Neues Datenschutzrecht: Wie bereiten sich Anwaltskanzleien richtig vor?

Der Zeitpunkt bis zum Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung rückt immer näher. Rechtsanwalt Prof. Niko Härting zeigt auf, was dies für die Anwaltschaft bedeutet und worauf Kanzleien in Zukunft besonders achten müssen.

Autor: Prof. Niko Härting

Am 25.5.2018 tritt die neue europäische Datenschutz-Grundverordnung (DSGVO) in Kraft. Von wenigen Ausnahmen abgesehen, gilt das neue Datenschutzrecht auch für Anwaltskanzleien. Bei Verstößen gegen das neue Recht drohen Bußgelder bis zu 20 Mio. EUR. Eine Übergangsfrist gibt es nach dem 25.5.2018 nicht. Höchste Zeit also, das Thema Datenschutz in der eigenen Kanzlei anzugehen. Viel Zeit bleibt nicht.

Datenschutz: Zukunftsthema auch in den Kanzleien

Dass das Datenschutzrecht nicht nur ein Beratungsthema für Mandanten ist, sondern die Kanzleien auch in eigener Sache betrifft, ist keineswegs neu. Allerdings war bislang umstritten, ob das Datenschutzrecht auch für mandatsbezogene Informationen gilt. Berufsrechtler und Datenschützer stritten darum, ob die Anwaltsakten für Aufsichtsbehörden tabu sind. Soweit es um die Daten des eigenen Personals oder auch um Marketingdaten ging, gab es nie einen Zweifel, dass das Datenschutzrecht auch für Anwaltskanzleien gilt. Auch betriebliche Datenschutzbeauftragte mussten schon nach bisherigem Recht bestellt werden, wenn mehr als neun Personen (Anwälte oder Personal) am Computer arbeiten.

Immer wieder standen Anwälte im Verdacht, allzu lax mit Daten umzugehen. So warf der schleswig-holsteinische Datenschützer Thilo Weichert der Anwaltschaft im Jahre 2009 in einem NJW-Beitrag vor, sich systematisch der Datenschutzkontrolle zu „entziehen". Bei der Beschreibung der (vermeintlichen) Drückeberger nannte Weichert Rechtsanwälte und Notare in einem Atemzug mit Geheimdiensten, Strafverfolgungs- und Finanzbehörden.

Es gab und gibt gute Gründe für eine gewisse Zurückhaltung der Anwaltschaft gegenüber den Datenschutzbehörden. Das Anwaltsgeheimnis ist ein hohes Gut, und Datenschutzbehörden sind staatliche Aufsichtsbehörden. Die staatliche Datenschutzaufsicht, die sich für Mandatsakten interessiert, kann zu einer Gefahr für das Anwaltsgeheimnis werden.

Die Berliner Datenschutzbehörde scheiterte 2010 vor dem Kammergericht mit ihren hartnäckigen, jahrelangen Bemühungen, einen renitenten Anwalt durch ein datenschutzrechtliches Auskunftsbegehren zu Angaben über die Herkunft von Informationen zu veranlassen. Das Kammergericht vertrat den Standpunkt, dass das Anwaltsgeheimnis Vorrang vor dem Datenschutzrecht hat. Der streitbare Anwalt verteidigte die berufsrechtliche Schweigepflicht erfolgreich gegen den langen Arm der Aufsichtsbehörde.

Die DSGVO gibt den Datenschutzbehörden neuen Aufwind. Wenn das neue Recht am 25.5.2018 in Kraft tritt, gilt es auch für Anwaltskanzleien. Viele Ausnahmen gibt es nicht. Doch immerhin hat der deutsche Gesetzgeber im neuen Bundesdatenschutzgesetz (BDSG), das gleichfalls am 25.5.2018 in Kraft tritt, von einigen Öffnungsklauseln der DSGVO zugunsten der Anwaltschaft Gebrauch gemacht. Zum einen gibt es Ausnahmen bei den Informations- und Auskunftspflichten, sodass es dabei bleibt, dass das Anwaltsgeheimnis gegen allzu große datenschutzrechtliche Neugier geschützt bleibt. Zum anderen sind Aufsichtsbehörden nicht befugt, gegen den Willen einer Anwaltskanzlei deren Räume zu betreten und Einblick in die elektronische Datenverarbeitung zu nehmen.

Dennoch stehen alle Kanzleien vor der Aufgabe, ihre Datenverarbeitungsprozesse auf das neue Recht umzustellen, da ansonsten hohe Bußgelder drohen.

Schritt 1: Bestellung eines betrieblichen Datenschutzbeauftragten

Sobald in einer Anwaltskanzlei mindestens zehn Personen ständig mit elektronischer Datenverarbeitung befasst sind, ist ein betrieblicher Datenschutzbeauftragter zu bestellen. Anwaltskanzleien, die bestellpflichtig sind, bislang aber keinen Datenschutzbeauftragten haben, sollten dies schnellstmöglich nachholen.

Ob und unter welchen Voraussetzungen ein Partner der Kanzlei zugleich betrieblicher Datenschutzbeauftragter sein kann, ist streitig. Unklar ist auch, ob ein IT-Leiter zum Datenschutzbeauftragten berufen werden kann. Optimal ist die Bestellung eines angestellten Anwalts oder eines anderen Mitarbeiters mit gewisser IT-Affinität. Auch die Bestellung eines externen Datenschutzbeauftragten ist möglich.

Für eine Datenschutzbehörde ist es eine sehr einfache Aufgabe zu überprüfen, ob eine Anwaltskanzlei einen Datenschutzbeauftragten bestellt hat. Dies gilt umso mehr, als der betriebliche Datenschutzbeauftragte in Zukunft in allen Datenschutzinformationen namhaft gemacht werden muss. Jede Anwaltskanzlei sollte daher bis zum 25.5.2018 prüfen, ob ein betrieblicher Datenschutzbeauftragter bestellt werden muss. Fällt die Auswahl einer geeigneten Person schwer, sollte die Kanzlei beachten, dass die Geeignetheit eines Datenschutzbeauftragten für die Behörde viel schwerer zu prüfen ist als dessen Bestellung. Besser ein schwach geeigneter Datenschutzbeauftragter als kein Datenschutzbeauftragter.

Schritt 2: Erstellung von Verfahrensverzeichnissen

Art. 30 DSGVO schreibt für jedes Datenverarbeitungsverfahren ein Verfahrensverzeichnis vor, sofern es sich um ein Verfahren handelt, das personenbezogene Daten umfasst. Als Verfahren gelten beispielsweise:

- die elektronische Anwaltsakte (Dokumentenmanagement-Systeme)
- die Kanzleisoftware (z.B. RA Micro oder Phantasy)
- elektronische Diktier- und Spracherkennungsprogramme
- die Buchhaltungssoftware
- die Software zur Versendung und Verwaltung von E-Mails

- Adressdatenbanken
- die Software zur Terminverwaltung
- die elektronischen Personalakten

Für die Verfahrensverzeichnisse ist keine bestimmte Form vorgeschrieben. Sie können somit als Word- oder Exceldatei geführt werden oder auch handschriftlich und müssen die Angaben enthalten, die Art. 30 DSGVO vorschreibt:

- den Namen und die Kontaktdaten der Kanzlei
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten
- 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, denen die Daten offengelegt worden sind oder noch offengelegt werden
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z.B. bei Cloud-Diensten);
- Löschfristen
- Maßnahmen der Datensicherheit, die nach Art. 32 DSGVO vorgeschrieben sind

Die Erstellung der Verfahrensverzeichnisse ist ein mühsamer Prozess, da es meist gar nicht so einfach ist, den Überblick darüber zu behalten, welche Datenverarbeitungsprozesse es in der Kanzlei gibt. Dies gilt umso mehr, wenn Partner und Mitarbeiter beruflich Smartphones, Tablets und Laptops ortsungebunden nutzen, sodass sich die Frage stellt, inwieweit Programme auf den Endgeräten gleichfalls als Datenverarbeitungsverfahren zählen, für die die Pflicht zur Führung eines Verfahrensverzeichnisses gilt.

Wenn erstmalig Verfahrensverzeichnisse angelegt werden, ist die 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 Verfahrensverzeichnisse angelegt werden, sollte dies Anlass sein, 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.

Schritt 3: „Gap Analysis"

Die Verfahrensverzeichnisse sind der Ausgangspunkt für eine „Lückensuche", die in den derzeitigen Bemühungen größerer Unternehmen um DSGVO-Konformität „Gap Analysis" genannt wird.

Jedes einzelne Verfahren muss in der „Gap Analysis" im Hinblick auf mögliche Schwachstellen überprüft werden. Zu diesen Schwachstellen zählen vor allem:

- Datensparsamkeit: Ist die Vorhaltung von Daten und deren Verarbeitung tatsächlich notwendig?
- Datenrichtigkeit: Ist gewährleistet, dass beispielsweise Adressdaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
- Rechtmäßigkeit: Lässt sich die Datenverarbeitung auf einen der Gründe des Art. 6 Abs. 1 DSGVO stützen? Dient die Datenverarbeitung der Vertragserfüllung? 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 jeweils gewährleistet?
- Zugriffsrechte: Haben ausschließlich Mitarbeiter Zugriff zu den Daten, die die Daten für ihre jeweiligen Aufgaben benötigen?
- Zugangskontrolle: Sind die Rechner in der Kanzlei ausreichend gegen den Zugang durch Unbefugte geschützt?

Am Ende jeder „Gap Analysis" steht ein Maßnahmenplan mit dem Ziel der möglichst umfassenden Datenschutzkonformität aller Verfahren, für die es ein Verfahrensverzeichnis gibt.

Schritt 4: Datensicherheit

Art. 32 DSGVO verpflichtet den Datenverarbeiter zur Datensicherheit. „Technische und organisatorische Maßnahmen" sind zu ergreifen, um die Sicherheit der in der Kanzlei verarbeiteten Personendaten zu gewährleisten.

Folgende Maßnahmen sind unter anderem 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.

Dokumentationspflichten werden in der gesamten DSGVO groß geschrieben. Dies gilt gerade auch für die „technischen und organisatorischen Maßnahmen" der Datensicherheit. Es sollte daher ein Papier geben, das die Bemühungen um solche Maßnahmen und deren Durchführung belegt.

Schritt 5: „Papierform"

Bei der Datenverarbeitung bedienen sich viele Kanzleien 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 schriftlicher Verträge bedurfte. Nach neuem Recht bleibt dies grundsätzlich so, allerdings werden Anpassungen an bestehenden Verträgen vorzunehmen sein. Sofern noch keine Verträge existieren, sollte ein Vertragsschluss vor dem 25.5.2018 nachgeholt werden.

Zum notwendigen „Paperwork" gehören auch Datenschutzinformationen. Die Informationspflichten sind nach neuem Datenschutzrecht wesentlich umfangreicher, als dies nach bisherigem Recht der Fall ist. Alle Datenschutzbestimmungen auf Kanzlei-Websites müssen überarbeitet werden. Zudem gelten die Informationspflichten nach neuem Recht nicht nur für Websites, sondern für jede Form der Datenverarbeitung. Daher empfehlen sich allgemeine „Hinweise zur Datenverarbeitung", die jeder Vergütungsvereinbarung beigefügt werden sollten. Dass sich entsprechende Formulare einbürgern werden, ist sicher.

Weitere Schritte

Selbst aus multinationalen Unternehmen, die mit Millionenbudgets an der DSGVO-Konformität arbeiten, ist zu hören, dass eine solche Konformität bei weitem nicht zu 100 Prozent erreicht werden wird. Dies ist naturgemäß bei mittelständischen und kleinen Kanzleien nicht anders. Dennoch gibt es auch nach den ersten fünf Schritten noch weitere Maßnahmen zur Datenschutz-Compliance, die realistisch und ratsam erscheinen:

- Betroffenenrechte: Neben dem Recht auf Information und den (durch das neue BDSG eingeschränkten) Auskunftsrechten gibt es noch weitere Betroffenenrechte, mit deren Geltendmachung gerechnet werden muss. In der Kanzlei sollte es klare Regeln geben, wie zu verfahren ist, wenn beispielsweise ein (früherer) Mandant sein gesetzliches Recht auf „Datenübertragbarkeit" nach Art. 20 DSGVO geltend macht und die Herausgabe aller Daten verlangt, die die Kanzlei über ihn gespeichert hat.
- Meldepflichten: Nach Art. 33 DSGVO muss jeder Datenschutzverstoß in Zukunft innerhalb von maximal 72 Stunden bei der zuständigen Datenschutzbehörde gemeldet werden. Auch wenn es für Anwälte nach dem neuen BDSG einige Ausnahmen von der Meldepflicht gibt, gilt die Meldepflicht grundsätzlich auch für Anwaltskanzleien. Verliert ein Mitarbeiter sein Dienst-Handy und befinden sich auf dem Handy personenbezogene Daten, kann dies zu einer Meldepflicht führen. Der bloße Verstoß gegen die Meldepflicht kann ein Bußgeld nach sich ziehen.
- Datenschutzrichtlinien: Nicht nur zum Umgang mit Datenschutzverstößen sind kanzleiinterne Richtlinien ratsam, die klare Regeln aufstellen zur Datenverarbeitung mit dem Ziel des rechtskonformen Handelns. Art. 24 DSGVO legt die Erstellung derartiger Richtlinien jedenfalls nahe.