Kanzlei & Mandat

Rechtsanwalt Dr. Bernd Schmidt*

Datenschutz-Organisation und -Dokumentation in der Anwaltskanzlei

I. Einleitung

Am 25.5.2018 treten die Datenschutz-Grundverordnung (DS-GVO) und das neue Bundesdatenschutzgesetz (BDSG-neu) in Kraft. Während vielerorts Aktivität zur Anpassung der Datenschutz-Organisation herrscht, ist das Gros der Anwaltschaft noch tiefenentspannt. Der Beitrag zeigt auf, was für die Kanzleien auf der Zielgeraden noch zu tun ist.

II. Gründe für den Aufbau einer Datenschutz-Organisation

Kanzleien sind kein datenschutzfreier Raum. Im Gegenteil. Anwälte müssen wie jeder andere Verantwortliche das Datenschutzrecht beachten (dazu *Kazemi*, NJW 2018, 443) und Maßnahmen zu dessen Einhaltung treffen (*Härting*, Mitteilungen der Rechtsanwaltskammer München 2017, 7). Darüber hinaus gelten für Anwälte besondere Pflichten zum Schutz des Mandantengeheimnisses gem. §§ 43 a II BRAO iVm § 2 BORA. Verstöße gegen diese Pflicht zur Wahrung des Mandantengeheimnisses sind bekanntlich strafbewehrt.

Wie andere Verantwortliche unterliegen auch Kanzleien der Datenschutzaufsicht durch die (Datenschutz-)Aufsichtsbehörden (*Kazemi*, NJW 2018, 443 [445]). Diese Zuständigkeit wird nicht durch die Zuständigkeit der Kammern für die Aufsicht über das Standesrecht ausgeschlossen. Die Aufsichtsbehörden sind gem. Art. 55 DS-GVO für die Durchsetzung des Datenschutzrechts zuständig und können Informationen über die Verarbeitung personenbezogener Daten durch Verantwortliche in ihrer Zuständigkeit anfordern und Untersuchungen durchführen (Art. 58 I Buchst. a, b, e und f DS-GVO), Verantwortliche und Auftragsverarbeiter verwarnen (Art. 58 II Buchst. b DS-GVO) und Anweisungen zur Gestaltung von Prozessen zur Verarbeitung personenbezogener Daten treffen und durchsetzen bis zu deren Verbot (Art. 58 II Buchst. f DS-GVO).

Am meisten gefürchtet ist die Zuständigkeit für die Verhängung von Bußgeldern von bis zu 20 Euro Mio. oder 4 % des weltweiten Jahresumsatzes pro Datenschutzverstoß. Datenschutz-Compliance wird damit zum wirtschaftlichen Risikofaktor für Kanzleien jeder Größenordnung (dazu *Faust/Spittka/Wybitul*, ZD 2016, 120). Neben diesen direkten Sanktionen sollte aber auch die hohe Sensitivität der Öffentlichkeit für das Datenschutzrecht und die möglichen Reputationsverluste bei einem „Datenskandal“ in Betracht gezogen werden.

Es gibt also gute Gründe, im Rahmen der allgemeinen Sorgfaltspflicht (dazu *Schmidt*, Compliance in Kapitalgesellschaften, 2010, 23 ff.), der allgemeinen Compliance-Pflicht (dazu *Thode*, CR 2016, 714) und dem Risikomanagement Maßnahmen zu treffen, um die Einhaltung des Datenschutzrechts in der Kanzlei sicherzustellen, also eine Datenschutz-Organisation aufzubauen (dazu III). Mit Art. 5 II DS-GVO wird zudem der Grundsatz der Rechenschaft eingeführt, so dass Maßnahmen der Datenschutz-Organisation im Allgemeinen und der Einhaltung datenschutzrechtlicher Pflichten im Besonderen angemessen zu dokumentieren sind (dazu IV).

III. Aufbau der Datenschutz-Organisation

Mit deutscher Brille betrachtet sind die Neuerungen der DS-GVO mehr Evolution als Revolution (*Kühling/Martini*, EuZW 2016, 448 [454]), so dass im Grundsatz gilt: Wer bisher alles richtig gemacht hat, wird keine Mühe haben, seine Datenschutz-Organisation auf die DS-GVO umzustellen (so auch *Hamann*, BB 2017, 1090 [1092]). Das ist aber meist nicht der Fall, vielmehr werden angesichts der Auseinandersetzung mit den mutmaßlich neuen Anforderungen der DS-GVO schon lange bestehende Defizite offenbar. Mit entsprechenden rechtlichen und wirtschaftlichen Risiken muss im Rahmen allgemeiner Sorgfaltspflichten bewusst umgegangen und sichergestellt werden, dass (datenschutz-) rechtliche Pflichten in der Kanzlei befolgt werden.

Das Datenschutzrecht dient dem Schutz der informationellen Selbstbestimmung im Verständnis der deutschen Grundrechtsdogmatik (dazu *Pötters* in *Gola*, DS-GVO, Art. 1 Rn. 8) sowie dem Schutz des Grundrechts auf Datenschutz nach Art. 8 GRCh. Damit verbundene Anforderungen sind hoch. Der Anspruch für den Aufbau einer Datenschutz-Organisation sollte sein, zügig einen angemessenen und vertretbaren Datenschutz-Standard zu erreichen und dann kontinuierlich zu verbessern.

> Wie für andere Compliance-Themen empfiehlt sich auch für den Aufbau der Datenschutz-Organisation oder die Datenschutz-Compliance der P-D-C-A-Zyklus (Plan-Do-Check-Act) als Prozessstruktur (anschaulich dazu *Lepperhoff*, RDV 2016, 197 [199 ff.]). Sich kontinuierlich wiederholende Schritte der Datenschutz-Organisation sollten daher sein
> - die Analyse und Dokumentation des Status quo mit bestehenden Defiziten (1),
> - die anschließende Festlegung und Umsetzung von Maßnahmen zu deren Behebung oder Verringerung (2) sowie
> - die Kontrolle des Umsetzungsstands (3).

Dieser Gedanke kontinuierlicher Auditierung und Verbesserung findet sich in der DS-GVO ausdrücklich für den Bereich des technisch-organisatorischen Datenschutzes in Art. 32 I Buchst. d DS-GVO.

Um bewusst mit datenschutzrechtlichen Risiken umgehen zu können, müssen diese transparent gemacht werden. Hierfür ist es erforderlich, sämtliche Prozesse der Verarbeitung personenbezogener Daten auf den Prüfstand zu stellen und zum Gegenstand interner oder externer Auditierung zu machen. Dabei sollten existierende Datenschutz-Dokumentationen, die Verarbeitungsprozesse, vertragliche Dokumentationen, technische Gegebenheiten, aber auch das Bewusstsein der Beschäftigten erfasst und bewertet werden. Welchen Umfang diese Auditierung haben muss, hängt von Faktoren wie der Größe und Organisationsstruktur ab. Die Bürogemeinschaft

* Der Autor ist Rechtsanwalt in Hamburg.

mit wenigen Berufsträgern wird dabei möglicherweise mit einem Selbstcheck alle relevanten Fakten erfassen und bewerten können, während die internationale Großkanzlei naturgemäß einen größeren Aufwand betreiben muss, um angemessene Risikotransparenz zu schaffen.

Typisches Ergebnis eines Datenschutz-Audits ist, dass es erheblichen Handlungsbedarf gibt. Die materiellen Rechtspflichten des Datenschutzrechts im Allgemeinen und der DS-GVO im Besonderen können hier nicht abschließend dargestellt werden. Klassische Ergebnisse sind aber

- fehlende dokumentierte Einwilligungen für werbliche Ansprache (Art. 7 DS-GVO),
- fehlende Prozesse zur Information von Betroffenen über die Verarbeitung ihrer personenbezogenen Daten (Art. 13 DS-GVO),
- fehlende Prozesse und Konzepte zur Löschung personenbezogener Daten (Art. 17 DS-GVO),
- fehlende oder nicht aktualisierte Vereinbarungen zur Auftragsverarbeitung und fehlende Dienstleisterprüfungen (Art. 28 DS-GVO),
- fehlende Verzeichnisse von Verarbeitungstätigkeiten (Art. 30 DS-GVO),
- fehlende Dokumentation technisch-organisatorischer Maßnahmen (Art. 32 DS-GVO),
- fehlende Prozesse zur Datenschutzfolgenabschätzung (Art. 35 DS-GVO),
- fehlende Bestellung eines Datenschutzbeauftragten oder dessen Meldung an die Aufsichtsbehörde (Art. 37 DS-GVO, § 38 BDSG).

Da es also in der Regel jede Menge zu tun gibt, müssen Maßnahmen priorisiert werden. Dabei gibt es kein absolut richtiges oder falsches Vorgehen. Jede Maßnahme, die zur Verringerung datenschutzrechtlicher Risiken beiträgt, ist hilfreich. Allgemein zweckmäßig und zu empfehlen ist aber ein Vorgehen, bei dem leicht erkennbare Defizite vor weniger offensichtlichen Defiziten abgestellt werden sowie strukturelle Aufgaben und Maßnahmen in Bereichen verstärkter Aktivität der Aufsichtsbehörden priorisiert werden.

So empfiehlt es sich etwa,

- die Datenschutzerklärung der Webseite,
- die Meldung des Datenschutzbeauftragten an die Aufsichtsbehörde,
- Konzepte zum internationalen Datentransfer,
- Prozesse zur Auswahl und datenschutzkonformen Beauftragung von Dienstleistern,
- die Datenschutz-Dokumentation,
- die vertragliche Verpflichtung von Dienstleistern gem. Art. 28 DS-GVO und
- die Verpflichtung von Mitarbeitern zum Datenschutz

zu priorisieren. Lassen sich mit geringem Aufwand „Quick-Wins“ erzielen, sollte diese Chance natürlich unbedingt genutzt werden.

IV. Rechenschaftspflicht und Datenschutzdokumentation

Mit Art. 5 II DS-GVO wird der Grundsatz der Rechenschaftspflicht eingeführt. Eine scheinbar kleine Neuerung, die jedoch erheblich Auswirkung auf jeden Verantwortlichen im Anwendungsbereich der DS-GVO hat (so auch *Veil*, ZD 2018, 9; *Hamann*, BB 2017, 1090 [1092]). Anders als bisher reicht es nicht mehr, alles richtig zu machen, man muss es darüber hinaus jederzeit nachweisen können. Damit werden die aktuellen Anforderungen an die Datenschutz-Organisation deutlich verschärft. Die Anwälte müssen sich daher Gedanken über eine angemessene Dokumentation ihrer Datenschutz-Organisation und der Prozesse zur Verarbeitung personenbezogener Daten machen.

Wie eine DS-GVO-konforme Datenschutz-Dokumentation auszusehen hat, ergibt sich nicht unmittelbar aus dem Gesetz. Im Sinne einer Pflichtdokumentation findet sich in Art. 30 DS-GVO lediglich das Verzeichnis von Verarbeitungstätigkeiten, welches jedenfalls Verantwortliche mit über 250 Mitarbeitern führen müssen. Dies ist nur für eine überschaubare Anzahl der deutschen Kanzleien der Fall, aber auch wenn Verarbeitungen ein Risiko für die Rechte und Freiheiten der Betroffenen bergen, besondere Kategorien personenbezogener Daten verarbeitet werden oder Informationen zu strafrechtlichen Verurteilungen oder Straftaten, kann die Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten bestehen. Davon unabhängig bietet die Dokumentation gem. Art. 30 DS-GVO einen guten Ansatz zur Erfüllung von Dokumentationspflichten. Kanzleien sind daher gut beraten, dieses Dokument zu führen.

Art. 30 DS-GVO ist hinreichend deskriptiv, so dass es hier keiner grundsätzlicher Erläuterung bedarf, welche Information in ein Verzeichnis von Verarbeitungstätigkeiten aufzunehmen ist (dazu *Gossen/Schramm*, ZD 2017, 7; *Licht*, ITRB 2017, 65; *Duda*, PinG 2016, 248; zum Vergleich zwischen bestehenden und zukünftigen Anforderungen DSK, Kurzpapier Nr. 1, 29.6.2017). Interessant und im Ergebnis gestaltungsoffen ist die Frage, was eine Verarbeitungstätigkeit ist. Gemäß Art. 4 Nr. 2 DS-GVO handelt es sich dabei um einen Vorgang oder eine Reihe von Vorgängen, bei dem mit oder ohne Hilfe automatisierter Verfahren mit personenbezogenen Daten umgegangen wird. Mit anderen Worten: Der Verantwortliche ist weitgehend frei darin, Verarbeitungen so zu definieren, dass sie zweckmäßig im Verzeichnis von Verarbeitungstätigkeiten abgebildet werden können. Im Grundsatz empfiehlt sich eine Orientierung an vorhandenen Prozessdokumentationen, die etwa im Rahmen des Qualitätsmanagements erstellt und geführt werden.

Mit dem Verzeichnis von Verarbeitungstätigkeiten haben Kanzleien eine strukturierte und konsistente Übersicht der Prozesse, mit denen sie personenbezogene Daten verarbeiten. Darin können die Pflichtangaben gem. Art. 30 DS-GVO und weitere, darüber hinausgehende Aspekte der Rechenschaftspflicht abgedeckt werden.

Dies gilt für den

- Grundsatz der Rechtmäßigkeit,
- Grundsatz der Datenverarbeitung nach Treu und Glauben,
- Grundsatz der Zweckbindung,
- Grundsatz der Transparenz,
- Grundsatz der Datenminimierung,
- Grundsatz der Speicherbegrenzung,
- Grundsatz der Richtigkeit von Daten,
- Grundsatz der Integrität und Vertraulichkeit.

Die Grundsätze der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben setzen voraus, dass personenbezogene Daten nur im Rahmen der Erlaubnistatbestände und berechtigten Erwartungen der Betroffenen verarbeitet werden (*Herbst* in *Kühling/Buchner*, DS-GVO, Art. 5 Rn. 8 ff.). Dieser Nachweis ist in Art. 30 DS-GVO nicht unmittelbar angelegt, kann aber abgebildet werden, indem für jede Verarbeitung die jeweils einschlägige Rechtsgrundlage ergänzt wird.

Der Zweckbindungsgrundsatz ist hingegen in Art. 30 I Buchst. b DS-GVO angelegt und wird durch ein Verzeichnis von Verarbeitungstätigkeiten abgebildet.

Ebenfalls nicht unmittelbar abgedeckt wird der Grundsatz der Transparenz. Er kristallisiert sich in Art. 13 DS-GVO und erfordert, Betroffene bei jeder Erhebung personenbezogener Daten umfassend zu informieren (Art. 13 DS-GVO). Dafür müssen die Kanäle, auf denen personenbezogene Daten in die Kanzlei gelangen, erfasst und für diese sichergestellt werden, dass jeweils eine Information gem. Art. 13 DS-GVO gegeben wird. Klassischerweise sind das Informationen gegenüber den Mitarbeitern als Anlage zum Arbeitsvertrag (dazu *Byers*, NZA 2017, 1086 [1087]) sowie Informationen an Mandanten und potenzielle Mandanten, die etwa in einer online-Information auf der Webseite vorgehalten und mit Verweisen in der Kommunikation (zB Link im E-Mail-Footer) referenziert werden können (dazu Art. 29 Datenschutzgruppe, WP 260, Nr. 7, 8 und 33).

Die Grundsätze der Datenminimierung und Speicherbegrenzung erfordern, personenbezogene Daten nur im Rahmen der Erforderlichkeit für den Zweck zu erheben und diese zu löschen, wenn der Zweck erfüllt ist und keine Aufbewahrungspflichten bestehen. Der Grundsatz der Datenminimierung kann in dem Verzeichnis von Verarbeitungstätigkeiten abgebildet werden, indem dort eine Übersicht der Daten aufgenommen wird, die Gegenstand der Verarbeitung sind. Ergänzend sollte ein Zugriffs- und Berechtigungskonzept oder eine ähnliche Dokumentation geführt werden. Der Grundsatz der Speicherbegrenzung erfordert die Festlegung und Umsetzung von Löschfristen. Für einzelne Verfahren mit geringer Komplexität können Löschfristen in den Verzeichnissen abgebildet werden. In der Regel wird dafür aber ein verfahrensübergreifendes Löschkonzept erforderlich werden.

Der Grundsatz der Richtigkeit erfordert, personenbezogene Daten mit korrekter Information zu verarbeiten und falsche Datensätze zu korrigieren. Hieran haben in der Regel sowohl Verantwortlicher als auch Betroffener Interesse. Die Einhaltung dieses Grundsatzes als Prozess ist fortlaufend zu dokumentieren, etwa indem Veränderungen an Datensätzen geloggt werden.

Art. 32 DS-GVO konkretisiert den Grundsatz der Integrität und Vertraulichkeit. Er lässt sich in dem Verzeichnis von Verarbeitungstätigkeiten dokumentieren, indem dort für jedes Verfahren technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten dokumentiert werden. Alternativ und wohl der klassische Ansatz ist die Erstellung eines separaten Konzepts zum technisch-organisatorischen Datenschutz. ■

Buchbesprechungen

Zivilprozessordnung. Kommentar. Begründet von *Richard Zöller*. 32., neu bearb. Auflage. – Köln, Otto Schmidt 2018. XXXII, 3296 S. geb. Euro 169,–. ISBN: 978-3-504-47023-4.

Zwei Jahre nach der Vorauflage ist der „*Zöller*“ zum Jahresende 2017 in 32. Auflage erschienen. Die Autoren bezeichnen ihr Werk im Vorwort – nicht zu Unrecht – als runderneuert. Der Inhalt hat neben Aktualisierungen und einer Änderung des Schriftbildes eine zusätzliche Ergänzung in Form von Querverweisen auf Mustertexte aus dem von *Vorwerk* herausgegebenen Prozessformularbuch erfahren (vgl. etwa § 253 Rn. 13 c). Bedingt durch den Tod von *Kurt Stöber* und das Ausscheiden von *Max Vollkommer* hat das Werk zudem mit *Christoph Althammer*, *Hendrik Schultzky*, *Mark Seibel* und *Gregor Vollkommer* vier neue Mitautoren bekommen.

Durch den Gesetzgeber veranlasst ist unter anderem die neue Kommentierung der zum 1.1.2018 in Kraft getretenen Fassung von § 130 a ZPO, die den elektronischen Rechtsverkehr nunmehr bundeseinheitlich regelt. *Greger* bewältigt diese Aufgabe in gewohnt souveräner Manier. Er zeigt dabei Querbezüge zu anderen maßgeblichen Vorschriften auf, etwa zu § 130 ZPO (§ 130 a Rn. 3 und 4), zur ERVV (§ 130 a Rn. 5, 8, 12 und 16) und zur VO (EU) 910/2014 (eIDAS, § 130 a Rn. 7). In der darauf abgestimmten Kommentierung zu § 130 ZPO stellt er der Entscheidung des *BGH* zur Wirksamkeit eines mit einfacher E-Mail übermittelten und im Gericht ausgedruckten Schriftsatzes das neue Urteil des *BSG* (NJW 2017, 1197) gegenüber, das einen mit EGVP übermittelten Schriftsatz ohne elektronische Signatur als unwirksam ansieht (§ 130 Rn. 18 d).

Ein weiteres im Vorwort angesprochenes Ziel ist die Straffung der bisherigen Kommentierung ohne Verlust wesentlicher Informationen. Dass dies gelungen ist, verdeutlich exemplarisch die Kommentierung von *Schultzky* zu § 32. Dort wurden etwa einzelne Details zum europäischen Recht durch einen Verweis auf die ausführliche Kommentierung zu Art. 7 Nr. 2 EuGVVO ersetzt (§ 32 Rn. 3). Ein weiteres gelungenes Beispiel bildet die nunmehr von *Vollkommer* übernommene Kommentierung zu § 321 a ZPO, wo Hinweise auf frühere Gesetzesfassungen, die aus heutiger Sicht nur noch von untergeordnetem Interesse sind, behutsam entfernt wurden (zB § 321 a Rn. 3 und 5). Der Aufbau einschließlich der prägnanten Aufzählung der Fallgruppen „Panne“, „Präklusion“, „Überraschung“ und „Übergehen“ (§ 321 a Rn. 8–11) wurde hingegen beibehalten.

Eine Kombination zwischen Straffung und Anpassung an Gesetzesänderungen findet sich zum Beispiel bei der Kommentierung zu § 174 ZPO. *Schultzky* geht hier unter anderem auf die Gesetzgebungsgeschichte ein (§ 174 Rn. 1) und erläutert zuverlässig die neuen Regelungen über die elektronische Übermittlung (§ 174 Rn. 11 f.) und das für diesen Fall zwingend vorgeschriebene elektronische Empfangsbekenntnis (§ 174 Rn. 19).

Insgesamt scheint die von den Autoren versprochene Runderneuerung gelungen. Sie bildet einen zusätzlichen Grund, dem für die Praxis ohnehin kaum entbehrlichen Werk auch in der Neuauflage treu zu bleiben.

Richter am BGH Dr. Klaus Bacher, Karlsruhe