DeutscherAnwaltVerein

Datenschutz-Checkliste für die Anwaltskanzlei

In jeder Anwaltskanzlei werden personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes verarbeitet. Ungeachtet der nach wie vor ungeklärten Frage des Verhältnisses des Datenschutzrechtes zur anwaltlichen Verschwiegenheit und der Verpflichtung zur einseitigen Wahrnehmung der Interessen des Mandanten haben Anwaltskanzleien Maßnahmen zum Schutz dieser personen- und mandatsbezogenen Daten im Interesse der Betroffenen schon auf Basis der berufsrechtlichen Rahmenbedingungen zu ergreifen.

1. Erhebung und Nutzung von personenbezogenen Daten

An den Anfang ist eine Analyse zu stellen darüber, welche Daten von wem auf welchem Weg erhoben und genutzt werden. Dabei erfolgt im Hinblick auf die anwaltliche Verpflichtung zur einseitigen Interessenwahrnehmung abweichend von den datenschutzrechtlichen Regelungen die Erhebung personenbezogener Daten des Gegners und anderer Beteiligter typischerweise nicht vorrangig beim Betroffenen selbst. Die Datenerhebungsvorgänge sind zum Beispiel durch Mandantenaufnahmebogen zu dokumentieren. In der Kanzlei verarbeitete Daten lassen sich regelmäßig in folgende Kategorien unterscheiden und unterliegen 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.

2. Datenschutzregelungen aufstellen und Sensibilität schaffen

Dem Datenschutz liegen folgende Prinzipien zugrunde:

- Verbot mit Erlaubnisvorbehalt: Nur dem BDSG vorrangige Rechtsvorschriften oder die – auch konkludente – Einwilligung der Betroffenen rechtfertigen die Erhebung und Verarbeitung personenbezogener Daten

- Zweckbindung: Die Erhebung, Speicherung, Verarbeitung und Nutzung personenbezogener Daten muss an einen konkreten Zweck gebunden sein. Die Daten dürfen nicht anderweitig verwandt werden.

- Datenvermeidung und Datensparsamkeit: Daten dürfen nur erhoben und verarbeitet werden, soweit dies für den gerechtfertigten/eingewilligten Zweck unbedingt erforderlich ist.

- Transparenz und Meldepflicht: Die Kanzlei muss namhaft und für die Datenverarbeitung verantwortlich gemacht werden können.

- Datensicherheit: Die Daten sind insbesondere vor Verlust, Verfälschung oder unerlaubter Kenntnisnahme zu schützen.

An diesen Prinzipien kann sich der Datenschutz in der Anwaltskanzlei orientieren, wobei die Transparenz und die Meldepflicht zugunsten des besonderen Vertrauensverhältnisses im Mandatsverhältnis nur eingeschränkt gelten. Es bietet sich an interne Datenschutzregeln aufzustellen und bei Erhebung von Daten auf die elektronische Verarbeitung hinzuweisen. Werden Daten über die Internetseite der Anwaltskanzlei erhoben, ist eine Daten-

schutzerklärung erforderlich. In jeder Kanzlei empfiehlt sich eine Datenschutzschulung durch externe Berater. Die Datenschutzschulung sollte auch umfassen, wie sich die Mitarbeiter bei der Anfrage einer Aufsichtsstelle (Datenschutzbeauftragter des Landes, zuständige Rechtsanwaltskammer) und bei Auskunfts- und Löschungsbegehren von Betroffenen zu verhalten haben.

3. 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.

4. 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.

5. 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.

6. Datenschutzbeauftragten bestellen

Können in der Anwaltskanzlei mehr als neun Personen elektronisch Daten verarbeiten, 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.

7. 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.

8. Vertraulichkeits- und Geheimhaltungs-vereinbarungen

Anwälte sind 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 in IT-Fragen unterstützt. Dabei ist für den Anwalt wichtig zu wissen, dass er damit nicht aus der Verantwortung entlassen ist, sondern weiterhin die Zuverlässigkeit des Dienstleisters zu überwachen hat.

Weiterführende Links:

- www.davit.de: Grundregeln der Anwaltschaft in der Informationsgesellschaft für Informationstechnik und Telekommunikation
- www.bsi.bund.de: IT-Grundschutzhandbuch
- www.bfdi.bund.de: Materialien zum Datenschutz
- www.datenschutzzentrum.de: Arbeitshilfen zum Datenschutz
- www.gdd.de: Download-Muster zur Auftragsdatenverarbeitung

Stand: August 2010