Rechtsanwalt Dr. Arnd-Christian Kulow, Stuttgart

>> BERUFSRECHT

Datenschutz in der Kanzlei nach der Datenschutzgrundverordnung

Von Rechtsanwalt Dr. Arnd-Christian Kulow, Stuttgart, zert. Datenschutzbeauftragter (TÜV-SÜD), Zert. Datenschutz-Auditor (TÜV-SÜD), zert. Beauftragter für Qualitätsmanagement nach DIN EN ISO 9001:2015 (QM-B) (TÜV-SÜD), zert. Programmierer (SGD)

A. Neues Datenschutzrecht ab 25.5.2018 – Wichtige Änderungen auch für Kanzleien

Ab 25.05.2018 gilt ein neues, europäisches Datenschutzrecht. Die Verordnung (EU) 2016/679 „Datenschutzgrundverordnung" (DSGVO) wird dann – ohne weitere Übergangsfrist – für die gesamte Europäische Union gelten. Als EU-Verordnung ist sie in den EU-Mitgliedstaaten unmittelbar, d. h. ohne weitere nationale Umsetzungsakte anwendbar. Die DSGVO besteht aus 99 Artikeln und 173 Begründungserwägungen. Letztere können zur Erläuterung der Normen herangezogen werden. Der europäische Datenschutz wurde bisher von der Richtlinie 95/46/EG gesteuert. Diese musste von den Mitgliedstaaten in nationales Recht umgesetzt werden. Mit der DSGVO soll nun der Datenschutz in der EU deutlich stärker vereinheitlicht werden als bisher. Ob die Verordnung dies erreichen kann und wird, darüber gehen die Meinungen stark auseinander.

Die Anforderungen an Kanzleien beim Umgang mit personenbezogenen Daten werden sich durch die Geltung der DSGVO sehr deutlich und spürbar ändern. Eine unrechtmäßige Verarbeitung personenbezogener Daten ist mit hohen Bußgeldsanktionen bedroht. Ferner verpflichtet die DSGVO die Kanzleien zu umfangreichen Nachweisen, die durch entsprechend umfassende Dokumentationen zu führen sind.

Gleichzeitig wird der deutsche Gesetzgeber durch viele Öffnungsklauseln und konkretisierungsbedürftige Normen zum „Ko-Regulierer" des europäischen Datenschutzrechts. Dies eröffnet andererseits auch berufspolitische Handlungsmöglichkeiten.

B. Anwendbarkeit des Datenschutzrechts auf Kanzleien?

Rechtsanwälte und Rechtsanwältinnen sind Berufsgeheimnisträger (§ 43a Abs. 2 BRAO, § 2 BORA, § 203 StGB, §§ 53, 53a StPO, § 97 StPO [Beschlagnahmeverbot], 2.3 CCBE). In der Vergangenheit wurde immer wieder die Frage thematisiert, ob angesichts solcher umfassenden Verpflichtungen zur Verschwiegenheit, das Datenschutzrecht überhaupt auf Anwaltskanzleien anwendbar ist und diese einer Kontrolle durch die Datenschutzbehörden unterliegen. Die Diskussion hat verdeutlicht, dass das Mandatsgeheimnis und der Datenschutz nicht deckungsgleich sind, mithin andere Ziele und Inhalte haben. Im Ergebnis wird das Datenschutzrecht grundsätzlich für anwendbar gehalten, allerdings geht das Mandatsgeheimnis im Konfliktfall vor.

Dies bekräftigt ab 25.5.2018 der dann anwendbare § 1 Abs. 2 Satz 3 BDSG neue Fassung: *„Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt."*

Damit ist das europäische Datenschutzrecht gleichwohl grundsätzlich anwendbar, die allgemeinen Datenschutzbehörden sind auch grundsätzlich prüfberechtigt, bei Konflikten von Datenschutz mit Mandatsgeheimnis – z. B. bei einigen Informations- und Auskunftspflichten – geht allerdings Letzteres vor („bleibt unberührt").

C. Gilt die DSGVO in der Kanzlei nur für elektronische Verarbeitungen?

Die DSGVO gilt – technikneutral – sowohl für den „Server" als auch für den „Aktenschrank". Personenbezogene Daten sind dabei alle Informationen die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Darunter fallen selbstverständlich die Mandantendaten, aber auch die Daten Dritter, Beschäftigtendaten, Lieferantendaten usw. Unter einer Verarbeitung versteht die DSGVO jeglichen Umgang mit personenbezogenen Daten im weitesten Sinn. Darunter fällt daher das Erfassen von Mandantendaten, das Ordnen, Abfragen, Löschen usw. Es bleibt festzuhalten, dass jegliche Datenverarbeitung von personenbezogenen Daten in der Kanzlei von der DSGVO erfasst wird. Ausgenommen werden lediglich Verarbeitungen zu rein privaten Zwecken oder solche außerhalb von – medienneutral zu verstehenden– „Dateisystemen" d. h., ungeordnete Sammlungen.

D. Pflichten der Verantwortlichen in den Kanzleien

Die Struktur der DSGVO legt es nahe, zwischen dem alltäglichen „Regelbetrieb", der „Sicherstellung der Beachtung von Betroffenenrechten" (z. B. Auskunft, Information, Berichtigung etc.) und den „Spezialthemen" wie der ggf. notwendigen Bestellung eines Datenschutzbeauftragten, der Auftragsverarbeitung, den Pflichten bei einem Datenschutzvorfall etc. zu unterscheiden.

I. Pflichten im „Regelbetrieb“

Nach Art. 6 Abs. 1 DSGVO muss die Verarbeitung personenbezogener Daten „rechtmäßig“ sein. Das ist kein großer Unterschied zur bisherigen Rechtslage. Eine rechtmäßige Verarbeitung (also z. B. das Erfassen von Mandantendaten in einem Fragebogen) bedeutet zunächst, dass der **Vorbehalt des Gesetzes** zu beachten ist. In die Verarbeitung personenbezogener Daten natürlicher, lebender Personen durch andere muss wirksam eingewilligt werden oder es muss ein formelles Gesetz die Verarbeitung legitimieren.

Art. 6 Abs. 1 DSGVO hält daher einen Katalog von Verarbeitungszwecken bereit, die z.B. die Ersterfassung und Speicherung von Mandantendaten rechtmäßig machen. So liegt sicher im Ausfüllen eines entsprechenden Fragebogens eine Einwilligung des Mandanten nach Art. 6 Abs. 1 Satz 1 lit. a) vor. Gleichzeitig dient die Verarbeitung aber auch der Erfüllung des Mandatsvertrages, gerechtfertigt durch Art. 6 Abs. 1 Satz 1 lit. b).

Art. 5 Abs. 2 DSGVO postuliert zudem eine „Rechenschaftspflicht“. Diese verpflichtet die Verantwortlichen – also diejenigen, die über Mittel und Zweck der Verarbeitung entscheiden (Art. 4 Nr. 7 DSGVO) – in den Kanzleien den abstrakt formulierten Grundsatzkatalog (u.a. die Grundsätze der „Zweckbindung“, „Vertraulichkeit“ oder auch der „Integrität“ der Daten) aus Art. 5 Abs. 1 DSGVO bei den Abläufen in der Kanzlei zu beachten, umzusetzen und die wirksame Umsetzung auch umfassend zu dokumentieren.

Dies bringt für die Verantwortlichen deutlich erweiterte Organisations-, Informations-, Konzeptions- und weitreichende Dokumentationspflichten mit sich. Die DSGVO selbst äußert sich zur konkreten Umsetzung der neuen Pflichten nicht. Im Gegenteil: Aufgrund vieler „weicher Formulierungen“ der DSGVO besteht derzeit große Unsicherheit welche Pflichten wie ganz konkret im Kanzleialltag umgesetzt und jeweils dokumentiert werden müssen.

II. „Sicherstellung der Beachtung von Betroffenenrechten“

Die DSGVO sieht umfassende Auskunfts-, Berichtigungs-, Löschungs- und Widerspruchsrechte vor. Vor allem diese bergen ein Konfliktpotential im Bezug auf das Mandatsgeheimnis. Wenn ein Mandant bspw. den Namen und die Adresse eines Dritten angibt, so besteht nach Art. 14 DSGVO diesem gegenüber grundsätzlich eine Informationspflicht. Dies konterkariert offensichtlich das Mandatsgeheimnis. Zwar räumt die DSGVO z.B. in Art. 14 Abs. 5 lit. d) den Mitgliedstaaten die Möglichkeit ein, hier Regelungen zur Wahrung des Berufsgeheimnisses zu erlassen (z. B. § 29 Abs. 2, 3, § 33 Abs. 1 Nr. 2 lit. a) BDSG neue Fassung postulieren hier insoweit Ausnahmen).

Andere Regelungen der DSGVO, wie z. B. das neue Recht auf „Datenübertragbarkeit“ (Art. 20 DSGVO) sehen solche Anpassungsregelungen durch die Mitgliedstaaten nicht vor, werfen aber, was die konkrete Umsetzung im Kanzleialltag angeht, erhebliche Fragen auf.

III. „Spezialthemen“ (Datenschutzbeauftragter, Auftragsverarbeitung, Datenschutzvorfall, ...)

Über das bisher Gesagte hinaus gibt es auch für die Kanzleien nicht wenige „Spezialthemen“, die ebenfalls zu bearbeiten sind. So besteht nach dem BDSG nF die Pflicht, ab 10 ständig mit Verarbeitungen beschäftigten Mitarbeitern einen Datenschutzbeauftragten zu bestellen. Wird etwa die Buchhaltung der Kanzlei extern erledigt, so muss ein Vertrag über diese Auftragsverarbeitung geschlossen werden. Zusätzlich sind Vorgehensweisen für den Fall von Datenunfällen zu dokumentieren.

E. Lösungsstrategien für Kanzleien

Die Kanzleien müssen also prinzipiell ein umfassenderes, konzeptgesteuertes Bild vom Datenschutz entwickeln. Darauf aufbauend kann dann die notwendige Doku-

mentation in Angriff genommen werden. Derzeit werden generische – selbstkonzipierte – Ansätze vorgeschlagen und solche, die auf Standards der International Standardisation Organisation (ISO) basieren, wie z. B. die ISO 27001 zur Datensicherheit.

Um die spezifischen Pflichten aus Art. 5 Abs. 2 DSGVO zum Nachweis der Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO zu erfüllen, bedarf es jedoch der Betrachtung eines weiteren Konzepts. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSKB) hat mit dem Standard-Datenschutzmodell (SDM) ein gut handhabbares und verstehbares Datenschutzmodell entwickelt. Dessen Stärke besteht in der vollständigen Erfassung und Abbildung der nach Art. 5 Abs. 2 DSGV nachweislich einhaltbaren Verarbeitungsgrundsätze der DSGVO.

F. Zu einem basalen Datenschutzkonzept in vier Schritten

Die konkrete Form des Datenschutzkonzepts und der Dokumentation hängt entscheidend von Art und Umfang der Verarbeitungsprozesse in der Kanzlei ab. Grundsätzlich empfiehlt es sich, folgende Schritte durchzugehen und zu dokumentieren. Dabei ist die Erstellung von zwei Dokumenten anzuraten: einer „Datenschutzleitlinie“ und eines „Datenschutz-Handbuchs“.

I. Die Datenschutzleitlinie: Datenschutzziele und Aufbau der Kanzlei in Bezug auf den Datenschutz

Die Datenschutzleitlinie stellt ein schriftliches Bekenntnis der Kanzleiführung zur Umsetzung der Datenschutzziele dar. Es beschreibt abstrahierend u. a. die Datenschutzziele der Kanzlei, den Aufbau der Kanzlei und die Form der konkreten Umsetzung.

II. Das Datenschutz-Handbuch

Das Datenschutz-Handbuch dokumentiert u. a. die personenbezogenen Verfahren und zeigt die eingesetzten Maßnahmen zur Einhaltung des Datenschutzes auf. Nach dem SDM sind dies vier zu dokumentierende Schritte:

1. Feststellen und Dokumentieren personenbezogener Verfahren

Hier hilft die einfache Orientierungsfrage: Wer verarbeitet in der Kanzlei, für welche Zwecke, was für Arten von personenbezogenen Daten.

2. Zuordnen der Erlaubnistatbestände (z. B. Art. 6 Abs. 1 DSGVO)

Hier geht es um die materiell-rechtliche Bewertung, ob ein oder mehrere Erlaubnistatbestände – vornehmlich aus Art. 6 Abs. 1 DSGVO – vorliegen. Immer bezogen auf die jeweils im ersten Schritt festgestellten personenbezogenen Verfahren.

3. Schutzbedarf für Daten, Systeme und Prozesse

Das Standard-Datenschutzmodell trennt bei einem personenbezogenen Verfahren die Komponenten „Daten“, „Systeme“ (also die „Server“ oder „Aktenschränke“) und die Prozesse im engeren Sinn. Für alle drei Komponenten muss jeweils der Schutzbedarf bezüglich jedes der Gewährleistungsziele (abgeleitet aus Art. 5 Abs. 1 DSGVO) bestimmt werden. Dieser Schritt stellt die Einhaltung der Schutzziele des Art. 5 Abs. 1 DSGVO sicher. Dieser Schritt muss ebenfalls dokumentiert werden.

4. Maßnahmen zur Gewährleistung der Einhaltung der Ziele des Datenschutzes

In diesem vierten und letzten Schritt werden die jeweils getroffenen Maßnahmen bezüglich der drei Komponenten der personenbezogenen Verfahren dokumentiert. Dieser Schritt ist gleichzeitig Bestandteil des Datenschutzmanagements. Es verwirklicht die notwendigen technischorganisatorischen Schutzmaßnahmen. Der Vorteil am Standard-Datenschutzmodell ist, dass hier für die verschiedenen Komponenten (Daten, Systeme, Prozesse) Referenzmaßnahmen angeboten werden. In der Dokumentation ist auch auf die Wirksamkeit der Maßnahmen einzugehen.

G. Schlussbemerkungen

Der ab 25.05.2018 auch von den Kanzleien geforderte „konzeptionelle Datenschutz“ verpflichtet zu umfassender Betrachtung aller personenbezogenen Verfahren nebst umfangreicher Dokumentation.

Es besteht aber auch berufspolitischer Handlungsbedarf. Viele Vorgaben der DSGVO – insbesondere bei den Betroffenenrechten, z. B. die Frage der Datenportabilität, Art. 20 DSGV – drohen die anwaltliche Praxis zu beeinträchtigen.

Wegen der überragenden Bedeutung des Mandatsgeheimnisses, auch für die rechtsstaatliche Rechtspflege, hat namentlich die Bundesrechtsanwaltskammer die gesetzliche Verankerung eines eigenen Datenschutzbeauftragten für die Anwaltschaft gefordert. Der Gesetzgeber ist dem indes nicht gefolgt.

Um so wichtiger ist es nun, den ganz konkreten Inhalt und den Umfang des anwaltlichen Mandatsgeheimnisses (auch im Verhältnis zu anderen vergleichbaren Berufsgeheimnissen wie z. B. der ärztlichen Schweigepflicht) zu präzisieren und mit den derzeitigen datenschutzrechtlichen Vorgaben abzugleichen. Dies dient vor allem dazu, einen entsprechenden Forderungskatalog für den deutschen Gesetzgeber zu formulieren. Auf europäischer Ebene ist auch an die Ausarbeitung von Verhaltensregeln nach Art. 40 DSGVO zu denken. Zwar können durch eine datenschutzrechtliche „regulierte Selbstregulierung“ die Pflichten der DSGVO weder quantitativ noch qualitativ vermindert werden, gleichwohl könnte aber das Pflichtenprogramm zumindest einigermaßen haftungssicher konkretisiert werden. Auch das wäre ein Vorteil. Die Anwaltschaft sollte, so oder so, das sich gerade entfaltende europäische Datenschutzrecht jedenfalls deutlich mitprägen. □