Anwaltsrecht

DAV-Merkblatt: Umsetzung der Datenschutz-Grundverordnung in Anwaltskanzleien

Wichtige Hinweise und konkrete Tipps zum Inkrafttreten am 25. Mai 2018*

Am 25. Mai 2018 tritt die neue europäische Datenschutz-Grundverordnung (DSGVO) in Kraft. Das neue Datenschutzrecht gilt – von wenigen Ausnahmen abgesehen – auch für Anwaltskanzleien. Es ist zu erwarten, dass es in Zukunft vermehrt zu Konflikten zwischen Anwälten und Datenschutzbehörden kommen wird. Anwälte sollten sich daher um eine rechtzeitige Umsetzung der DSGVO in der Kanzlei bemühen. Noch bleibt ausreichend Zeit, um sich auf die neuen gesetzlichen Anforderungen vorzubereiten.

I. Neuregelung des Datenschutzrechts

Thema: Keine Übergangsfrist

Nach dem 25. Mai 2018 gibt es keine Übergangsfrist. Soweit die DSGVO auf Anwaltskanzleien anwendbar ist, müssen sämtliche Anforderungen des neuen Rechts ab dem 25. Mai 2018 eingehalten werden. Sollte dies nicht der Fall sein, werden die Datenschutzbehörden per Verwaltungsakt aufsichtsrechtliche Maßnahmen erlassen und Bußgelder verhängen.

Hintergrund: Verordnung gilt unmittelbar

Als Verordnung gilt das neue europäische Datenschutzrecht in allen EU-Mitgliedsstaaten ab dem 25. Mai 2018 unmittelbar und vorrangig. In einer Neufassung des Bundesdatenschutzgesetzes (BDSG-neu) hat Deutschland einige Spielräume genutzt, die sich in den Öffnungsklauseln der DSGVO finden. Das BDSG-neu tritt zusammen mit der DSGVO am 25. Mai 2018 in Kraft.

Warum handeln? Bußgelder nach der DSGVO

Anwaltskanzleien, deren Datenverarbeitung nach dem 25. Mai 2018 nicht dem neuen Recht entsprechen, müssen mit Bußgeldern rechnen, die nach neuem Recht bis zu 20 Millionen Euro betragen können. Die deutschen Datenschutzbehörden sind entschlossen, von dem neuen Bußgeldrahmen Gebrauch zu machen, und halten sich hierzu sogar nach europäischem Recht für verpflichtet. Dies umso mehr, als neue förmliche Beschwerdebefugnisse der Betroffenen eingeführt werden. Beschweren sich in Zukunft Mandanten oder Mitarbeiter bei der zuständigen Datenschutzbehörde, darf die Behörde nicht untätig bleiben und muss den Beschwerden nachgehen.

Das Datenschutzrecht ist im Wirtschaftsverkehr *Ländersache*. Für die Verfolgung von Datenschutzverstößen ist die Datenschutzbehörde des Bundeslandes zuständig, in der die Anwaltskanzlei ihren Hauptsitz hat.

II. Datenschutz vs. Anwaltsgeheimnis

Herausforderung: Keine Grauzone mehr

Nach neuem Recht gibt es keinen Zweifel mehr daran, dass das Datenschutzrecht auch für Mandats- und Mandantendaten gilt. Es ist nur eine Frage der Zeit, bis es neue Verfahren der Aufsichtsbehörden gegen Anwaltskanzleien gibt.

Problem: Vielfältige Formen der Datenverarbeitung

In jeder Mandatsakte befinden sich zahlreiche Daten mit Personenbezug. Dies sind keineswegs nur die Informationen über den *Mandanten*, sondern auch Informationen über *Prozessgegner, Verhandlungspartner, Zeugen und Richter*. Neben den Mandatsdaten und den Mandantenadressen finden sich auf jedem Kanzleirechner zahlreiche Namen und Anschriften von Mitarbeitern, Lieferanten und Dienstleistern. Sofern die Anwaltskanzlei Marketing betreibt, verfügt sie zudem über Adressdaten und weitere Angaben zu potenziellen Mandanten, Newsletter-Abonnenten und Website-Besuchern.

Sobald diese Daten verarbeitet werden, gilt die DSGVO. Dabei ist der Begriff der „Verarbeitung“ weit zu verstehen: Ob Erheben („Sammeln“), Speichern, Weitergeben oder Löschen, es handelt sich stets um eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO.

Wissen: Wenige, aber wichtige Ausnahmen vom Datenschutz

Die DSGVO lässt Ausnahmen vom Datenschutz nur in wenigen Öffnungsklauseln zu. Von diesen Öffnungsklauseln hat Deutschland immerhin Gebrauch gemacht, um das Anwaltsgeheimnis vor übermäßigen Begehrlichkeiten der staatlichen Datenschützer zu bewahren.

- Anders als bei anderen Unternehmen haben die Aufsichtsbehörden bei Anwaltskanzleien *kein Recht auf Zugang* zu den Kanzleiräumen (§ 29 Abs. 3 BDSG-neu).
- Die Behörden haben zudem *keine Zugriffsrechte* und dürfen keine Einblicke in die anwaltliche Datenverarbeitung verlangen. Die Kanzleiserver und -rechner sind für die Behörden tabu (§ 29 Abs. 3 BDSG-neu).
- Auch bei den Betroffenenrechten gibt es *Ausnahmen* zum Schutz des Anwaltsgeheimnisses. Prozessgegner und andere Außenstehende können *keine Informations- und Auskunftsrechte* aus Art. 14 und 15 DSGVO geltend machen, wenn es um Daten geht, die dem Anwaltsgeheimnis unterliegen (§ 29 Abs. 1 BDSG-neu). Die Mandatsakte bleibt auf diese Weise davor geschützt, dass unter dem Deckmantel des Datenschutzrechts Auskunft über Akteninhalte verlangt wird.

Hintergrund: Überholte Rechtsprechung zum Anwaltsgeheimnis

In einer Kanzlei werden sowohl mandatsbezogene Daten verarbeitet als auch Daten außerhalb des Mandats. Dass das Datenschutzrecht für die Verarbeitung der Daten des Personals oder

im Bereich des Marketings auch für Anwaltskanzleien gilt, war stets unstreitig. Problematisch und umstritten war und ist die Anwendung des Datenschutzrechts jedoch, wenn es um mandatsbezogene Daten geht. Erhalten staatliche Aufsichtsbehörden Einblicke in die Anwaltsakten, ist das Anwaltsgeheimnis in Gefahr. Dass das Anwaltsgeheimnis nach bisherigem Recht grundsätzlich Vorrang vor dem Datenschutzrecht hat, entschied vor einigen Jahren das Berliner Kammergericht (KG vom 20. August 2010, 1 Ws (B) 51/07, AnwBl 2010, 802). Seitdem sind keine größeren Konflikte zwischen Datenschutzbehörden und Anwälten bekannt geworden. Anders als Ärzte und Zahnärzte gerieten Anwälte in den letzten Jahren nur selten in das Visier der Datenschutzaufsicht. Mit Inkrafttreten der DSGVO ändert sich für Anwälte die Rechtslage.

III. Fünf Schritte zur Umsetzung der DSGVO

Die DSGVO erlegt den Datenverarbeitern *umfangreiche Pflichten* auf. Kenner der Materie wissen zugleich, dass das Ziel einer hundertprozentigen Befolgung aller Regeln illusorisch ist. Auch den Datenschutzbehörden ist bewusst, dass es keinem Unternehmen gelingen wird, das neue Recht lückenlos zu befolgen. Bei der Umsetzung des neuen Rechts empfiehlt sich daher eine ebenso *gründliche wie pragmatische Herangehensweise*. Zunächst sollten die wichtigsten Anforderungen des neuen Rechts nachweisbar erfüllt werden. Dies kann *in fünf Schritten* geschehen. Damit ist dann eine Basis gelegt für weitere Maßnahmen, mit denen sich nach und nach Schwachstellen schließen lassen, um den Erfordernissen der DSGVO in größtmöglichem Umfang zu genügen.

1. Erster Schritt: Betrieblicher Datenschutzbeauftragter

Filterfrage: 10-Personen-Regel

Wie nach dem bisherigen Recht gibt es auch nach Art. 37 Abs. 4 DSGVO in Verbindung mit § 38 Abs. 1 BDSG-neu eine *10-Personen-Regel*: Sind mindestens zehn Personen in der Kanzlei mit der Datenverarbeitung beschäftigt, muss ein Datenschutzbeauftragter bestellt werden. Ist dies bislang nicht der Fall, sollte man die Bestellung schnellstmöglich nachholen.

Bei der 10-Personen-Regel ist zu beachten, dass es allein um die Anzahl der Personen geht, die mit Datenverarbeitung ständig befasst sind. Ob es sich um Partner oder Studenten, Buchhalter oder freie Mitarbeiter, Vollzeit- oder Teilzeitkräfte handelt, spielt keine Rolle. Es kommt allein auf die *Kopfzahl* an.

Aufgabe: Der Datenschutzbeauftragte in der Kanzlei

Der Datenschutzbeauftragte ist der Kanzleiführung direkt unterstellt, in der Wahrnehmung seiner gesetzlichen Aufgaben aber *nicht weisungsgebunden* (Art. 38 Abs. 3 DSGVO). Er überwacht die Datenverarbeitungsprozesse in der Kanzlei, unterrichtet und berät die Kanzleiführung und wirkt auf die Einhaltung des Datenschutzrechts hin. Zudem soll er die an den Verarbeitungsvorgängen beteiligten Anwälte und Mitarbeiter sensibilisieren und schulen. Gibt es eine Beschwerde, ist der Datenschutzbeauftragte die *erste Anlaufstelle* für die Datenschutzbehörde.

Tipp: Angestellter Anwalt mit IT-Affinität

Ob und unter welchen Voraussetzungen ein Partner der Kanzlei zugleich Datenschutzbeauftragter sein kann, ist unter den Datenschutzrechtlern umstritten. Unklar ist

auch, ob ein IT-Leiter zum Datenschutzbeauftragten berufen werden kann. Optimal ist die Bestellung eines angestellten Anwaltes oder eines anderen Mitarbeiters mit gewisser *IT-Affinität*. Auch die Bestellung eines *externen Datenschutzbeauftragten* ist möglich. Dies ist mit § 203 StGB-neu konform.

Warum handeln? Nichts ist leichter zu überwachen

Für eine Datenschutzbehörde ist es leicht zu prüfen, ob eine Anwaltskanzlei einen Datenschutzbeauftragten hat, da der Datenschutzbeauftragte in allen Datenschutzinformationen namhaft gemacht werden muss (Art. 37 Abs. 7 DSGVO). Jede Kanzlei, in der mindestens zehn Personen am Rechner tätig sind, sollte daher bis zum 25. Mai 2018 einen Datenschutzbeauftragten haben. Fällt die Auswahl schwer, sollte man beachten, dass ein schwach geeigneter Datenschutzbeauftragter allemal besser ist als kein Datenschutzbeauftragter.

2. Zweiter Schritt: Erstellung eines Verzeichnisses

Aufgabe: Erfassen der Verarbeitungstätigkeiten

Art. 30 DSGVO schreibt die Führung eines Verzeichnisses *aller Verarbeitungstätigkeiten* vor. Das Verzeichnis dient dem Nachweis einer DSGVO-konformen Datenverarbeitung in der Kanzlei. Als Verarbeitungstätigkeiten gelten beispielsweise:

- elektronische Anwaltsakten;
- Kanzleisoftware (zum Beispiel RA Micro, Phantasy usw.);
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware (Finanzbuchhaltung und Lohnbuchhaltung);
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- Kanzlei-Websites;
- Kanzleiseiten in Sozialen Netzwerken (z.B. Twitter, Facebook, Xing);
- elektronische Personalakten;
- betriebliches Intranet;
- Urlaubslisten.

Für das Verzeichnis ist kein bestimmter Aufbau vorgeschrieben. Es muss schriftlich oder elektronisch (etwa als *Word- oder Exceldatei*) geführt werden.

Für jede einzelne Verarbeitungstätigkeit sind folgende Angaben vorgeschrieben:

- den Namen und die Kontaktdaten der Kanzlei;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls erforderlich);
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (z.B. Mandanten, Beschäftigte oder Lieferanten);
- die Art der verarbeiteten Daten;
- die möglichen Empfänger der Daten, an die Daten übermittelt werden oder worden sind;

- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z.B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- Löschfristen;
- Maßnahmen der Datensicherheit nach Art. 32 DSGVO.

Tipp: Der Lohn der Arbeit – Erkenntnisse für das Kanzleimanagement

Die Erstellung des Verzeichnisses ist ein *mühsamer Prozess*, da es meist gar nicht so einfach ist, den Überblick darüber zu gewinnen, welche Datenverarbeitungsprozesse es in der Kanzlei gibt. Dies gilt umso mehr, wenn Anwälte und Mitarbeiter beruflich Smartphones, Tablets und Laptops ortsungebunden nutzen. Auch die Arbeit auf derartigen Endgeräten kann als Verarbeitungstätigkeit gelten, für die die Pflicht zur Aufnahme in das Verzeichnis gilt.

Wenn erstmalig ein Verarbeitungsverzeichnis angelegt wird, ist dies nach aller Erfahrung mit einem *hilfreichen Klärungsprozess* verbunden. Denn stets sind die Verarbeitungszwecke zu definieren, und die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern „verstauben“ zu lassen. Wenn ein umfangreiches Verzeichnis über die gesamte Datenverarbeitung in der Kanzlei erstellt wird, ist dies ein guter Anlass, über die Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung nachzudenken. Dies kann nicht nur dem Schutz von Mandantendaten und der Datensicherheit dienen, sondern auch der Effizienz der Arbeitsabläufe in der Kanzlei.

Die Erstellung des Verzeichnisses erfordert eine Vielzahl von Entscheidungen:

- Wie werden Speicherfristen für die Datenbank mit den Mandantenadressen definiert?
- Wer entscheidet in welchen zeitlichen Abständen, ob Adressdaten gelöscht werden?
- Wie verfährt man mit Bewerberdaten?
- Braucht man Einwilligungen für die Mitarbeiterfotos, die sich auf der Kanzlei-Website oder im Intranet finden?
- Lässt sich die Speicherung uralter Mandantendaten noch rechtfertigen? Gibt es einen guten Grund, weshalb Urlaubsanträge, Krankschreibungen, Fristenzettel und Gesprächsvermerke jahrelang gespeichert werden?

Sonderaufgabe: Datensicherheit

Maßnahmen der *Datensicherheit* sind nach Art. 32 DSGVO im Verarbeitungsverzeichnis zu definieren. Hier ist IT-Sachverstand gefragt, an der Hinzuziehung entsprechender *Fachleute* führt kein Weg vorbei. Wie funktioniert die Datensicherheit? Wie sind die Zugriffsrechte auf Daten organisiert? Haben ausschließlich Personen Zugriff, die die Daten bei ihrer täglichen Arbeit benötigen, oder ist die gesamte Kanzlei-IT ein „offenes Buch“, in dem sich jeder Mitarbeiter nach Belieben umschauen darf? Welche Maßnahmen gibt es zur Abwehr von Hackerangriffen und zum Virenschutz?

Sollte es in der Kanzlei bislang eher mäßigen Aufwand bei der Datensicherheit gegeben haben, bietet die DSGVO einen willkommenen Grund, Versäumtes nachzuholen und damit auch die Anforderungen des seit 1. Januar 2018 geltenden § 2 Abs. 7 BORA zu erfüllen. Anwälte wissen, dass das Vertrauen der Mandanten ein hohes Gut ist. Und dieses Vertrauen gerät in Gefahr, wenn Kanzleien nachlässig bei der Sicherung ihrer Datenbestände sind. Der Aufwand, den eine Anwaltskanzlei bei der Datensicherheit treibt, kann gar nicht groß genug sein. Die Einhaltung der gesetzlichen Anforderungen markiert nur das Mindestmaß für den Aufwand, der notwendig ist.

Sind die Prozesse und Zwecke der Datenverarbeitung definiert, sind Löschroutinen und Maßnahmen der IT-Sicherheit im Verarbeitungsverzeichnis festgelegt, ist das Verzeichnis laufend zu pflegen. Ändern sich Verarbeitungsprozesse oder kommen neue hinzu, muss dies im Verarbeitungsverzeichnis festgehalten werden. Damit können Verarbeitungsprozesse auch in Zukunft Anlass geben, regelmäßig die Rechtmäßigkeit der Datenverwaltung zu überdenken und dabei zugleich die Effizienz der kanzleiinternen Arbeitsabläufe zu steigern.

Warum handeln? Kontrolle ist Chefsache

Das Verfahrensverzeichnis ist der Grundpfeiler der *Dokumentation*, zu der die DSGVO umfassend verpflichtet. Auf Anforderung der Aufsichtsbehörde muss die Kanzlei jederzeit in der Lage sein, durch Vorlage des Verzeichnisses nachzuweisen, welche Verarbeitungsprozesse zu einem bestimmten Zeitpunkt aktiv waren. Für die *laufende Pflege* des Verzeichnisses sollte es daher klare Regeln geben. Zuständig hierfür kann der betriebliche Datenschutzbeauftragte oder auch ein IT-Dienstleister sein. Die Kontrolle, ob alle Regeln eingehalten werden, sollte jedenfalls stets *Chefsache* sein. Partner, denen es zu mühsam erscheint, sich mit der Datenverarbeitung im eigenen Hause zu befassen, gehen ab dem 25. Mai 2018 erhebliche (und durch keine Versicherung gedeckte) Risiken ein.

3. Dritter Schritt: „Gap Analysis“

Aufgabe: Gut sein und besser werden

Die Verarbeitungsverzeichnis ist der Ausgangspunkt für eine „Lückensuche“, die in den DSGVO-Umstellungsprozessen „Gap Analysis“ genannt wird.

Warum handeln? Maßnahmenplan

Jede einzelne Verarbeitungsverfahren muss in der „Gap Analysis“ überprüft werden im Hinblick auf mögliche *Schwachstellen*. Zu diesen Schwachstellen zählen vor allem:

- Datensparsamkeit: Ist die Vorhaltung von Daten und deren Verarbeitung tatsächlich notwendig?
- Datenrichtigkeit: Ist gewährleistet, dass Mandantendaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
- Rechtmäßigkeit: Ist die Datenverarbeitung gem. Art. 6 Abs. 1 DSGVO rechtlich zulässig? Dient die Datenverarbeitung der Erfüllung eines Vertrages? Gibt es Einwilligungen der Betroffenen? Lässt sich die Datenverarbeitung durch eigene „berechtigte Interessen“ oder durch „berechtigte Interessen“ der Mandanten legitimieren?
- Löschfristen: Werden Daten gelöscht, sobald sie nicht mehr benötigt werden? Gibt es eine Löschroutine, die eine rechtzeitige Löschung gewährleistet?
- Zugriffsrechte: Haben Mitarbeiter ausschließlich Zugriff auf Daten, die sie für ihre jeweiligen Aufgaben benötigen?
- Zugangskontrolle: Sind die Rechner in der Kanzlei ausreichend gegen den Zugang durch Unbefugte geschützt?
- Schutz gegen Hacker und Malware: Gibt es eine Firewall? Sind aktuelle Virenscanner installiert?

Am Ende jeder „Gap Analysis“ steht ein *Maßnahmenplan* mit dem Ziel der möglichst umfassenden Datenschutzkonformität aller Verfahren.

4. Vierter Schritt: Datensicherheit

Aufgabe: TOMs kennen und ergreifen

„Technische und organisatorische Maßnahmen“ – abgekürzt TOMs – sind zu ergreifen, um die Sicherheit der in der Kanzlei verarbeiteten Personendaten zu gewährleisten (Art. 32 DSGVO). Die Vorschrift konkretisiert den Grundsatz der „Integrität und Vertraulichkeit“ gem. Art. 5 Abs. 1 lit. f DSGVO.

Folgende Maßnahmen sind vorgeschrieben:

- Verschlüsselung: Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Es empfiehlt sich daher beispielsweise, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen zu ermöglichen.
- Stabilität: Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es einer fachkundigen Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
- Wiederherstellbarkeit: Verarbeitungsprozesse müssen gegen Datenverlust geschützt werden durch eine fachgerechte Datensicherung. Auch hierzu bedarf es der Unterstützung durch IT-Fachleute.
- Regelmäßige Überprüfung: Eine regelmäßige Routineprüfung ist für die Datensicherheit gleichfalls vorgeschrieben.

Die DSGVO schreibt keinen „optimalen Schutz“ vor, sondern ein *„angemessenes Schutzniveau“*, das anhand der bestehenden Risiken und des Stands der Technik zu bestimmen ist. Investitionen, die außer Verhältnis zu der Größe der Kanzlei stehen, fordert die DSGVO nicht. Jedoch sollten Kanzleien überprüfen, ob die vorhandenen Maßnahmen bereits in die Jahre gekommen sind. Gab es bisher keine Unterstützung durch eine IT-Fachfirma, kann es ratsam sein, sich über eine zukünftige Beauftragung Gedanken zu machen.

Warum handeln? Dokumentation zwingend

Dokumentationspflichten werden in der DSGVO groß geschrieben. Es sollte daher ein Papier geben, das die Bemühungen um „technische und organisatorische Maßnahmen“ der Datensicherheit und deren Durchführung belegt. Auf dieses Papier kann im Verarbeitungsverzeichnis verwiesen werden, um der Verpflichtung Genüge zu tun, die Maßnahmen der Datensicherheit im Verzeichnis zu beschreiben.

5. Fünfter Schritt: „Papierform“

Erste Aufgabe: Verträge zur Auftragsdatenverarbeitung

Bei der Datenverarbeitung bedienen sich Kanzleien meist der Unterstützung durch *Dienstleister* aller Art. Dies können IT-Servicefirmen sein oder auch Cloud-Dienstleister für die Textverarbeitung, Terminverwaltung oder Spracherkennung. All diese Verfahren waren bereits nach bisherigem Recht als *Auftragsdatenverarbeitung* anzusehen mit der Folge, dass es entsprechender Verträge bedurfte. Nach neuem Recht bleibt dies so, allerdings müssen bestehende Verträge an das neue Recht angepasst werden. Sofern noch keine Verträge existieren, sollte ein Vertragsschluss vor dem 25. Mai 2018 nachgeholt werden.

Zweite Aufgabe: Datenschutzinformationen

Zum notwendigen „Paperwork“ gehören auch *Datenschutzinformationen*. Die Informationspflichten sind nach neuem Recht wesentlich umfangreicher als dies bisher der Fall war (Art.13 und 14 DSGVO). Die Datenschutzbestimmungen auf *Kanzlei-Websites* müssen überarbeitet werden. Zudem empfehlen sich allgemeine „Hinweise zur Datenverarbeitung“, die jedem Mandatsvertrag beigefügt werden sollten. Entsprechende Hinweise gehören zudem in Zukunft in jeden Arbeitsvertrag. Dass sich entsprechende Formulare einbürgern werden, ist sicher.

Die neuen Informationspflichten umfassen unter anderem

- den Namen und die Kontaktdaten der Kanzlei;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten;
- die Art der verarbeiteten Daten;
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (z.B. Mandanten, Beschäftigte oder Lieferanten);
- die möglichen Empfänger der Daten, an die die Daten übermittelt werden;
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z.B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- Löschfristen;
- die Ansprüche des Betroffenen nach der DSGVO (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht, Datenübertragbarkeit);
- das Recht des Betroffenen auf Widerruf einer Einwilligung;
- das Recht des Betroffenen auf Beschwerde bei einer Datenschutzbehörde.

6. Weitere Schritte zur Datenschutzkonformität

Nach dem ersten „Maßnahmenpaket“ gibt es noch weitere Schritte zur Datenschutzkonformität, die ratsam erscheinen:

- Betroffenenrechte: Die DSGVO gibt dem Betroffenen eine Palette von Rechten an die Hand. In der Kanzlei sollte es daher klare Regeln geben, wie zu verfahren ist, wenn beispielsweise ein (früherer) Mandant sein gesetzliches Recht auf „Datenübertragbarkeit“ gem. Art. 20 DSGVO geltend macht und die Herausgabe aller Daten verlangt, die die Kanzlei über ihn gespeichert hat. Auch für andere Betroffenenrechte, wie etwa das Auskunftsrecht (Art. 15 DSGVO) oder das Recht auf Löschung (Art. 17 DSGVO) sollten kanzleiinterne Reglungen existieren.
- Meldepflichten: Jeder Datenschutzverstoß muss gem. Art. 33 DSGVO innerhalb von maximal 72 Stunden bei der zuständigen Datenschutzbehörde gemeldet werden. Verliert ein Mitarbeiter sein Dienst-Handy und befinden sich auf dem Handy personenbezogene Daten, muss geprüft werden, ob eine Meldepflicht in Betracht kommt. Der bloße Verstoß gegen die Meldepflicht kann ein Bußgeld nach sich ziehen. Interne Arbeitsanweisungen sollten festlegen, wie bei einer Datenpanne vorzugehen ist.
- Datenschutzrichtlinien: In kanzleiinternen Richtlinien sollten klare Regeln für die Datenverarbeitung aufgestellt werden mit dem Ziel des rechtskonformen Handelns. Art. 24 DSGVO legt die Erstellung derartiger Richtlinien nahe. Kanzleiinterne Richtlinien geben Mitarbeitern Orientierung, wenn es darum geht, Datenschutzverstöße, Datenpannen und Datenlecks zu vermeiden. Zugleich lässt sich durch Datenschutzrichtlinien gegenüber der Aufsichtsbehörde dokumentieren, dass die

Kanzlei die gesetzlichen Pflichten zur Vorsorge gegen Datenschutzverstöße ernstgenommen hat.

V. Ausblick: Professionalisierung der Datenverabeitung

Herausforderung: Jeder kann sich beschweren

Es wird nicht allzu lange dauern, bis es erste Berichte gibt über Datenschutzkontrollen und Datenpannen in Anwaltskanzleien. Spätestens wenn Mandanten oder Ex-Mandanten, Prozessgegner oder Querulanten, Mitarbeiter oder Ex-Mitarbeiter sich bei der Aufsichtsbehörde beschweren, muss die Kanzlei damit rechnen, dass die Behörde kritische Fragen stellt. Spätestens zu diesem Zeitpunkt sollte es ein vorzeigbares Verarbeitungsverzeichnis sowie Datenschutzinformationen und -richtlinien geben, die die Einhaltung des Datenschutzrechts dokumentieren.

Warum handeln? Jeder Schritt in die richtige Richtung führt zum Ziel

In der Kürze der Zeit bis zum Inkrafttreten der DSGVO wird man auf Perfektionismus verzichten müssen. Die Datenschutzbehörden werden Verständnis haben, wenn am 25. Mai 2018 nicht jeder Spiegelstrich des neuen Rechts in der Kanzlei umgesetzt ist. Es wäre jedoch leichtfertig, auf allzu viel Verständnis zu setzen. Die Datenschutzbehörden werden in Zukunft auf jede Beschwerde mit förmlichen Verfahren reagieren und auf grobe Gesetzesverstöße mit empfindlichen Bußgeldern reagieren.

[*] Das DAV-Merkblatt ist für die Mitglieder der Anwaltvereine von Rechtsanwalt Prof. Niko Härting (unter Mitwirkung seines DSGVO-Teams) erstellt worden. Für Fragen, Anmerkungen und Kritik: anwaltsblatt@anwaltverein.de.