Datenschutz in Kanzleien & Sozietäten

(Teil 1: Einführung)

In Gesprächen mit Anwälten, aber auch mit **Steuerberatern** trifft man häufig auf das Argument, die Regelungen des Bundesdatenschutzgesetz (BDSG) würden die Kanzlei oder den Anwalt nicht betreffen, da es eigene Regelungen zur Verschwiegenheit und Vertraulichkeit gäbe.

Personenbezogene Daten werden in jeder Anwaltskanzlei be- und verarbeitet. Hierbei ist das Bundesdatenschutzgesetz zu achten, auch wenn Anwälte zur anwaltlichen Verschwiegenheit verpflichtet sind und einseitig die Interessen des Mandanten wahrnehmen müssen. Dennoch haben Anwaltskanzleien Maßnahmen zum Schutz der personen- und mandatsbezogenen Daten im Interesse der Betroffenen schon aus berufsrechtlichen Gründen zu ergreifen.

Das Bundesdatenschutzgesetz sieht hier eindeutig vor, dass für Sachverhalte, die durch kein bereichsspezifisches Recht explizit geregelt werden, die (allgemeineren) Regelungen des Bundesdatenschutzgesetzes zum Tragen kommen. Dazu gehören insbesondere Punkte wie

- Verfahrensverzeichnisse
- Datenschutzregelungen
- Nutzungsrichtlinien
- IT Sicherheit
- Backup– und Recovery-Strategien
- Verschlüsselung und Signatur
- Bestellpflicht eines Datenschutzbeauftragten
- Auftragsdatenverarbeitung externe Dienstleister z.B. Fernwartung etc.

Die Brisanz des Themas, u.a. die mit Verstößen gegen das BDSG verbundenen Bußgeldrisiken hat der Deutsche Anwaltverein in seiner Depesche 2010–42 aufgegriffen und zusätzlich eine Checkliste mit Empfehlungen zur Umsetzung in der Kanzlei herausgegeben. Hierin verweist der DAV auf die Möglichkeit der Bestellung eines **externen Datenschutzbeauftragten**, aber auch auf die Inanspruchnahme eines **externen Datenschutzberaters** für die Sicherstellung der notwendigen Umsetzungen und Formulierungen.

Erhebung und Nutzung personenbezogener Daten

Die Analyse, welche Daten von wem, wann wo, wie, auf welchem Weg erhoben und genutzt werden, steht immer am Anfang. Mit Blick auf die anwaltliche Verpflichtung zur einseitigen Interessenwahrnehmung erfolgt die Erhebung per-sonenbezogener Daten des Gegners und anderer Beteiligter typischerweise nicht vorrangig beim Betroffenen selbst. Damit weicht er von den datenschutzrechtlichen Regelungen ab. Daher sind die Datenerhebungsvorgänge zu dokumentieren (z.B. durch Mandantenaufnahmebogen).
In einer Kanzlei verarbeitete Daten lassen sich in bestimmte Kategorien unterteilen und unterliegen dann jeweils anderen gesetzlichen Vorgaben: Mandatsbezogene Daten – Berufspflichten insbesondere nach §§ 43, 43 Absatz 2 BRAO und § 5 BORA, Mitarbeiterdaten – Arbeitnehmerdatenschutz § 32 BDSG, Lieferantendaten und Akquise-/Networking-Daten – Datenschutz nach BDSG ggf. mit weiteren Anforderungen für Telemediendienste nach dem TMG. Wenn möglich sind diese verschiedenen Datenkategorien getrennt voneinander zu speichern und zu verwalten.

Einsatz bedarfsgerechter IT-Lösungen mit regelmäßiger Statuskontrolle

Die Anforderung nach sach- und fachgerechten IT-Anwendungen ergibt sich sowohl aus dem Datenschutz als auch aus den Anforderungen an die Einrichtungen zur anwaltlichen Berufsausübung. Art und Umfang der geeigneten Ausstattung richten sich nach der Größe und dem verarbeiteten Datenvolumen der Anwaltskanzlei. Die Anforderungen an die Sicherheit ergeben sich aus dem konkreten Einsatz und insbesondere der Art der eingesetzten – insbesondere mobilen – Kommunikationslösungen sowie Zugriffsmöglichkeiten auf die gespeicherten Informationen. Selbstverständlich sind Spam- und Virenfilter, eine Firewall und ggf. weitere Sicherheitsvorkehrungen zu treffen, um sich vor Datenverlust und Beeinträchtigung der IT-Anwendungen zu schützen. Richtlinien zu technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage zu § 9 BDSG. Meist werden Anwaltskanzleien hier nicht mehr ohne professionelle auf sie zugeschnittene Unterstützung durch Berater auskommen.

Datensicherungskonzept und Archivierung einführen und kontrollieren

Datensicherung erfolgt schon im ureigenen Interesse der Anwaltskanzlei an der lückenlosen Verfügbarkeit des Datenbestandes als Arbeitsgrundlage. Dabei ist auch der Anwaltskanzlei eine externe Online-Datensicherungslösung ohne Verstoß gegen das Anwaltsgeheimnis gestattet, wenn Daten nur verschlüsselt übermittelt und abgelegt werden. Die lokale Lösung birgt oftmals das Risiko, dass die Datensicherung vergessen oder aber Datensicherungsdatenträger im Serverschrank verwahrt werden, so dass diese bei einem Kanzleibrand oder einer anderen Haverie mit vernichtet werden. Die Datensicherungsroutine sollte in jedem Fall täglich geprüft werden. Daneben steht die strukturierte Archivierung der Mandatsunterlagen sowie der Belege zu den Geschäftsvorfällen der Kanzlei im Rahmen der anwaltlichen und steuerlichen Dokumentationspflichten.

Einsatz der elektronischen Signatur und Verschlüsselung prüfen

Zur anwaltlichen Grundausstattung gehören regelmäßig die elektronische Signatur sowie die Möglichkeit mit den Beteiligten verschlüsselt zu kommunizieren. Die Kanzlei sollte technische Einrichtungen vorhalten, um der Anforderung der Mandanten nach authentifizierter und verschlüsselter elektronischer Kommunikation entsprechen zu können. Dieses können auch verschlüsselte Dateiablagesysteme sein, zu denen der Anwalt dem Mandanten den Zugriff auf seine Korrespondenz gewährt. Bei besonders anfälligen Übertragungswegen wie zum Beispiel WLAN hat der Anwalt auf hinreichende Verschlüsselung der Datenkommunikation zu achten, will er sich nicht dem Vorwurf der Verletzung des Anwaltsgeheimnisses aussetzen.

Datenschutzbeauftragten bestellen

Können in der Anwaltskanzlei oder in dem Steuerbüro mehr als neun Personen elektronisch Daten verarbeiten oder werden sensible Daten verwaltet, so ist ein Datenschutzbeauftragter zu bestellen. Dies ergibt sich zwingend, wenn diese Personen auch nicht mandatsbezogene Daten verarbeiten, aus den datenschutzrechtlichen Regelungen. Bei reiner mandatsbezogener Datenverarbeitung empfiehlt sich die Ernennung eines Datenschutzbeauftragten. Dabei kann die Anwaltskanzlei einen internen Angestellten, **nicht** die Inhaber der Kanzlei oder den IT-Beauftragten, oder aber einen externen Dritten beauftragen. Bei der Bestellung eines Mitarbeiters der Kanzlei bietet es sich an, diesem ein Budget für Beratung zu technischen Fragen frei zu geben und diesen zu entsprechenden Schulungen frei zu stellen, denn das BDSG fordert zwingend einen Datenschutzbeauftragten, der fachlich qualifiziert ist!.

Zulässigkeit und Rahmenbedingungen der externen IT-Lösungen prüfen

Bei der Beauftragung von IT-Leistungen, bei denen personen- und/oder mandatsbezogene Daten außerhalb der Kanzlei verarbeitet werden, ist zu prüfen, ob die Voraussetzungen des § 11 BDSG an die Auftragsdatenverarbeitung erfüllt und ferner das Anwaltsgeheimnis gewahrt ist. Hierzu gehört auch die Fernwartung der Systeme, welche in jedem Fall nur auf vorherige Freigabe im Einzelfall durch die Kanzlei erfolgen darf.

Vertraulichkeits- und Geheimhaltungsvereinbarungen

Anwälte und Steuerberater sind wie Wirtschaftsprüfer generell verpflichtet, ihre Mitarbeiter und sonstigen Personen, welche sie bei der Ausübung ihres Berufes unterstützen ausdrücklich auf die Verschwiegenheit zu verpflichten. Dies gilt selbstverständlich auch für die Dienstleister, welche die Kanzlei/Sozietät in IT-Fragen unterstützen. Dabei ist für den Anwalt und Steuerberater oder Wirtschaftsprüfer wichtig zu wissen, dass er damit nicht aus der Verantwortung entlassen ist, sondern weiterhin die Zuverlässigkeit des Dienstleisters zu überwachen hat.

Teil 2: Datensicherheit
Teil 3: Datensicherung
Teil 4: Strategien zu Datenschutz und -Sicherheit

Wenn Sie an diesen oder weiteren Themen interessiert sind, mailen Sie uns. Wir nehmen Sie gerne in den Verteiler auf.

H.-Hubert Brenner
Kanutenstr. 7
41472 Neuss
Deutschland

+49.2131.745885 (T)
+49.2131.745887 (F)
+49.175.5690687 (M)
info@ehcon.org (eM)