Rechtsanwalt Dr. Arnd-Christian Kulow, Stuttgart

Informationspflichten nach Art. 13 Datenschutz-Grundverordnung (DSGVO) in der Anwaltskanzlei

RA Dr. Arnd-Christian Kulow –
Stand: August 2018

Die DSGVO geizt nicht mit Pflichten für die Verantwortlichen. Dazu gehört auch die Verpflichtung, aus Art. 13 bzw. 14 DSGVO bei der „Erhebung" personenbezogener Daten die jeweiligen Betroffenen zu informieren.

Kanzleien verpflichtet dies mindestens zur Erstellung einer „Datenschutzerklärung" für die Kanzleihomepage, zum anderen zur Information neuer Mandanten über die beabsichtigten Verarbeitungen im Rahmen der Mandatsbearbeitung. Es stellen sich aber tatsächlich noch weitergehende Fragen: Muss auch der Gegnervertreter „informiert" werden? Wie ist es mit Korrespondenzanwälten? Mit Sachverständigen? Reicht die einmalige Information oder muss diese vielleicht wiederholt gegeben werden?

Viele der ganz konkreten Fragen rund um die Informationspflichten sind offen. Daher kann hier nur eine erste Konturierung des Themas vorgeschlagen werden. Diese soll in erster Linie einen „lebbaren", robusten und effizienten Datenschutz in der Kanzlei beschreiben.

Die Informationspflichten sind zunächst von den Rechtsmäßigkeitsbedingungen der Verarbeitung von personenbezogenen Daten (pbD) nach Art. 6 Abs. 1 DSGVO zu trennen. Die Informationspflichten knüpfen an den Verarbeitungsvorgang des „Erhebens" von pbD an. Dieses „Erheben" kann einmal beim Betroffenen selbst erfolgen (Art. 13 DSGVO) und zum anderen nicht beim Betroffenen, also z.B. bei bzw. über Dritte(n) (Art. 14 DSGVO).

Das „Wie" der Erfüllung der Informationspflichten regelt dabei der sehr unübersichtliche Art. 12 DSGVO. Dabei soll die Information in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden (Art. 12 Abs. 1 Satz 1 DSGVO). Die in dieser Formulierung angelegten Zielkonflikte sind augenscheinlich. Bei der Formulierung sollte daher auf den Sprachgebrauch der jeweiligen Mandantschaft und den generellen Sprachstil der Kanzlei abgestellt werden.

Da schon der Begriff des „Erhebens" von personenbezogenen Daten nicht in der DSGVO definiert ist, fangen hier gleich die Auslegungsprobleme an. Die Aufgabe besteht zunächst einmal darin festzustellen, „wann" überhaupt „wer" zu informieren ist. Solange keinerlei belastbare Vorgaben von Behörden oder gar Rechtsprechung verfügbar sind, wird man sich hier wohl zunächst eine eigene Meinung bilden müssen.[1] In diesem Sinn soll diese kleine Darstellung diese Meinungsbildung bei den Kollegen und Kolleginnen unterstützen. Eine Diskussion der hier vorgeschlagenen Sichtweise ist daher sehr erwünscht und dient der Fortschreibung dieses Papiers.

Zunächst soll kurz unter A. die gesetzgeberische Intention bezüglich der Art. 13, 14 DSGVO skizziert werden. Danach wird unter B. die besondere Verarbeitungssituation in der Anwaltskanzlei angesprochen, unter C. die inhaltlichen Fragestellungen dargelegt und unter D. kurz auf die möglichen Sanktionen im Falle einer Pflichtverletzung eingegangen. Abschließend werden unter E. konkrete Vorschläge zur praktischen Umsetzung anhand zweier kommentierter Checklisten gemacht.

1 So ausdrücklich auch Moos/Schefzig in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, 2018, S. 5 (Praxishinweis).

A. Gesetzgeberische Intention der Informationspflichten

Die Informationspflichten dienen der Gewährleistung einer fairen und transparenten Verarbeitung personenbezogener Daten (Art. 13 Abs. 2 DSGVO).

Hierzu unterscheidet die DSGVO grundsätzlich zwei Sachverhalte: die Erhebung der Daten beim Betroffenen (Art. 13 DSGVO) und den Sachverhalt, dass die Daten nicht bei der betroffenen Person erhoben werden (Art. 14 DSGVO). Beide Sachverhalte kommen in der Kanzlei vor. Auf das Thema der „Zweckänderung" (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO) wird hier nicht eingegangen.

Die Informationspflicht soll dabei bei jeder Erhebung bestehen, lediglich wenn und soweit der Betroffene bereits über die betreffende Information verfügt, besteht die Pflicht nicht mehr (Art. 13 Abs. 4, Art. 14 Abs. 5 DSGVO). Damit wird der Begriff des „Erhebens" zentral bedeutsam.

B. „Erheben" von personenbezogenen Daten vs. „Übermitteln" bzw. „Zufluss" von personenbezogenen Daten

I. Erheben

Der Begriff des „Erhebens" ist in der DSGVO nicht näher definiert, wird also nur von Art. 4 Nr. 2 DSGVO als Beispiel einer Verarbeitung genannt. Gleichwohl erwähnt die DSGVO bzw. das BDSG den Begriff an verschiedenen Stellen. Dabei wird das Erheben der Daten wenig überraschend als Beginn des Verarbeitungsprozesses zu einem bestimmten Zweck gesehen[2] (z. B. Art. 5 Abs. 1 lit. b), Erwägungsgrund 39 Satz 6 („Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen."). Das Erheben ist damit der zielgerichtete Zugriff auf personenbezogene Daten[3] zu einem vorher bestimmten Zweck.

II. Bei der betroffenen Person

Diese Erhebung muss „bei der betroffenen Person" stattfinden. Hier gehen die Meinungen schon stark auseinander. Die eine Meinung[4] fordert das aktive und bewusste Mitwirken des Betroffenen[5], andere hingegen halten es für „irrelevant, ob die betroffene Person aktiv an der Datenerhebung mitwirkt, sich ihr entziehen kann oder auch nur von ihr weiß."[6]

Folgt man der ersten Meinung, so ist der Kreis der nach Art. 13 DSGVO zu Informierenden sehr eingeschränkt. Die Erfassung von Daten auf einer Website des Betroffenen wäre dann keine Erhebung beim Betroffenen, sondern eine Erhebung nach Art. 14 DSGVO. Dieser – das sei an dieser Stelle schon gleich gesagt – schließt in seinem Abs. 5 lit. d) die Informationspflicht aus, wenn die pbD nach dem Recht des Mitgliedstaats dem Berufsgeheimnis unterfallen und daher vertraulich zu behandeln sind.

Folgt man der zweiten Meinung, die eher auf die Sphäre aus der die Information stammt abstellt, vergrößert sich der Kreis der zu Informierenden.

III. Übermittlung, Zufluss

Informationen, die der Verantwortliche nicht durch ein „Erheben" erhält, unterliegen folglich nicht den Informationspflichten der Art. 13, 14 DSGVO. Sie fließen dem Verantwortlichen vielmehr zu bzw. werden ihm „übermittelt". Der Übermittlungsbegriff beschreibt somit auch die zur Erhebung komplementäre Verarbeitung. Dieser Begriff ist ebenfalls nicht näher definiert und wird lediglich in Art. 4 Nr. 2 DSGVO als Beispiel einer Verarbeitung aufgeführt.

Es stellt sich damit die Frage, wo in der Kanzlei in diesem Sinn pbD „erhoben" werden und wo und wie folglich zu informieren ist und wann und wo – dazu komplementär – Daten der Kanzlei lediglich übermittelt werden bzw. dieser „zufließen". Da die DSGVO mit der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO die Vorstellung eines umfassenden Datenmanagements auf Seiten des Verantwortlichen hat, sind alle Verarbeitungen bzw. Verfahren der Kanzlei, bei denen pbD „hereinkommen", entsprechend abzuprüfen.

Dabei kommt zunächst - wenn vorhanden – die Kanzleihomepage in Betracht, sodann die Mandantendaten und Mitarbeiterdaten, die Daten der Kolleginnen und Kollegen in diversen Rollen, die gegnerische Partei selbst, die Sachverständigen und ggf. Weitere.

2 Paal/Pauly, DSGVO, 2. Aufl., 2018, Rz. 11 zu Art. 13.
3 Bäcker in: Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 12 zu Art. 13; Ingold in: Sydow (Hrsg.), DSGVO, 2. Aufl., 2018, Rz. 8: „das aktive und gezielte Beschaffen von Daten ...".
4 Ingold in: Sydow (Hrsg.), DSGVO, 2. Aufl., 2018, Rz. 8.
5 BeckOK DatenschutzR/Schmidt-Wudy, 24. Ed. 1.5.2018, DSGVO Art. 13 Rn. 30-32.
6 Vgl. nur Bäcker in: Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 13 zu Art. 13, m.w.N.

IV. Einzelfälle

1) „Erheben" von IP-Adressen auf der Kanzleihomepage

Die zum Funktionieren des Internet und des darauf basierenden World Wide Web erforderliche Adresse (IP-Adresse) wird überwiegend als personenbezogenes Datum angesehen. Diese IP-Adressen werden vom Server aktiv ausgelesen und gespeichert und somit nach der o. a. Definition „erhoben". Damit ist eine entsprechende Information nach Art. 13 bzw. Art. 14 DSGVO als „Datenschutzerklärung" auf der Kanzleihomepage vorzuhalten. Sie folgt dem Aufbau von Art. 13 DSGVO.

Weitere Verarbeitungen der Daten auf der Homepage durch Dienstleister, die diese IP-Adressen auswerten, um mehr über das Verhalten der Website-Besucher zu erfahren (Tracking-Tools) oder der „Einbau" von Dienstleistungen Dritter (Plugins) wie etwa Google Maps, erfordern weitergehende Informationen, dazu unten mehr.

Bezüglich der Informationspflichten über die Erhebung und Weiterverarbeitung von IP-Adressen auf und durch die Kanzleihomepage sind derzeit viele Fragen offen. Platt formuliert bedeutet dies Folgendes: Je mehr mit den IP-Adressen „angestellt" wird, desto komplexer und derzeit auch rechtlich labiler wird die „Datenschutzerklärung" zur Kanzlei-Website.

Für die Kanzleien stellt sich die Homepage in der Regel als „Visitenkarte im Web" dar. Dazu werden die Leistungen der Kanzlei und das Team vorgestellt. Zuweilen wird dies ergänzt durch Fachbeiträge oder ähnliche Zusammenstellungen. Für dieses „Normalangebot" einer Kanzlei reicht eine kurze Erklärung absolut aus. Im Grunde sind dazu auch keine Cookies notwendig. Wenn dann noch darauf geachtet wird, dass keine Schriften oder Ähnliches von Drittanbietern (wie z.B. Google Fonts) in die Seite eingebunden wird, hat man einen auch rechtlich sehr robusten Auftritt, der jedenfalls insoweit (also abgesehen von entsprechenden inhaltlichen Aussagen) keinen Ansatzpunkt zur Abmahnung oder gar Bußgeldverhängung bietet. Von daher ist es fast schon tragisch, dass offenbar nicht wenige Kollegen und Kolleginnen ihre Websites abgeschaltet haben, obwohl es sich um im besten Sinne „normale" Seiten und damit unproblematische Seiten handelt.

In diesem Zusammenhang zeigt sich häufig ein weiteres Thema: Die Kanzleien haben in der Regel die Wartung und das Vorhalten der Website (Hosting) ausgelagert. Manchmal wissen die Verantwortlichen in der Kanzlei gar nicht so genau, was die Website „macht".

Hier ist ein Tätigwerden geboten. Es besteht eine Pflicht aus den Art. 5 Abs. 1 lit. d), 12 -2 2, 30, 32, 33, 40 Abs. 2 lit a) DSGVO (Transparenz der Verarbeitungen) sich zu informieren und sich notfalls vom Dienstleister erklären zu lassen, was die Website genau „macht", wie sie die IP-Adressen verarbeitet. Dabei zeigt sich unter Umständen, dass eine Website sehr viel mehr verarbeitet als vielleicht nötig ist. Dies sollte immer mit dem konkreten Nutzen abgewogen werden. Unter Umständen ist es tatsächlich derzeit besser, eher weniger Zusatzverarbeitungen und Auswertungen auf der Kanzleihomepage vorzunehmen, um einen rechtlich robusteren Auftritt zu erreichen.

So ist der beliebte „Dienst" Google Analytics derzeit zwar wohl (noch) datenschutzkonform auf einer Website zu betreiben (entsprechend umfangreiche Erklärungen und Belehrungen nebst Auftragsverarbeitungsvertrag eingeschlossen). Derweil gerät allerdings ein Element der Rechtmäßigkeit, nämlich der sogenannte „Privacy Shield", immer mehr unter Beschuss der EU, sodass hier die Entwicklungen fast täglich zu beobachten sind.

Im Folgenden wird kurz auf die verschiedenen Kategorien von Verarbeitungen von IP-Adressen über Websites eingegangen. Hierbei steht zunächst mal die „einfache" Website für die normale Nutzung im Vordergrund. Dann folgt das Thema der Newsletterbestellung über die Website, dann die sogenannten „Tracking"-Technologien mithilfe von Dritten oder letztlich die Einbindung von Dritten über sogenannte „Plugins".

a) „Normale" Nutzung

Die hierzu nach Art. 13 DSGVO jeweils abzugebenden Erklärungen sollten tatsächlich „abgearbeitet" werden und immer Bestandteil der Datenschutzerklärung der Website sein. Wenn nichts Weiteres „eingebaut" wird, bleibt es bei der entsprechenden Erklärung (vgl. Muster mit Erläuterungen).

Die Website dient nur der Darstellung des Leistungsangebots und der Bereitstellung der Kontaktdaten. Hier werden die zur Funktionsfähigkeit notwendigen Daten erhoben (Näheres unten).

WAS SIND COOKIES? >>

„Cookies" sind kleine Textdateien, die dem Besucher einer Webseite, von dieser automatisch auf den Browser übertragen werden. Der Verwender der Cookies kann die Speicherdauer auf dem Besucherrechner bestimmen. Diese können daher nach dem Besuch der Seite automatisch gelöscht werden (Session Cookies) oder über den Besuch hinaus auf dem Besucherrechner beliebig lange gespeichert bleiben (Tracking Cookies).

Da die IP-Adresse der meisten Besucher „dynamisch" ist, kann man Besucher der Seite daran nicht wiedererkennen. Die Tracking-Cookies dienen dazu, einen Besucher als solchen zu identifizieren und damit auch wiederzuerkennen (ohne das hier freilich der Name ohne Weiteres erkannt werden kann).

Es zeichnet sich ab, auch vor dem Hintergrund der kommenden E-Privacy Verordnung, dass die Session-Cookies regelmäßig nach Art. 6 Abs. 1 lit. f) DSGVO aufgrund des berechtigten, überwiegenden Interesses des Verwenders zulässig sind. Alle Arten von Tracking-Cookies, die also über die Zeitdauer des Seitenbesuchs hinaus gespeichert werden, sind dagegen einwilligungspflichtig.

Dieses „Opt-in", also die Einwilligung, wird in der Regel durch einen „Banner", – also einen Informationsstreifen, der bei Aufruf der Seite erscheint – belehrt und zur Bestätigung der Erlaubnis Tracking-Cookies einzusetzen auffordert, realisiert.

Eine Speicherung ist für kurze Zeit (zwei Wochen) aus Gründen der Angriffserkennung und -abwehr zulässig. „Cookies" werden nicht gebraucht. Schriften oder sonstige Software von Dritten werden im Idealfall nicht über das Web eingebunden, sondern auf dem eigenen Server abgelegt.

b) Newsletter

Manche Kanzleihomepages sehen die Anmeldung zu einem Newsletterversand vor. Die DSGVO erlaubt Direktwerbung grundsätzlich nach Art. 6 Abs. 1 lit. f) DSGVO und geht insofern zunächst von einem überwiegenden Interesse des werbenden Unternehmens aus. Nach § 7 Abs. 2 Nr. 3 UWG stellt allerdings der Versand eines Newsletters per Mail grundsätzlich eine unzumutbare Belästigung dar. Es bedarf zur Rechtmäßigkeit der Zusendung einer entsprechenden Einwilligung. Die Anforderungen an eine wirksame Einwilligung sind unionsrechtskonform zu bestimmen[7] und richten sich daher nach Art. 7 Abs. 1 DSGVO. Hierzu muss der Einwilligende über den Umstand des Newsletterversands informiert werden und freiwillig und aktiv seine Einwilligung dokumentierbar abgeben. Dies kann durch einen entsprechenden „Button" oder einen aktiv zu setzenden Haken im Webauftritt der Kanzlei realisiert werden.

Diese Maßnahmen alleine würden jedoch das Risiko nicht ausschließen, dass ein Dritter die E-Mail-Adresse des Anmelders missbraucht. Es ist daher eine neutrale, werbefreie Mail an den Anmelder zu schicken. Über einen Link o.Ä. bestätigt der Anmelder jetzt nachweisbar seine Einwilligung zum Empfang. Dieses Verfahren nennt man daher auch „Double-opt-in-Verfahren". Aus Gründen der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) ist nur die E-Mail-Adresse zu erheben. Alle anderen Angaben müssen freiwillig sein. Da die E-Mail-Adresse regelmäßig ein personenbezogenes Datum ist, muss die Webseite für eine verschlüsselte Übertragung der eingegebenen Adresse sorgen.

c) Webformulare zur Erfassung von Mandanten-, Bewerber- oder sonstigen personenbezogenen Daten

Hier ist ebenfalls auf alle Fälle eine Verschlüsselung der Website Pflicht (siehe Punkt 2 oben). Das Schutzziel der Vertraulichkeit aus Art. 5 Abs. 1 lit. f), 25 Abs. 2 und 32 Abs. 1 DSGVO verpflichtet die Kanzlei dazu, nachweisbar (Art. 5 Abs. 2 DSGVO) sicherzustellen, dass niemand außer den Berechtigten auf die unverschlüsselten Daten zugreifen kann.[8]

d) Sogenannte „Tracking Tools" wie z. B. Google Analytics

Um festzustellen, wie viele Interessenten sich welche Seiten ansehen, um also generell mehr über die Nutzer des Webauftrittes zu erfahren, kann man die notwendigerweise anfallenden IP-Adressen der Besucher weiter auswerten. Dies macht in der Regel nicht der Webdienstleister, sondern darauf spezialisierte Unternehmen wie z. B. Google. Diese bieten die Auswertungen als Dienst an. Dies ist auch unter der DSGVO nicht per se verboten. Der datenschutzkonforme Betrieb ist jedoch davon abhängig, dass mehrere Maßnahmen zum Schutz der natürlichen Personen, die hinter den IP-Adressen stehen, unternommen werden.

Wenn die Daten die EU verlassen, müssen sie zuvor durch Kürzung anonymisiert werden. Da die Kürzung der Daten in der Regel vom jeweiligen Dienstleister durchgeführt wird, ist allein schon deshalb mit ihm ein Vertrag über eine Auftragsverarbeitung zu schließen. Dieser ist – anders als nach früherem Datenschutzrecht – nicht mehr zwingend an die Schriftform gebunden.

Aufgrund von Abweichungen in der verwendeten Technik müssen die Erklärungen nach Art. 13 DSGVO für jeden verwendeten Tracking Dienst einzeln formuliert werden. Man sollte es sich daher gut überlegen, ob man überhaupt Trackingtools einsetzen will und was der konkrete Nutzen für das eigene Beratungsgeschäft ist.

e) Plugins und andere Drittanbieter (Facebook, Google Maps, Google Fonts etc.)

Nicht nur die sogenannten „Social Media", auch andere Anbieter stellen sogenannte „Plugins" für Webseiten bereit. Diese können vom Webseitenbetreiber häufig kostenlos in die Website eingebaut werden. Bei den Kanzleihomepages kommt hier sicherlich häufig Google Maps in Betracht, weil dadurch die Kanzlei geographisch rasch gefunden werden kann. Versteckt und daher häufig unbewusst ist vielen Verantwortlichen, dass z.B. auch Schriften, die die Website zur optisch anspruchsvollen Darstellung benötigt, nicht mehr auf dem Server der Kanzleihomepage liegen, sondern vom Benutzer bei der Anzeige der Seite von einem Drittanbieter – z. B. Google – heruntergeladen werden.

Bei all diesen Vorgängen wird die IP-Adresse des Webseitenbesuchers diesen Dritten übermittelt. Häufig in Drittstaaten. Diese

WAS IST UND WIE BEKOMME ICH EINE VERSCHLÜSSELTE WEBSITE? >>

Was ist eine verschlüsselte Website?

Voreingestellt werden die Daten im World Wide Web (häufig auch „Internet" genannt) nicht verschlüsselt übertragen. D.h. die Inhalte der in Datenpakete aufgeteilten Website-Inhalte sind lesbar, wie eine Postkarte. Durch die Verwendung einer Verschlüsselung, wird die Nachricht (also z. B. die in ein Formular eingegebenen personenbezogenen Daten) verschlüsselt übertragen und können somit nicht mehr von jedem, der Zugriff auf die Datenleitungen hat, gelesen werden. Man erkennt verschlüsselnde Websites an der Protokollbezeichnung „https://" in der Adresszeile des Browsers.

Wie bekomme ich so eine verschlüsselte Website?

Die meisten Website-Hoster bieten die Verschlüsselung als kostenpflichtigen Dienst an. Dies ist der einfachste Weg. Wer sich etwas näher mit der Materie befassen will, der kann über die Adresse https://letsencrypt.org/ Informationen darüber bekommen, wie man seine Website kostenlos verschlüsselt.

7 Ohly/Sosnitza, UWG, 7. Aufl., 2016, Rz. 66 zu § 7.
8 Zur Vertiefung: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Auflage, 2018, H. I. 7.

Dritten – wie z. B. Google – können dann diese IP-Adressen wiederum mit eigenen Datenbeständen abgleichen und zusammenführen.

Für den Webseitenbetreiber bleibt oft völlig unklar, wie die Daten weiterverarbeitet werden. Hier wurde teilweise eine datenschutzrechtliche Verantwortung des Betreibers grundsätzlich verneint. Durch die Facebook- Entscheidung des EuGH (C-210/16, v. 5.6.2018) ist deutlich geworden, dass hier durchaus eine Mitverantwortung in Betracht kommt. Wieweit diese im Einzelnen reicht, wird sich noch zeigen.

Google hatte schon Ende 2017 einen solchen Vertrag über eine gemeinsame Verantwortung bei der Nutzung von Google Maps zur Verfügung gestellt. Ob dieser sehr knappe Vertrag letztlich den Anforderungen des Art. 26 DSGVO gerecht wird, ist offen.

Grundsätzlich sollte die Seite so konfiguriert werden, dass keine automatischen Weiterleitungen von IP-Adressen an die Dritten stattfinden. Links zu Sozialen Medien sollten echte Links sein, die erst beim Anklicken die betreffende Seite aufrufen. Die für die Darstellung der benötigten Schriften erforderlichen Schriftpakete sollten auf dem Webseiten-Server vorgehalten werden. Die fehlende Information bezüglich des Nachladens von Schriften über Google war z. B. schon Gegenstand ganz vereinzelter Abmahnung. Andere Programmbibliotheken wie etwa JQuery für die vereinfachte Programmierung von JavaScript sollten ebenfalls lokal vorgehalten werden. Ansonsten muss hier nach Art. 13 DSGVO entsprechend informiert werden.

2) Informationspflichten in den Social Media, insbesondere Facebook

Wenn und soweit über Social Media Auftritte personenbezogene Daten erhoben werden, kommen hier ebenfalls die Informationspflichten zum Tragen. Das dürfte jedenfalls der jetzt schon zu ziehende Schluss aus dem Facebook-Urteil des EuGH sein. Dabei geht der EuGH von einer gemeinsamen Verantwortung (Art. 26 DSGVO) aus. Dies beinhaltet auch die Erfüllung der Informationspflichten. Zurzeit (Mitte August 2018) hat allerdings Facebook noch keine entsprechenden Informationen bereitgestellt. Das Betreiben einer Facebook-Seite zu Kanzleizwecken ist daher derzeit mit einem gewissen Risiko behaftet.

3) „Erheben" von Mandanten- und Mitarbeiterdaten

a) Mandantendaten

Name und Adresse sowie ggf. die Bankdaten der Mandanten werden daher in der Regel bei diesem selbst zum Zweck der Durchführung des Anwaltsvertrags „erhoben". Hier sind unstreitig die entsprechenden Informationen nach Art. 13 DSGVO mitzuteilen. Dies kann am einfachsten durch eine entsprechende Beilage bei der Mandatsbestätigung vorgenommen werden.

b) Mitarbeiterdaten

Bei den Mitarbeiterdaten ist zu unterscheiden:

aa) Bewerberdaten

aaa) In Papierform

Unaufgeforderte Bewerbungen, die in Papierform in der Kanzlei eintreffen, sind als Übermittlung bzw. als Zufluss zu bewerten. Daher müsste normalerweise nicht informiert werden. Es fragt sich aber, ob nicht unter dem Gesichtspunkt des Beschäftigtendatenschutzes der Art. 13 DSGVO teleologisch erweitert ausgelegt werden muss und somit von einer Informationspflicht auszugehen ist. Dies umso mehr, als ja ohnehin der Bewerber eine Eingangsbestätigung oder Ablehnung erhält.

Bei Ablehnung werden die Unterlagen nach Art. 6 Abs. 1 lit. b) bzw. c) noch zwei bis sechs Monate aufbewahrt und dann zurückgesendet oder vernichtet.

bbb) Per Mail

Etwas schwieriger ist die Lage bei der nur einfach signierten Mailzusendung. Diese Übermittlungsform ist deutlich unsicherer als die Post, was die Authentizität des Absenders betrifft. Zuweilen werden solche Bewerbungsmails von Kanzleien ohne Weiteres gelöscht. Das Vorhalten und Speichern solcher – unangeforderter Bewerbungsmails – ist sicher als Verarbeitung einzuordnen. Mit Art. 11 Abs. 1 DSGVO kann man allerdings sagen, dass an einer (weiteren, sicheren) Identifizierung kein Interesse besteht – zumal ja die Daten ohnehin sofort gelöscht werden. Damit entfiele hier eine Informationspflicht.

Will man eine Initiativ-Bewerbung per Mail ernst nehmen, handelt es sich nach der hier vertretenen Auffassung um eine Übermittlung und keine Erhebung. Allerdings wäre hier unter dem Gesichtspunkt des Beschäftigtendatenschutzes eine Information nach Art. 13 DSGVO gleichwohl zu empfehlen.

ccc) Bewerbungsformular online

Ein online gestelltes Bewerbungsformular, ob als PDF oder Webformular, wird man wohl als Hilfsmittel einer Erhebung ansehen müssen. Dateneingänge über solche Kanäle sind damit keine Übermittlung bzw. Zufluss, sondern lösen als Ergebnis einer Erhebung Informationspflichten nach Art. 13 DSGVO aus.

bb) Neue Mitarbeiter

Bezüglich bestehender Mitarbeiterverhältnisse ist nicht zu informieren, wenn und soweit nicht neu erhoben wird. Das dürfte wohl selten der Fall sein. Bei neu eingestellten Mitarbeitern ist nach Art. 13 DSGVO zu informieren bzw. sind die Informationen, die im Rahmen des Bewerbungsverfahrens erteilt wurden, entsprechend zu ergänzen.

4) „Erheben" von Daten der Kolleginnen und Kollegen

Wenn und soweit personenbezogene Daten in der Kanzlei ohne „beim Betroffenen" „erhoben" worden zu sein, zufließen, unterfallen sie nach der hier vertretenen Meinung eben nicht den Informationspflichten nach Art. 13 DSGVO. Das initiale Schreiben der gegnerischen Kanzlei ist daher nicht unter Beifügung eines Informationsblattes zu beantworten.

Bei bestehenden geschäftlichen Kontakten sind ohnehin die Ausnahmen der Art. 13 Abs. 3 und Art. 14 Abs. 5 DSGVO einschlägig, sodass hier nicht zu informieren ist. Bei diesen Kontakten sind in der Regel alle von Art. 13 und Art. 14 geforderten Informationen dem Betroffenen bekannt.

Ansonsten ist tatsächlich zu überlegen, ob hier nicht die Art. 13/14 DSGVO teleologisch zu reduzieren sind. Der Schutzbedarf von Kollegen und Kolleginnen, die in ihrer beruflichen Sphäre tätig sind, könnte eine entsprechende Einengung der Anwendung der Transparenzvorschriften nahelegen.

5) „Erheben" von Daten sonstiger Dritter (Gegner, Sachverständige, Gericht, Behörde)

a) Gegnerische Partei

Werden vom Mandanten personenbezogene Daten Dritter, also etwa Gegnerdaten benannt oder Schriftverkehr (auch mit Behörden) mit personenbezogenen Daten vorgelegt, so ist von einem informationspflichtfreien Zufluss auszugehen. Sollten personenbezogene Informationen zu Dritten auf Nachfrage durch den Mandanten erfolgen, käme eine Informationspflicht nach Art. 14 DSGVO in Betracht. Da diese jedoch regelmäßig dem anwaltlichen Berufsgeheimnis unterliegen, entfällt eine entsprechende Informationspflicht nach Art. 14 Abs. 5 lit. d) DSGVO.

b) Sachverständiger, außerhalb einer ständigen Geschäftsbeziehung

Wird von der Kanzlei ein Sachverständiger ermittelt und beauftragt, unterfällt dies der Informationspflicht nach Art. 13 DSGVO, wenn er aktiv beteiligt war (enge Auffassung[9]). Wird die Adresse bspw. von der Website des Sachverständigen erhoben, kommt nur Art. 14 DSGVO in Betracht. Da allerdings diese Daten regelmäßig dem Berufsgeheimnis unterliegen, ist eine Informationspflicht nach Art. 14 Abs. 5 lit. d) DSGVO nicht gegeben. Dies gilt bei vergleichbaren Sachverhalten auch für Ermittlungen und Erhebungen personenbezogener Daten sonstiger Betroffener.

c) Gerichte

Die Korrespondenz mit den Gerichten wird ja zunächst mit der Institution geführt. Im Rahmen dieser Korrespondenz anfallende personenbezogene Daten (Name des Richters, der Richterin, der Mitarbeiter) „fließen zu" und sind daher nicht informationspflichtig. Werden hier gleichwohl pbD erhoben, fehlt aber die aktive Mitwirkung der Betroffenen, kommt wiederum nur Art. 14 und hier die Ausschlussklausel des Abs. 5 lit. d) DSGVO in Betracht.

d) Sonstige Dritte z. B. Dienstleister, Lieferanten

Dem Wortlaut nach lösen auch natürliche Personen bei Dienstleistern und Lieferanten, wenn und soweit deren personenbezogene Daten im Anwendungsbereich der DSGVO erhoben werden, die Informationspflichten nach Art. 13/14 DSGVO aus. Hier gilt das unter b) Gesagte.

Wenn und soweit diese pbD nicht dem anwaltlichen Berufsgeheimnis unterliegen, kommt unter Umständen eine teleologische Reduktion der Art. 13/14 DSGVO in Betracht. Man kann sich hier nämlich schon fragen, ob umfassende Informationspflichten tatsächlich noch sinnvoll und risikoadäquat sind, wo natürliche Personen als Beschäftigte in der beruflichen Sozialsphäre tätig sind. Es könnte sich die konsequente allseitige Erfüllung allfälliger Informationspflichten als Informations-Overkill herausstellen.

9 BeckOK DatenschutzR/Schmidt-Wudy, 24. Ed. 1.5.2018, DS-GVO Art. 13 Rn. 30-32.
10 Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 1 zu Art. 13; Paal/Pauly, DSGVO, 2. Aufl. 2018, Rz. 5 zu Art. 13.
11 https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbststaendige-Heilberufler-beachten.html, abgerufen am 12.8.2018.

C. Informationspflichten

I. Inhalt der Informationspflicht

Die Informationspflichten im Einzelnen ergeben sich aus dem Wortlaut von Art. 13 DSGVO. Es herrscht mittlerweile weitgehend Einigkeit, dass die unterschiedlichen Formulierungen von Absatz 1 und 2 bezüglich der Übermittlung der Informationen (einmal heißt es „teilt mit", dann aber „stellt zur Verfügung") unerheblich sind. Auch die weitere Einschränkung bezüglich der Pflichten aus Abs. 2 Informationen auf solche, die zur transparenten und fairen Verarbeitung notwendig sind, ist in der Praxis schwer vorzunehmen. Daher sollten derzeit als sicherer Weg alle Informationen aus Art. 13 DSGVO erteilt werden.

Die einzelnen Informationen finden sich im Muster unter E. bzw. in den Erläuterungen.

Zu beachten ist auch, dass die Informationen „mitgeteilt" werden müssen und diese Mitteilung grundsätzlich auch nachzuweisen ist. Darunter wird „aktives" Tun verstanden[10]. Näheres regelt Art. 12 DSGVO (s.o.).

II. Zeitpunkt der Informationsmittteilung

Nach Art. 13 Abs. 1 DSGVO ist „zum Zeitpunkt der Erhebung" mitzuteilen. Dies würde bedeuten, dass z. B. eine Kanzleimitarbeiterin bei der telefonischen Abfrage des Mandantennamens und der Adresse zur Eintragung in das Kanzleisystem sofort eine Information nach Art. 13 erteilen müsste. Dies ist teilweise – z. B. bei Arztpraxen – wohl tatsächlich über entsprechende telefonische Informationsschleifen realisiert worden. Die Behörden scheinen dies nicht ganz so strikt zu sehen. So hält das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) einen „zeitlichen Zusammenhang mit der Erhebung der Daten" bei Arztpraxen bzw. generell Heilberufen für ausreichend:

„Ebenso wenig ist es erforderlich, den Patienten die Informationen schon am Telefon vorzulesen, wenn diese anrufen, um einen Termin zu vereinbaren. Hier genügt es, wenn die Informationen auf der Homepage der Praxis leicht auffindbar sind. Nicht ausreichend wäre es andererseits, wenn die Informationen lediglich in der Praxis ausgehängt werden."[11]

Damit nähert sich die Auslegung des Art. 13 dem Wortlaut des Art. 14 Abs. 3 DSGVO an, der von einer „angemessenen Frist", „dem ersten Zeitpunkt der Kommunikation" bzw. dem „Zeitpunkt der ersten Offenlegung" spricht.[12]

D. Sanktionen

Ein mindestens fahrlässiger Verstoß gegen Art. 13/14 kann eine Geldbuße nach Art. 83 Abs. 5 lit.b) DSGVO nach sich ziehen, gleichzeitig ist die Möglichkeit einer Verbandsklage nach Art. 80 DSGVO, zudem Schadensersatz nach Art. 82 Abs. 1 DSGVO gegeben[13].

Welche sonstigen Folgen eine Nichtbeachtung oder mangelhafte Beachtung nach sich zieht, regelt die DSGVO nicht. Nach einer Meinung wird Rechtmäßigkeit der Verarbeitung nicht zwingend beeinträchtigt[14]. Andere[15] lehnen eine Auswirkung auf die Rechtmäßigkeit der Verarbeitung in jedem Fall ab.

Es ist nach der ersten Meinung zu unterscheiden, ob die ordnungsgemäße Information nur mit Willen des Betroffenen rechtmäßig erhoben werden kann, die Erfüllung der Informationspflichten mithin konstitutiv für die Rechtmäßigkeit der Verarbeitung ist. Dies soll beispielsweise bei der Einwilligung oder bei einer Willenserklärung zum Vertragsschluss der Fall sein[16]. Für die Kanzlei hätte diese Ansicht erhebliche Folgen. Eine vergessene oder nicht nachweisbare Informationserteilung könnte die gesamte Verarbeitung der pbD im Rahmen des Mandats bewirken.

Insofern empfiehlt sich, als sicherer Weg, die Informationen nach Art. 13 DSGVO robust d.h. nachweisbar in das Mandatsannahmeverfahren zu integrieren.

12 Skeptisch bzgl. der „Zweiteilung der Informationspflichten" auch W. Veil in Gierschmann (Hrsg.), DSGVO, 2018, Rz. 1 zu Art. 13 und 14.
13 BeckOK DatenschutzR/Schmidt-Wudy, 24. Ed. 1.5.2018, DS-GVO Art. 13 Rn. 17-20.
14 Paal/Pauly, DSGVO, 2. Aufl. 2018, Rz. 9a zu Art. 13; Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 63.
15 Arning in: Moos (Hrsg.), Die neue DSGVO, 2018, Kapitel 6, Rz. 64 m.w.N.
16 Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 66 zu Art. 13; Noch weiter differenziert Schmidt-Wudy in: BeckOK DatenschutzR/Schmidt-Wudy, 24. Ed. 1.5.2018, DS-GVO Art. 13 Rn. 17-20. Er hält auf fehlerhafter Erfüllung der Informationspflicht nach Art. 13 DSGVO beruhende Einwilligungen eher für unwirksam, als in vertraglichen Kontexten. Er gibt allerdings der Interessenabwägung im Einzelfall den Vorzug vor pauschalen Lösungen.

E. Muster zur Erfüllung der Informationspflichten nach Art. 13 DSGVO für die Kanzleiwebsite und für die Mandatsdurchführung

1) Norm	Kanzlei-Website „normal“	Mandanteninformation
2) Überschrift	Informationen zur Datenerhebung nach Art. 13 DSGVO	Informationen zur Datenerhebung nach Art. 13 DSGVO
3) Einleitung	Beim Abruf unseres Kanzleiauftritts im Web, erheben wir personenbezogene Daten. Nachfolgend finden Sie dazu nähere Informationen. Sollten Sie dazu Fragen haben, können Sie gerne unter den angegebenen Kontaktdaten Verbindung mit uns aufnehmen.	Zum Zweck der Durchführung des Mandatsvertrags müssen wir einige personenbezogene Daten von Ihnen erheben. Nachfolgend finden Sie dazu nähere Informationen. Sollten Sie dazu Fragen haben, können Sie gerne unter den angegebenen Kontaktdaten Verbindung mit uns aufnehmen.
4) Art. 13 Abs. 1 lit a) Name und Kontaktdaten Verantwortlicher	Kanzlei Mustermann Musterstraße 1 00000 Musterstadt Tel.: ##### Mail: ####	Kanzlei Mustermann Musterstraße 1 00000 Musterstadt Tel.: ##### Mail: ####
5) Art. 13 Abs. 1 lit b) ggf. Kontaktdaten DSB	c/o Kanzlei Mustermann Musterstraße 1 00000 Musterstadt info@datenschutz-mustermann.de	c/o Kanzlei Mustermann Musterstraße 1 00000 Musterstadt info@datenschutz-mustermann.de
6) Art. 13 Abs. 1 lit c) Zwecke und Rechtsgrundlage(n)	Bereitstellung der Website zum Zwecke der Information über das Leistungsangebot der Kanzlei Art. 6 Abs. 1 lit. f) DSGVO	Die Datenerhebung ist notwendig zur Durchführung des Mandatsvertrages. Art. 6 Abs. 1 lit. b) DSGVO
6a) § 13 Abs. 1 Telemediengesetz Art, Umfang und Zweck der Erhebung und Verwendung	Zu den Zugriffsdaten gehören die IP-Adresse Ihres Geräts, der von Ihnen verwendete Browser, das Zugriffsdatum und die Uhrzeit, die Webseite, von der aus Sie uns besuchen, sowie die Webseiten, die Sie bei uns besuchen.	
6b) Art. 14 Abs. 1 lit. d) DSGVO	Kategorien personenbezogener Daten, die verarbeitet werden	Kategorien personenbezogener Daten, die verarbeitet werden – Adressdaten – Bankverbindung
7) Art. 13 Abs. 1 lit d) ggf. Art. 6 Abs. 1 lit. f) berechtigtes Interesse	Informationen von Mandanten und Interessierten über das Leistungsangebot der Kanzlei	((entfällt))
8) Art. 13 Abs. 1 lit e) ggf. Empfänger bzw. Kategorien von Empfängern	Webhoster der Kanzlei	Ggf. Gegner, Gerichte, Sachverständige
9) Art. 13 Abs. 1 lit f) Ggf. Drittlandsübermittlung	((nur bei Weitergabe z. B. an Google))	((entfällt))
10) Art. 13 Abs. 2 lit a) Speicherdauer bzw. Kriterien	Drei Wochen	10 Jahre gem. HGB und AO
11) Art. 13 Abs. 2 lit b) Rechte des Betroffenen Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;	Es besteht ein Recht auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;	Es besteht ein Recht auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

12) Art. 13 Abs. 2 lit c) ggf. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;	((bei einer einfachen Website nicht gegeben)) ((Bei einer Einwilligung in Cookies kann der Widerruf paradoxerweise nur durch einen entsprechenden Cookie realisiert werden – Matomo-Lösung))	((entfällt))
13) Art. 13 Abs. 2 lit d) Beschwerderecht bei einer Aufsichtsbehörde	Sie haben das Recht, sich bei der zuständigen Aufsichtsbehörde zu beschweren.	Sie haben das Recht, sich bei der zuständigen Aufsichtsbehörde zu beschweren.
14) Art. 13 Abs. 2 lit e) Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte	Ohne die Erhebung der IP-Adresse ist eine Bereitstellung der Website im World Wide Web aus technischen Gründen nicht möglich.	Ohne die erhobenen Daten kann der Mandatsvertrag nicht ordnungsgemäß erfüllt werden.
15) Art. 13 Abs. 2 lit. f) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person	Eine automatisierte Entscheidungsfindung besteht nicht.	Eine automatisierte Entscheidungsfindung besteht nicht.

Erläuterung zu den Mustererklärungen

Zu 1): Allgemeine Datenschutzerklärung oder Erfüllung einer Informationspflicht?

Aus dem Wortlaut von Art. 13 Abs. 1 DSGVO geht hervor, dass sich die Informationspflicht auf einen bestimmten Erhebungsvorgang bezieht. Es reicht daher wohl nicht aus, etwa auf der Kanzleiwebsite alle möglichen Erhebungsvorgänge zu allen möglichen Zwecken aufzuführen.

Für die Kanzlei ist zunächst die Information auf der Kanzleiwebsite und die des Mandanten die wichtigste. Die Erfüllung der Informationspflichten gegenüber Kollegen oder Dritten s.o.

Zu 2): „Informationen zur Datenerhebung"

Die Überschrift ist grundsätzlich frei wählbar. Häufig findet man hier z.B. „Datenschutzerklärung". Es ist zu empfehlen, die Erklärung möglichst konkret zu benennen und durchaus die Norm zu zitieren. Dabei verdeutlicht die Überschrift „Informationen zur Datenerhebung" eben genau, worum es geht.

Zu 3): Die „Anmoderation" oder zweck- und adressatenbezogene Einleitung

Es macht die Informationen lesbarer, wenn diese zweck- und adressatenbezogen „anmoderiert" werden. Die Erfüllung der Informationspflichten kann in ganz unterschiedlicher Weise vorgenommen werden. Für die Kanzlei ist auch dies ein Teil der Corporate Identity. Die konkrete Ausformulierung hat sehr stark mit der Zielgruppe zu tun. Nach der hier vertretenen Sicht macht es z.B. für eine Wirtschaftskanzlei wenig Sinn, die Erklärungen jeweils in „leichter Sprache" zu formulieren. Wichtig ist vielmehr, dass die Datenschutzziele im jeweiligen Kontext erreicht werden.

Generell sollten Stereotypen vermieden werden. Mit „Wir nehmen den Datenschutz sehr ernst …" zu beginnen, ist ein solches Stereotyp. Man kann daher die Einleitung sehr knapp halten oder sachlich informierend etwa wie folgt formulieren:

„Die Datenschutz-Grundverordnung (DSGVO) verpflichtet uns, bei Erhebungen von personenbezogenen Daten bei Ihnen bestimmte Informationen mitzuteilen. Dem kommen wir im Folgenden gerne nach. Sollten Sie darüber hinaus Fragen hierzu haben, stehen wir Ihnen unter den angegebenen Kontaktdaten gerne zur Verfügung."

Zu 4): Name und Kontaktdaten des/der Verantwortlichen

Hier ist mindestens die Kanzleianschrift anzugeben.

Zu 5): Kontaktdaten des Datenschutzbeauftragten

Der Streit, ob der Name anzugeben ist, kann als beendet betrachtet werden. Der Name des DSB ist nicht pflichtgemäß zu nennen. Er kann gleichwohl angegeben werden. Ansonsten ist eine eigene E-Mail-Adresse einzurichten, auf die nur der DSB Zugriff hat. Dies folgt aus der Vertraulichkeit der Kommunikation mit dem DSB.

Zu 6): Zwecke und Rechtsgrundlagen

Hier ist es zum einen der Werbezweck, zum anderen die Durchführung des Mandatsvertrages. Beides sind legitime Zwecke. Als Rechtsgrundlagen sind hier Art. 6 Abs. 1 lit. f) bzw. lit. b) DSGVO zu nennen.

Zu 6a): Art und Umfang der erhobenen Daten

Vom Art. 13 DSGVO ausdrücklich nicht gefordert sind Informationen zu Art und Umfang der erhobenen Daten.

Entsprechende Informationen sind gleichwohl zu empfehlen. Zwar genießt die DSGVO gegenüber den spezifisch datenschutzrechtlichen Normen des Telemediengesetzes (TMG) einen Anwendungsvorrang, das schließt aber weitergehende Anforderungen nicht unbedingt aus. In diesem Sinne normiert § 13 Abs. 1 Satz 1 TMG die Pflicht, Angaben zu Art und Umfang der erhobenen Daten zu machen.

Zu 6b): Kategorien personenbezogener Daten

Erstaunlicherweise fordert Art. 13 DSGVO nicht, die Kategorien der personenbezogenen Daten, die verarbeitet werden, mitzuteilen. Da absehbar ist, dass Art. 13 und 14 DSGVO in der Praxis immer mehr zusammen gesehen werden und Rechtsgedanken wechselseitig übertragen werden, sollten hier die Kategorien angegeben werden.

Zu 7): Das berechtigte Interesse

Stützt sich der Erhebungszweck auf ein berechtigtes Interesse, so ist dieses hier darzulegen. Eigenwerbung ist nach der DSGVO ein generell anerkanntes berechtigtes Interesse. Dabei ist immer auch an Art. 21 DSGVO zu denken. Dieser sieht grundsätzlich ein „Widerspruchsrecht" des Betroffenen vor. Bei einer Website wird dies allerdings schwierig zu beachten sein, da die Website ja vom Betroffenen aktiv aufgerufen werden muss.

Zu 8): Empfänger oder Kategorien von Empfängern

Hier findet sich in der Literatur[17] die Ansicht, dass stets der konkrete Empfänger benannt werden müsste und die Kategorie nur ausnahmsweise in Betracht komme. Nach der hier vertretenen Auffassung besteht hier ein Wahlrecht des Verantwortlichen. Die Benennung z. B. des Webhosters schafft Sicherheitsrisiken. Mit einfachen Mitteln des „Webscrapings" lassen sich hier die entsprechenden Namen elektronisch „einsammeln", auswerten und interessante Hosting-Unternehmen als Angriffsziele markieren.

Zu 9): Drittlandsübermittlung

Die wohl häufigsten Fälle der Drittlandsübermittlung ergeben sich wenn und soweit auf der Kanzleiwebsite entsprechende Weiterleitungen an Dienstleister wie Google etc. stattfinden. Das Grundproblem

17 Kühling/Buchner, DSGVO, 2. Aufl., 2018, Rz. 30 zu Art. 13.

der Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. mittlerweile des EWR besteht im nicht angemessenen Schutzniveau. Wenn also in der Informationserteilung nach Art. 13 DSGVO eine Drittlandsübermittlung angegeben wird, dann sollte sichergestellt sein, dass diese auch rechtmäßig erfolgt.

Zu 10): Speicherdauer bzw. Kriterien

Die DSGVO unterscheidet bei der Frage der Löschverpflichtung bzw. der Aufbewahrungsfrist nach den jeweiligen Zwecken (Art. 5 Abs. lit. e) Satz 1 DSGVO). Eine Rechtmäßigkeitsbedingung aus Art. 6 Abs. 1 lit. c) DSGVO ist dabei die Aufbewahrung in Erfüllung entsprechender gesetzlicher Pflichten.

Es besteht in der Literatur Einigkeit, dass der bloße Verweis auf die „Einhaltung der gesetzlichen Vorgaben zur Datenspeicherung" nicht ausreichend ist.

Wie genau darüber hinaus zu informieren ist, ist derzeit eher unklar.

Bei der Website sind die Speicherfristen ggf. durch Nachfrage beim Dienstleister in Erfahrung zu bringen und wiederum auf Rechtmäßigkeit zu überprüfen. Das Schutzziel der „Speicherbegrenzung" bzw. der Intervenierbarkeit (Art. 5 Abs. 1 lit. e) DSGVO) verbietet die zweckunabhängige beliebige Speicherung von pbD. Der alte Satz von der „revisionssicheren" Aufbewahrung bedeutet daher nicht mehr „ewige" Aufbewahrung. Die in Kanzleien anzutreffende Praxis, analoge Akten i. d. R. nach 10 Jahren zu schreddern, die Digitalkopien jedoch weiter aufzubewahren, könnte daher datenschutzrechtlich problematisch sein.

Bei einer „einfachen" Kanzlei-Website – also ohne Tracking-Tools und Cookies – ergibt sich aus dem berechtigten Interesse der Kanzlei am sicheren Betrieb der Website aus Art. 5 Abs. 1 lit. e) i. V. m. 6 Abs. 1 lit. f) DSGVO eine rechtmäßige Aufbewahrungsmöglichkeit zum Erkennen von Angriffsmustern bzw. zum Vornehmen von Ermittlungen von zwei bis drei Wochen. Im Einzelnen ist dies mit dem jeweiligen Webhoster zu klären.

Bei der Mandantenakte ist die Lage etwas komplexer. Hier kommen neben den allgemeinen Aufbewahrungspflichten aus § 147 Abs. 1 AO (10 bzw. 6 Jahre) oder § 257 Abs. 1 HGB (10 bzw. 6 Jahre) auch noch berufsrechtliche Regelungen hinzu.

Mit Verweis auf den „Möglichkeitsvorbehalt" im Text des Art. 13 DSGVO lassen Gierschmann, Schlender, Stentzel, Veil, Kommentar zur DSGVO, 2018, Rz. 43 zu Art. 30 die abstrakte Umschreibung in einer solchen Lage ausreichen.

In der Kanzlei stellt sich allerdings vor dem Hintergrund des Schutzziels der Intervenierbarkeit bzw. der Speicherbegrenzung – unabhängig von der Erfüllung der Informationspflichten – die Frage, wann denn nun welche Daten gelöscht werden.

Ob nicht aus Haftungsgründen eine längere Aufbewahrung vorgenommen werden kann ist fraglich. Nach § 195 BGB beträgt die regelmäßige Verjährungsfrist von Ansprüchen 3 Jahre bzw. in Fällen des § 199 Abs. 3 bzw. Abs. 3a BGB 10 Jahre bzw. 30 Jahre.

Hier fragt sich allerdings, ob die Berücksichtigung von Verjährungspflichten nicht eher eine Obliegenheit als die Beachtung einer gesetzlichen Pflicht ist. Auf der anderen Seite schließt Art. 17 Abs. 3 lit. e) DSGVO die Verpflichtung zur Löschung auf Verlangen des Betroffenen aus, wenn die Verarbeitung – also hier die Speicherung – zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Nach § 50 BRAO können Handakten – soweit keine abweichende Vereinbarung mit dem Mandanten getroffen wurde, nach 6 Jahren gelöscht werden. Die Frist beginnt mit Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde.

Eine im Zusammenhang mit den Löschpflichten bzw. Aufbewahrungsfristen sehr beachtliche berufsrechtliche Pflicht stellt § 43a Abs. 4 BRAO, Verbot der Vertretung widerstreitender Interessen, dar. Die genaue Prüfung bedingt Zugang zu den Unterlagen. Ansonsten können Art und Umfang der Vertretung nicht mehr genau bestimmt werden. Da das Verbot der Vertretung widerstreitender Interessen zeitlich nicht begrenzt ist, besteht hier die Möglichkeit, die Akten entsprechend lange zu speichern.

Zu 11): Rechtsbelehrung

Hier besteht – je nach Kontext – ein Gestaltungsspielraum, wie ausführlich die Darstellung der Rechte ausfallen soll. Es empfiehlt sich, alle Rechte zu nennen.

Zu 12): Widerrufsrecht

Bei einer einfachen Kanzleiwebsite ohne Tracking und Cookies entfällt der Punkt. Im Rahmen der Mandatsannahme dürfte in der Regel auch keine Einwilligung nötig sein. Selbst wenn es um Mandate mit Bezug zu besonderen Kategorien personenbezogener Daten geht - wie etwa im Arbeitsrecht, Familienrecht, Medizinrecht oder Strafrecht – „schaltet" Art. 9 Abs. 2 lit. f) DSGVO die Geltung des generellen Verarbeitungsverbots des Art. 9 Abs 1 DSGVO aus. Die Verarbeitung wird ja regelmäßig zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sein.

Zu 13): Beschwerderecht

Hier muss die konkrete Behörde nicht benannt werden.

Zu Art. 14): Folgen der Nichtbereitstellung

Die Folgen der Nichtbereitstellung ergeben sich häufig schon aus dem Zweck der Erhebung. Die „Folgenaufklärung" liest man bislang eher selten. Sicherheitshalber sollte hier doch mindestens ein Satz angemerkt werden.

Zu Art. 15): Automatisierte Entscheidung

Bislang werden in Kanzleien wohl eher sehr selten automatisierte Entscheidungen im Zusammenhang mit Mandanten getroffen. □