelle berichtet und gewarnt wird – schlicht untätig bleibt.

Das Kriterium der Unverzüglichkeit[31] sowie die Berechnung der 72-Stunden-Frist[32] werden in der DSGVO nicht näher konkretisiert. Mangels eines Verweises auf das jeweils einschlägige nationale Recht der Mitgliedsstaaten, welcher dem Harmonisierungsbestreben des europäischen Datenschutzrechts zuwiderlaufen würde, sind diese nach überwiegender Ansicht unionsrechtskonform auszulegen.

3. Meldepflicht des Auftragsverarbeiters gem. Art. 33 Abs. 2 DSGVO

Regelmäßig in kanzleiinterne Datenverarbeitungen eingebunden werden Auftragsverarbeiter, welche z.B. die technische Infrastruktur für Videokonferenzdienste, Clouds oder Dienste zur elektronischen Aktenverwaltung bereitstellen. Die Meldepflicht eines Auftragsverarbeiters, der von einer Datenpanne Kenntnis erlangt, ergibt sich aus Art. 33 Abs. 2 DSGVO und besteht gegenüber dem Verantwortlichen, nicht hingegen gegenüber der Aufsichtsbehörde.

---

29 Martini in Paal/Pauly, DS-GVO BDSG, Art. 33 Rn. 19.

30 S. hierzu die Berichterstattung über die Schwachstelle „Log4j". Neben u.a. dem BSI und Heise Security warnten auch die Tagesschau (Ursprungsmeldung s. https://www.tagesschau.de/inland/bsi-schadsoftware-101.html) sowie diverse Tageszeitungen (s. u.a. https://www.sueddeutsche.de/wirtschaft/bsi-bedrohungslage-warnstufe-log4j-1.5485806) mit einer geringen zeitlichen Differenz zu den Fachmedien vor dieser gravierenden Schwachstelle.

31 U.a. Marschall, DuD 2015, 183, 186; Schreibauer in Auernhammer, DSGVO/BDSG, Art. 33 Rn. 13; Piltz/Pradel, ZD 2019, 152, 156.

32 DSG, WP 250 rev0.1, S. 15, Fn. 24; Schreibauer in Auernhammer, DSGVO/BDSG, Art. 33 Rn. 12.

II. Sanktionen

Verstöße gegen vorgenannte Dokumentations- und Meldepflichten stellen gem. Art. 83 Abs. 4 lit. a) DSGVO bußgeldbewehrte Verstöße des Verantwortlichen bzw. des Auftragsverarbeiters dar, welche mit einem Bußgeld von bis zu 10 Millionen Euro oder 2% des globalen auditierten Vorjahresumsatzes geahndet werden können.

Während §§ 42 Abs. 4, 43 Abs. 4 BDSG die Verwendung von Datenpannenmeldungen gegen den Verantwortlichen in einem Straf- oder Bußgeldverfahren unter den Vorbehalt der Zustimmung desselben stellen, fehlt es in der DSGVO an einer solchen Regelung. Aus dem nemo-tenetur-Grundsatz aus Art. 2 Abs. 1, 1 Abs. 1, 20 Abs. 3 GG sowie aus dem in Art. 6 EMRK kodifizierten Fair-Trial-Grundsatz folgt jedoch, dass eine solche Regelung in Art. 83 Abs. 4 DSGVO hineinzulesen ist.[33]

III. Präventives Management – eine lohnende Investition?

Wie vorangehend beschrieben sind in der konkreten Krisensituation zahlreiche rechtliche Vorgaben zu beachten, deren Nichtbefolgung für die Verantwortlichen der Kanzlei weitreichende Konsequenzen zur Folge haben kann. Somit empfiehlt es sich einerseits, die technischen und organisatorischen Maßnahmen regelmäßig zu evaluieren und ggf. anzupassen, andererseits sollten auch die Zuständigkeiten und die wesentlichen Reaktionsschritte der Entscheidungsträger vorab in Form eines Krisenreaktionsplans definiert werden.

Im Rahmen der Festlegung geeigneter technischer und organisatorischer Maßnahmen i.S.d. Art. 32 Abs. 1 DSGVO gilt es auf technischer Ebene insb. Systeme zu etablieren, durch die eine Datenpanne vermieden, zumindest aber eine Datenpannenmeldung obsolet gemacht werden kann. Hierzu zählen – je nach Sensibilität der Daten – ein engmaschiges Monitoring der Systeme, geeignete Zugriffs- und Rechtekonzepte, der Einsatz geeigneter Antivirensoftware, zuverlässige Alert-Systeme, der Einsatz einer Verschlüsselung sowie regelmäßige, externe Backups. Es wäre jedoch verfehlt, im Rahmen der Prävention allein auf technische Maßnahmen zu setzen, stellen doch die Beschäftigten die größte Schwachstelle im Hinblick auf die IT-Sicherheit einer Kanzlei dar.[34] Auf organisatorischer Ebene gilt es somit, IT-Richtlinien für die Mitarbeiter aufzustellen und diese allgemein zugänglich zu machen. Die Richtlinien sollten fortlaufend aktualisiert und über verpflichtende, regelmäßig stattfindende Schulungen präsent gemacht werden, um die Awareness bzw.

---

33 Zum selben Ergebnis bei vergleichbarer Argumentation kommen Wilhelm in Sydow, EU-DSGVO, Art. 33 Rn. 29; Martini in Paal/Pauly, DSGVO/BDSG, Art. 33 Rn. 27; Dix in Simitis/Hornung/Spiecker, DSR, Art. 33 Rn. 25; DSGVO, EG 148 S. 2.

34 Diercks, ZdiW 2021, 27, 27; Kuhrau, ZdiW 2021, 23, 24.

das allgemeine Problembewusstsein im Bereich der IT-Sicherheit zu stärken. Im Rahmen der Schulungen sollte auf einen standardisierten Meldeweg für vermutete Sicherheitsvorfälle hingewiesen und hierbei betont werden, dass eine schnelle Meldung durch die Beschäftigten den Eintritt eines größeren Schadens verhindern kann. Insoweit ist der Referentin zuzustimmen, dass die Etablierung einer Heldenkultur hinsichtlich Verdachts- und Schadensmeldungen förderlich ist und den Beschäftigten aus einer Meldung einer Datenschutzverletzung keine arbeitsrechtlichen Nachteile erwachsen sollten.[35] Weiterhin empfiehlt es sich auf organisatorischer Ebene, die wesentlichen Reaktionsschritte und Zuständigkeiten der Beteiligten für den Fall des Eintritts einer Datenschutzverletzung vorab in Form eines Krisenreaktionsplans zu definieren. Dieser Plan ist in die vier Schritte „Zuständigkeiten, Verantwortlichkeiten und Meldewege", „Schadensanalyse und -eingrenzung", „rechtliche Bewertung des Vorfalls" sowie „Kommunikation intern / extern" zu unterteilen.[36]

D. Fazit

Zusammenfassend ist festzuhalten, dass mit einer Datenpanne umfangreiche Melde- und Dokumentationspflichten sowie nicht zu unterschätzende Bußgeldrisiken und Reputationseinbußen einhergehen können. Es gilt mithin, die Gefahr des Eintritts einer Datenschutzverletzung zu minimieren, was sich insb. durch geeignete technische und organisatorische Maßnahmen realisieren lässt. Aufgrund des Umstandes, dass die Beschäftigten die größte Schwachstelle in der IT-Sicherheit der Kanzlei darstellen, ist der Fokus durch Schulungen und Sensibilisierungsmaßnahmen auf die Mitarbeiter-Awareness zu datensicherheitsrechtlichen Themen zu legen, wenngleich die technischen Maßnahmen nicht vernachlässigt werden dürfen. Für den Fall, dass es entgegen aller Bemühungen in der Kanzlei zu einer Datenpanne kommt, erleichtert ein vorab erarbeiteter Krisenreaktionsplan mit fest definierten Zuständigkeiten und Abläufen die Dokumentation und Kooperation mit den Behörden ungemein. Somit empfiehlt es sich insgesamt, vorgenannte Präventionsmaßnahmen – sofern noch nicht (vollständig) geschehen – zeitnah umzusetzen. Bedingt durch die nicht unerheblichen Bußgeldrisiken und drohenden Schadensersatzforderungen der potenziell Betroffenen, welche die Kosten für vorgenannte Maßnahmen um ein Vielfaches übersteigen können, stellt die frühzeitige Implementierung vorgenannter Vorsorgemaßnahmen eine lohnende Investition dar.

35 Sieling, Vortrag Datenpannen, Folie 23.
36 Ebenso Wybitul, NJW 2020, 2577, 2581.