DIE DATENSCHUTZ-GRUNDVERORDNUNG DER EU

RECHTSANWALT PROF. DR. ARMIN HERB*

Europa ist auf dem Weg zur digitalen Datenwirtschaft und ein wesentlicher Baustein ist die EU-Datenschutz-Grundverordnung (DS-GVO). Ob Unternehmen oder Anwaltskanzlei, alle sind ab dem 25.5.2018 davon betroffen, Übergangsvorschriften gibt es nicht. Zusätzlich hat der deutsche Gesetzgeber mit Hilfe des sog. Datenschutzanpassungsgesetzes ein neues BDSG geschaffen, welches die Verordnung ergänzt und das ebenfalls am 25.5.2018 in Kraft tritt. Der Autor stellt die für Anwälte wichtigsten neuen Regelungen im Datenschutzrecht vor.

I. RECHTSRAHMEN

Bislang war der Datenschutz auf europäischer Ebene durch Richtlinien geprägt. Eine Richtlinie verpflichtet die nationalen Gesetzgeber zwar zur Umsetzung, sie hat aber im Gegensatz zu einer Verordnung keine unmittelbare Geltung. Weil aber die verschiedenen nationalen Datenschutzgesetze zu sehr auseinanderliefen, wurde die unmittelbar gegenüber jedem Bürger und jedem Unternehmen geltende Europäische Datenschutz-Grundverordnung 2016/679 v. 27.4.2016[1] erlassen. Sie ist nach jahrelangen Verhandlungen (zuletzt im sog. Trilog mit einer englischen Urfassung) im Mai 2016 in Kraft getreten und gilt unmittelbar ab dem 25.5.2018 (Art. 99 DS-GVO). Ergänzend gilt das neue BDSG v. 30.6.2017.[2] Daneben soll die bisherige ePrivacy-Richtlinie durch eine EU-ePrivacy-Verordnung ersetzt werden; Stichworte sind hier Telemediengesetz, Cookies und Trackingverfahren. Für Anwälte ist daneben die BRAO zu berücksichtigen (z.B. § 50 BRAO zur Handakte).

1. SONDERREGELUNGEN FÜR DEN ÖFFENTLICHEN BEREICH

Bereits hier muss festgestellt werden, dass die DS-GVO zwar für die Privatwirtschaft und damit für die Unternehmen (sowie Rechtsanwälte) gilt, für Behörden und öffentliche Stellen besteht aber die Möglichkeit, dass der Gesetzgeber abweichende Regelungen trifft. Die Verordnung hat also für Behörden und öffentliche Stellen teilweise auch Richtlinien-Charakter, was sich auch in einer für Justiz und Polizei geltenden separaten Richtlinie für den Bereich der Strafverfolgung und Gefahrenabwehr[3] zeigt.

* Der Autor ist Rechtsanwalt in Stuttgart und Rundfunkbeauftragter für den Datenschutz beim Südwestrundfunk (SWR). Er ist Vorsitzender des BRAK-Ausschusses Datenschutzrecht.

[1] ABl. EU Nr. L 119 v. 4.5.2016, 1 ff.

[2] BGBl. 2017 I, 2097 ff.

[3] Sog. Justizrichtlinie 2016/680 v. 27.4.2016, ABl. EU Nr. L 119 v. 4.5.2016, 89 ff.

2. NICHT ALLES IST NEU

Wer das bisherige Bundesdatenschutzgesetz kennt und beherrscht, wird in der DS-GVO viele vertraute Prinzipien wiederfinden. Die gesetzlichen Definitionen wurden indessen erweitert; es gibt andererseits nur noch den (Ober-)Begriff der Verarbeitung und aus der verantwortlichen Stelle wurde der Verantwortliche, aus dem Auftragnehmer der Auftragsverarbeiter. Die Verordnung verstärkt die Betroffenenrechte und erhöht die Dokumentations- und Nachweispflichten. Aber auch Möglichkeiten zur Geltendmachung von Schadenersatzansprüchen oder die exorbitante Erhöhung der Bußgeldbestimmungen schaffen neue Möglichkeiten für die fast übermächtigen Datenschutzaufsichtsbehörden.

II. INHALT

Anhand einiger Stichworte soll skizzenartig der Inhalt der DS-GVO dargestellt werden:

1. MARKTORTPRINZIP

Ein ganz wichtiges und neues Prinzip (und eine Triebfeder des Verordnungsgebers) ist das Marktortprinzip (Art. 3 DS-GVO). Dies bedeutet nicht nur, dass in allen Mitgliedstaaten diese Verordnung als unmittelbar geltendes Gesetz direkt wirkt, sondern besagt auch: Jedes Unternehmen, sei es innerhalb oder außerhalb Europas, welches auf jeden in der EU „Ansässigen" einwirkt und mit seinen Daten umgeht, hat die DS-GVO zu beachten. Dabei ist es gleichgültig, ob kommerzielle Interessen verfolgt werden oder lediglich andere (z.B. karitative) Motive zugrunde liegen. Jeder, der auf in Europa lebende Bürger einwirkt, und sei es nur durch eine Beobachtung, muss die DS-GVO beachten. Wessen Unternehmen keinen Sitz in Europa hat, muss nach Art. 27 DS-GVO einen Vertreter bestellen.

2. ALLGEMEINE PRINZIPIEN

Die in der DS-GVO niedergelegten Grundsätze und Prinzipien unterscheiden sich praktisch nicht von den bisherigen Regelungen: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung oder Gewährleistung von Integrität und Vertraulichkeit, wie in Art. 5 I DS-GVO gefordert, sind für Datenschützer keine Neuigkeiten.

In Art. 5 II DS-GVO wird allerdings ein in dieser Form neuer Grundsatz aufgestellt, der sich durch die ganze Verordnung zieht: So muss der Verantwortliche die Einhaltung aller Regelungen nachweisen können. Es bestehen (weite) Nachweis- und Rechenschaftspflichten (in der englischen Urfassung: accountabilities). Ein Anwalt ist dabei nicht nur für die Einhaltung dieser in Art. 5 I

DS-GVO formulierten Grundsätze verantwortlich, sondern „muss dessen Einhaltung nachweisen können", Art. 5 II DS-GVO (ebenso nochmals Art. 24 I 1 DS-GVO).

Im Gegensatz dazu legt die DS-GVO ein großes Gewicht darauf, dass es zu bereichs- und unternehmensspezifischen Datenschutzstandards kommt. Deshalb sind Verhaltensregelungen (Art. 40 und 41 DS-GVO) und Zertifizierungen (Art. 42 und 43 DS-GVO) möglich. Für eine Anwaltskanzlei kann so die Verantwortlichkeit z.B. für die Datensicherheit dadurch gewahrt werden, dass man nur zertifizierte Anbieter wählt oder sich selbst zertifizieren lässt.

3. VERBOT MIT ERLAUBNISVORBEHALT

Beibehalten wurde das sog. Verbot mit Erlaubnisvorbehalt (Art. 6 DS-GVO). Dies bedeutet, dass jede Datenverarbeitung – diese reicht von der Erhebung, also Beschaffung von Daten über die Speicherung, Nutzung und Verwendung bis hin zur Weitergabe und Löschung – einer Rechtsgrundlage bedarf. Dies kann die DS-GVO selbst sein, ein bereichsspezifisches Gesetz (worunter auch das neue BDSG oder die BRAO fallen können) oder aber eine Einwilligung der betroffenen Personen. Für Mandatsverhältnisse ändert sich hier nichts, sie sind die Rechtsgrundlage für die mandatsbezogene Datenverarbeitung eines Anwalts.

4. EINWILLIGUNG

Eine Einwilligung als Rechtfertigung für eine Datenverarbeitung gab es schon im BDSG (erforderte dort aber Schriftform) und bescherte im Bereich des Beschäftigtendatenschutzes immer wieder Probleme. Jetzt wird der Beschäftigtendatenschutz den jeweiligen nationalen Gesetzgebern überantwortet, weshalb wir vielleicht irgendwann einmal in Deutschland ein Beschäftigtendatenschutzgesetz erhalten werden. Für die Einwilligung nach Art. 7 DS-GVO wird zwar keine Schriftlichkeit gefordert, aber eine Nachweispflicht. Wird die Einwilligung mit anderen Sachverhalten verknüpft, so ist eine klare Trennung vorzunehmen und grundsätzlich besteht ein Koppelungsverbot. Neu sind die speziellen Regelungen zur Einwilligung eines Kindes, welches das 16. Lebensjahr noch nicht vollendet hat (Art. 8 DS-GVO).

5. GESETZLICHE RECHTFERTIGUNG FÜR EINE DATENVERARBEITUNG

Eine gesetzliche Rechtfertigung für die Verarbeitung von Daten von betroffenen Personen kann sich insbesondere aus Art. 6 DS-GVO ergeben. Dort wird allerdings – wie in der (ersten) BDSG-Fassung vor 40 Jahren – nur mit Generalklauseln gearbeitet: Die schutzwürdigen Betroffeneninteressen müssen mit den berechtigten Interessen einer verantwortlichen Stelle abgewogen werden. Im alten BDSG sind hingegen im Laufe der Jahre immer wieder spezielle Regelungen für Auskunfteien, Adresshändler und die Werbewirtschaft geschaffen worden. Weil in der DS-GVO indessen z.B. Regelungen zu Bonitätsauskünften oder Scoring fehlen, versucht der deutsche Gesetzgeber mit dem neuen, ebenfalls ab dem 25.5.2018 geltenden BDSG eine Lückenfüllung bzw. Konkretisierung der DS-GVO. § 31 BDSG-2018 trifft Regelungen zum „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften". Dies sind im Wesentlichen die bislang in den §§ 28a und 28b BDSG enthaltenen Regelungen zu Scoring und für Auskunfteien.

Die Videoüberwachung kommt in der DS-GVO nur rudimentär im Zusammenhang mit der Datenschutz-Folgenabschätzung vor. Der deutsche Gesetzgeber hat indessen mit § 4 des neuen BDSG-2018 eine umfangreiche Vorschrift für die Überwachung öffentlicher Räume geschaffen.[4] Anwaltskanzleien können damit zwar zur Wahrnehmung des Hausrechts z.B. ihre Grundstücke und Eingänge überwachen, müssen aber zum Schutz des Mandatsgeheimnisses entsprechende Vorkehrungen sowohl im Hinblick auf die Speicherung als auch die Auswertung sowie die Zugriffsmöglichkeiten treffen.

Ein Konzernprivileg gibt es zwar nach wie vor nicht, doch über sog. „verbindliche interne Datenschutzvorschriften" (binding corporate rules) wird für Unternehmensgruppen (Definition in Art. 4 Nr. 19 DS-GVO) eine Erleichterung geschaffen. Im Einzelfall können auch große und überregional tätige „Anwaltsfirmen" darunter fallen.

Für die Beschäftigtendaten ist durch die DS-GVO den Mitgliedstaaten die Möglichkeit eröffnet worden, durch Gesetz oder durch Kollektivvereinbarung (collective agreements) spezifische Vorschriften im „Beschäftigungskontext" zu erlassen (Art. 88 I DS-GVO). Sie müssen aber den Anforderungen der DS-GVO entsprechen, die auch im Übrigen gilt (Art. 88 II DS-GVO), was z.B. im Hinblick auf die Betroffenenrechte der Beschäftigten von großer Bedeutung ist.

Aufgrund der Staatsferne der Medien und ihrer Bedeutung für die Freiheit von Berichterstattung und Meinungsäußerung müssen die Mitgliedstaaten wegen Art. 85 DS-GVO entsprechende nationale Regelungen vorsehen (Stichwort Medienprivileg). Die Kirchen können eigenständige Regelungen entsprechend der DS-GVO erlassen (Art. 91 DS-GVO).

6. BETROFFENENRECHTE

Die DS-GVO will im Einklang insbesondere mit Art. 8 der EU-Grundrechte-Charta das Persönlichkeitsrecht der Betroffenen schützen. Folgerichtig enthält die Verordnung Rechte von Betroffenen, die gegenüber den deutschen Datenschutzgesetzen zum Teil erheblich erweitert wurden (Art. 12 bis 22 DS-GVO).

a) INFORMATIONSPFLICHTEN

Betroffene müssen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" informiert werden. Die EU-Kommission kann hierzu sogar verbindliche Bildsymbole erlassen (Art. 12 DS-GVO).

[4] Vgl. dazu *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 6b BDSG a.F., der bereits dem neuen § 4 BDSG-2018 entspricht.

Erweitert wurden insbesondere die Informationspflichten bei der Erhebung von Daten (Art. 13 und 14 DS-GVO) sowie die Auskunftsrechte (Art. 15 DS-GVO).

Selbst wenn Daten von Mandanten bei Beginn einer Mandatsbeziehung von ihm persönlich und direkt erhoben werden, müssen nach dem Wortlaut des Art. 13 DS-GVO eine Reihe von Informationen dem Mandanten (!) gegeben werden. Eine Ausnahme besteht nur, wenn die betroffene Person bereits über die Informationen verfügt, was jedoch insbesondere bei Naturparteien nicht in allen Fällen vorausgesetzt werden kann (z.B. die Kenntnis im Hinblick auf die möglichen Empfänger der personenbezogenen Daten). Hier müssten ggf. im Zusammenhang mit der Vollmachtserteilung durch den Mandanten diesem die entsprechende Informationen auf einem Merkblatt gegeben werden.

Werden im Rahmen eines Mandats Daten vom Gegner erhoben, so müsste dieser nach der DS-GVO informiert werden und hätte Auskunftsansprüche (Art. 14 und 13 DS-GVO). Hier hat die BRAK in letzter Minute erreicht, dass es eine Öffnungsklausel gibt und der deutsche Gesetzgeber dann mit § 29 I und II BDSG-2018 diese widersinnigen Regelungen eingeschränkt hat: Danach wird die Pflicht zur Information des Gegners (oder sonstiger Dritter) eingeschränkt. Die Interessen des Mandanten haben insoweit grundsätzlich Vorrang. Dies gilt auch im Hinblick auf eventuelle Auskunftsansprüche des Gegners.

b) „RECHT AUF VERGESSENWERDEN"

Neu ist das so bezeichnete „Recht auf Vergessenwerden" als besondere Ausprägung von Löschungspflichten (Art. 17 DS-GVO). Danach besteht der Grundsatz, dass nicht mehr benötigte Daten unverzüglich gelöscht werden müssen (also z.B. zum Ende einer Mandatsbeziehung). Allerdings wird durch § 17 III lit. b DS-GVO dieses unverzügliche Löschungsrecht des Mandanten aufgrund § 50 I (i.V.m. IV) BRAO durch die Pflicht zur Aufbewahrung der Handakten (auch soweit sie elektronisch geführt werden) für den Zeitraum von sechs Jahren (plus dem laufenden Jahr) eingeschränkt. Unterlagen mit steuerlicher Relevanz müssen aufgrund der Regelungen (insbesondere in der AO) grundsätzlich für zehn Jahre aufbewahrt werden. Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen kann auch eine längere Aufbewahrung erforderlich sein (§ 17 III lit. e DS-GVO).

Ist dann die Löschung vorzunehmen, hat sie datenschutzkonform entsprechend DIN 66399 (also nach Schutzklasse 3) zu erfolgen und ist auch zu dokumentieren. Selbst Papierakten wird man in der Regel durch einen (zertifizierten) Fachbetrieb entsorgen lassen.

c) WEITERE BETROFFENENRECHTE

Das Recht auf Einschränkung der Verarbeitung entspricht im Wesentlichen dem bisherigen Recht auf Sperrung der Daten (Art. 18 DS-GVO) und erfasst z.B. den geschilderten Fall, dass Daten zwar für den Kanzleibetrieb nicht mehr notwendig sind, aufgrund steuerlicher Vorschriften aber weiter aufbewahrt werden müssen und dann für diesen Zeitraum auch nur einem eingeschränkten Zugriff durch wenige Mitarbeiter unterliegen dürfen.

Gänzlich neu ist Art. 20 DS-GVO mit seinem „Recht auf Datenübertragbarkeit". Damit soll gewährleistet werden, dass dann, wenn ein Betroffener (z.B. als Kunde eines Unternehmens), wechselt, seine „Stammdaten" auf das neue Unternehmen elektronisch übergehen. Dem Wortlaut nach gilt dies auch bei einem Anwaltswechsel.

Wie bislang kann ein Betroffener im Grundsatz der Verarbeitung seiner Daten widersprechen, insbesondere was die Direktwerbung anbelangt (Art. 21 DS-GVO). Bereits bislang enthielt das BDSG Regelungen zur automatisierten Einzelfallentscheidung und zum Scoring. Jetzt werden diese Rechte der Betroffenen gestärkt, wenn es um eine automatisierte Entscheidung im Einzelfall (einschließlich Profiling) geht (Art. 22 DS-GVO).

Die §§ 32–37 BDSG-2018 regeln „ergänzend" zur DS-GVO, dass Betroffenenrechte unter bestimmten Voraussetzungen nicht gelten oder eingeschränkt werden können. Ob dies in jedem Fall europarechtskonform ist, muss zumindest im Hinblick auf die Rechte gegenüber nicht-öffentlichen Stellen stark bezweifelt werden.

Im Zusammenhang mit den Betroffenenrechten ist auch erwähnenswert, dass nicht nur Beschwerden bei Aufsichtsbehörden oder Rechtsbehelfe gegen Verantwortliche möglich sind (Art. 77–79 DS-GVO), sondern dass auch durch (Verbraucher-)Schutzorganisationen gegen Verantwortliche vorgegangen werden kann, also (über das deutsche Unterlassungsklagengesetz hinaus) eine Art Verbandsklagerecht besteht (Art. 80 DS-GVO).

Das in Art. 82 DS-GVO geregelte Recht auf Schadenersatz erfasst nicht nur materielle, sondern auch – was bislang zum Teil bestritten war – immaterielle Schäden (immaterial damage). Somit könnte es auch zu Schmerzensgeldansprüchen gegen einen Anwalt kommen, wenn bei der Verarbeitung der Mandantendaten die DS-GVO verletzt worden ist.

7. AUFTRAGSDATENVERARBEITUNG

Wird die Datenverarbeitung nicht vollständig selbst durchgeführt, sondern werden Auftragnehmer eingeschaltet, so ist zwar wie bislang ein Vertrag zur Auftragsdatenverarbeitung abzuschließen. Die Regelungen in Art. 28 DS-GVO sind aber umfangreicher und insbesondere für die Auftragnehmer (jetzt Auftragsverarbeiter genannt) bestehen neue und umfangreiche gesetzliche Pflichten, bis hin zur Haftung. Eine Auftragsdatenverarbeitung liegt vor, wenn Dritte eingeschaltet werden bzw. Aufgaben ausgelagert werden. Dies kann bereits ein Schreib- oder Übersetzungsbüro oder Call-Center sein, aber auch sämtliche Personen, die Computeranlagen warten und reparieren oder Daten in ihrer Cloud speichern. Hierfür ist ein entsprechender Vertrag zur Auftragsdatenverarbeitung abzuschließen.[5] Die strafrechtliche Dimension wurde jetzt durch die Ände-

[5] Vgl. den Mustervertrag bei *Bergmann/Möhrle/Herb*, Art. 28 DS-GVO, Anl. 2.

rung des § 203 StGB mit seinen Vorschriften zum Outsourcing geregelt (vgl. auch § 2 BORA).

8. DATENSICHERHEIT

Bereits bisher enthielten die Datenschutzgesetze Regelungen zur Datensicherheit (also praktisch zur IT-Sicherheit). Während bislang die Datenschutzgesetze einen Katalog von Maßnahmen vorgaben, indem sie technische und organisatorische Maßnahmen zur Datensicherheit forderten (z.B. Regelungen zum Zugriffsschutz, Schutz für die Weitergabe usw.), sind jetzt nur noch allgemeine Prinzipien vorgegeben. Es müssen nach wie vor geeignete technische oder organisatorische Maßnahmen getroffen werden, die sich am Stand der Technik (also nicht der angewandten Technik oder dem Stand der Wissenschaft) zu orientieren haben (Art. 24, 32 DS-GVO). Wie bislang ist damit dem technologischen Wandel gerade im Bereich der Datensicherheit Rechnung zu tragen. Durch Art. 25 DS-GVO wird aber auch die Gewährleistung des Datenschutzes durch Technikgestaltung (data protection by design) sowie durch datenschutzfreundliche Voreinstellungen (data protection by default) gefordert.

Wie bislang ist es erforderlich, dass eine Zugriffs- und Benutzerverwaltung existiert, damit jeweils nur solche Personen auf Daten zugreifen können, die hierzu auch berechtigt sind. Die Regelungen zur Passwortvergabe können sich beispielsweise an den Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) orientieren. In all diesen Fällen sind nicht nur Regelungen und Überprüfungen notwendig, sondern inzwischen auch eine entsprechende Dokumentation.

9. BETRIEBLICHE UND BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

Neben den Aufsichtsbehörden, die die hoheitlichen Befugnisse ausüben, gibt es nach wie vor behördliche oder betriebliche Datenschutzbeauftragte. Die in Art. 37–39 DS-GVO getroffenen Regelungen werden durch nähere Bestimmungen im neuen BDSG-2018 ergänzt (§§ 5–7 sowie § 38), womit das bisherige Datenschutzbeauftragtensystem in der Bundesrepublik beibehalten wird. Schon für mittelgroße Anwaltskanzleien kann sich damit die Pflicht ergeben, einen betrieblichen Datenschutzbeauftragten zu bestellen. Voraussetzung ist, dass mindestens zehn Personen mit der Datenverarbeitung beschäftigt sind, also am PC sitzen (Teilzeitkräfte zählen wie eine Person). Für die Berechnung müssen die Inhaber der Kanzlei nicht mit berücksichtigt werden, wohl aber angestellte Anwälte.

Neu ist die Pflicht gem. Art. 37 VII DS-GVO, nicht nur die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen (bspw. auf der Homepage), sondern auch an die Aufsichtsbehörde zu melden.

10. AUSLANDSDATENVERARBEITUNG

Werden Daten innerhalb der Europäischen Union verarbeitet, so gilt aufgrund des Marktortprinzips die DS-GVO. Sollen die Daten ins außereuropäische Ausland übermittelt, dort gespeichert oder sonst verarbeitet werden, so müssen die in den Art. 44–50 DS-GVO enthaltenen Regelungen eingehalten werden. So kann beispielsweise die Europäische Kommission feststellen, dass ein Land ein angemessenes Datenschutzniveau hat (z.B. Schweiz) oder aber dass die Verarbeitung zulässig ist, wenn sie aufgrund bestimmter vorgegebener Standardvertragsklauseln erfolgt.

Für Anwaltskanzleien mit Tätigkeiten in den USA stellt sich eine besondere Herausforderung, nachdem Safe Harbor vom EuGH gekippt wurde und niemand weiß, ob dasselbe nicht auch mit dem Privacy Shield geschieht. In vielen Fällen dürfte der mühsame Weg über Einwilligungen die derzeit einzige zukunftssichere Lösung sein.

11. AUFSICHTSBEHÖRDEN

Nicht nur bei der Frage der Auslandsverarbeitung spielen die Aufsichtsbehörden (und mittelbar die EU-Kommission) eine große Rolle. Die Aufgaben und Befugnisse der Aufsichtsbehörden (Art. 51–76 DS-GVO) wurden erheblich ausgeweitet.

Während in den übrigen Mitgliedstaaten regelmäßig nur eine Aufsichtsbehörde besteht, wird in Deutschland das bisherige, bewährte System beibehalten, welches auf verfassungsrechtlichen Prinzipien und dem föderalen Aufbau beruht. Neben der Bundesdatenschutzbeauftragten gibt es weitere Aufsichtsorgane.

- Die Bundesdatenschutzbeauftragte ist für die Bundesbehörden zuständig, aber auch für den Bereich der Telekommunikation, der Postdienstleistungen und jetzt neu nach dem § 36a Sicherheitsüberprüfungsgesetz (SÜG) sowie zukünftig für die gesamten Finanzverwaltungen (§ 32h AO).
- Daneben gibt es die Landesdatenschutzbeauftragten, welche für die jeweiligen Landesbehörden und die Privatwirtschaft in ihrem Bereich zuständig sind.
- Schließlich bestehen Sonderregelungen, also eigenständige „sektorale“ Aufsichtsbehörden für die Kirchen und die öffentlich-rechtlichen Rundfunkanstalten.

Durch das neue BDSG wurde die Koordination der verschiedenen nationalen Aufsichtsbehörden der Bundesdatenschutzbeauftragten übertragen (§§ 17–19 BDSG-2018).

Die DS-GVO enthält indessen auch umfangreiche Regelungen zur Frage, welche der vielen nationalen Aufsichtsbehörden in Europa zuständig ist. Wichtig ist dies z.B. für Unternehmen, aber auch Anwaltskanzleien, die in verschiedenen Staaten der EU tätig sind. Schließlich gibt es mit dem Europäischen Datenschutzausschuss (Art. 68–76 DS-GVO) ein supranationales Organ, welches verbindliche Entscheidungen mit Zweidrittelmehrheit treffen kann, also letztlich für die Auslegung der DS-GVO zuständig ist. Darüber gibt es dann nur noch den EuGH.

Die Befugnisse der Aufsichtsbehörden sind nicht nur sehr umfangreich, sondern auch anlassunabhängig. Sie verfügen nach Art. 58 DS-GVO über Untersuchungsbefugnisse, also die Möglichkeiten, Untersuchungen und Überprüfungen vor Ort bei einem Unternehmen vorzunehmen. Sie können mit ihren weitreichenden Abhilfebefugnissen letztlich auch Datenverarbeitungsvor-

gänge untersagen, beschränken oder in bestimmter Weise vorgeben. Daneben gibt es noch Genehmigungsbefugnisse (z.B. im Hinblick auf Verhaltensregelungen oder Zertifizierungen).

Schließlich ist noch auf die umfangreichen Ordnungswidrigkeitentatbestände hinzuweisen: So ist nicht nur fast jeder Verstoß gegen die Verordnung sanktioniert, sondern die Aufsichtsbehörden können auch Bußgelder erheben, die je nach Art des Verstoßes bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes (nicht Gewinns!) betragen können (Art. 83 DS-GVO).

12. SONDERREGELUNGEN FÜR DIE KONTROLLE VON BERUFSGEHEIMNISTRÄGERN

Der EU-Gesetzgeber erlaubt auch nationale Regelungen zu Berufsgeheimnissen und gleichwertigen Geheimhaltungspflichten (Art. 90 DS-GVO). Deshalb hat der deutsche Gesetzgeber mit § 29 III BDSG-2018 eine Sonderregelung für die Datenschutzaufsicht geschaffen. Sie wird aber insbesondere von (ehemaligen) staatlichen Datenschützern heftig kritisiert[6] und selbst in juristischen Kommentaren werden Funktion, Aufgabe und verfassungsrechtliche Gewährleistung der Rechtsanwälte negiert.[7]

Die Aufsichtsbehörden haben nach Art. 58 DS-GVO umfangreichste Befugnisse: Im Rahmen der Untersuchungsbefugnisse nach Art. 58 I DS-GVO können sie Informationen anfordern, Überprüfungen vornehmen, Zugang zu allen Daten und Informationen verlangen bis hin zum Zugang zu den Geschäftsräumen. Die Abhilfebefugnisse nach Art. 58 II DS-GVO gestatten es einer Aufsichtsbehörde, nicht nur Hinweise zu geben und Verwarnungen auszusprechen, sondern auch konkrete Anweisungen zu geben, wie bestimmte Verarbeitungen zu erfolgen haben, bis hin zur vorübergehenden oder endgültigen Beschränkung oder dem Verbot einer Verarbeitung. Auch die Berichtigung und Löschung von Daten kann verlangt werden oder die Aussetzung von Übermittlungen in Drittstaaten (z.B. USA) angeordnet werden. Hinzu kommen die Möglichkeiten von Geldbußen nach Art. 83 DS-GVO (bis zu 20 Mio. Euro). Wenn man sich dann noch vergegenwärtigt, dass eine Kontrolle anlasslos und ohne Vorliegen eines Grundes geschehen kann und die Aufsichtsbehörden aufgrund ihrer von demokratischen Prozessen abgelösten Unabhängigkeit weder einer Dienst-, Fach- noch Rechtsaufsicht unterliegen, so werden die Gefahren der Kontrollmöglichkeiten im Hinblick auf die Anwaltschaft offenbar.

Nach Art. 90 DS-GVO können indessen durch den nationalen Gesetzgeber die Befugnisse der Aufsichtsbehörden bei Berufsgeheimnisträgern eingeschränkt werden (wobei es notwendig gewesen wäre, die Rechte der Aufsichtsbehörden zu Gunsten der anwaltlichen Verschwiegenheitspflicht noch weiter einzuschränken) – dies jedoch nur im Hinblick auf einen kleinen Teil der Untersuchungsbefugnisse nach Art. 58 I lit. e DS-GVO (Zugang zu allen personenbezogenen Daten und Informationen) sowie Art. 58 I lit. f DS-GVO (Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte).

Der deutsche Gesetzgeber hat von dieser „kleinen" Öffnungsklausel durch § 29 III BDSG-2018 Gebrauch gemacht. Dabei wird völlig übersehen, dass ein Anwalt nur die Interessen seines Mandanten vertritt, dieser bei eigener Verarbeitung seiner Daten nicht der DS-GVO unterliegen würde (Art. 2 II lit. c DS-GVO) und selbst europarechtlich das Recht auf einen Anwalt durch Art. 47 II EU-Grundrechtecharta verbürgt ist, ganz abgesehen von den deutschen verfassungsrechtlichen Gewährleistungen des Anwaltsberufs. Es geht auch nicht um die Rechte des Anwalts, sondern um den Schutz des Mandanten[8].

Um die rechtsstaatliche Funktion und Aufgaben der Anwaltschaft zu wahren, ist es mehr denn je notwendig, die nach Art. 51 DS-GVO bestehende Möglichkeit einer sektoralen Datenschutzaufsicht auszuschöpfen. Die BRAK fordert deshalb seit langem die Schaffung einer eigenen Aufsichtsbehörde für Rechtsanwälte in Form eines Datenschutzbeauftragten für die Anwaltschaft. Nur durch ein derartiges sektorales Kontrollorgan kann gewährleistet werden, dass die berufsspezifischen Regelungen genügend Berücksichtigung finden.[9] Damit würde vermieden werden, dass staatliche Organe die Datenverarbeitung in Mandatsbeziehungen kontrollieren können und damit in das Mandatsgeheimnis eingreifen.

13. VERFAHRENS- UND DOKUMENTATIONS-REGELUNGEN

Wer personenbezogene Daten verarbeitet, muss dazu nicht nur eine Rechtsgrundlage haben, sondern auch bestimmte Formalien und Verfahrensweisen beachten:

Die bislang in den Datenschutzgesetzen vorgesehene Vorabkontrolle wird ersetzt durch die Verpflichtung, eine sog. Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DS-GVO) und hierbei notfalls die Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO).

Erwähnenswert in diesem Zusammenhang ist z.B. auch, dass sowohl Auftraggeber als auch Auftragnehmer (wie im Prinzip jeder Verantwortliche) nach Art. 30 DS-GVO sog. Verfahrensverzeichnisse zu erstellen haben.[10] Sie sind für die Aufsichtsbehörden gedacht (und müssen nicht mehr, wie bislang teilweise vorgesehen, veröffentlicht werden). Auch Anwaltskanzleien müssen in der Regel ein solches Verfahrensverzeichnis führen.

Bereits bislang mussten unter bestimmten Voraussetzungen Datenschutzverletzungen an die Aufsichtsbehörde gemeldet werden (data breach notification). Diese Pflichten wurden jetzt sowohl inhaltlich ausgeweitet, indem auch die betroffenen Mandanten informiert werden müssen, als auch zeitlich dahingehend verschärft,

[6] Z.B. *Weichert*, DANA 2017, 76 ff.; LfDI Berlin, RDV 2017, 210.
[7] *Kranig*, in Ehmann/Selmayr, Art. 90 Rn. 2–4.
[8] Was von *Kranig*, in Ehmann/Selmayr, Art. 90 Rn. 4 völlig verkannt wird.
[9] Vgl. z.B. BRAK-Stn. 41/2016 (Dezember 2016) sowie *König*, Sektorale Datenschutzkontrolle bei Rechtsanwälten, 2015.
[10] Vgl. z.B. das Muster bei *Bergmann/Möhrle/Herb*, Art. 30 DS-GVO, Anl. 2.

dass die Meldung binnen 72 Stunden erfolgen soll (Art. 33 DS-GVO). Wird also beispielsweise ein Datenleck in einer Anwaltskanzlei festgestellt, sei es durch Hacker von außen oder Mitarbeiter von innen, so müssen die Aufsichtsbehörden, also staatliche Organe, informiert und eingeschaltet werden.

III. ZUSAMMENFASSENDE WÜRDIGUNG

Die DS-GVO ist ein Meilenstein auf dem Weg zu gemeinsamen europäischen Datenschutzregelungen und muss auch im Kontext einer sich abzeichnenden europäischen digitalen Datenwirtschaft gesehen werden. Die bisherige deutsche Datenschutzgesetzgebung wird nicht nur materiell geändert, sondern wird zusätzlich geprägt durch ein noch komplizierteres Regelungsgeflecht. Bis der Umfang der Geltung einzelner Bestimmungen sowohl in der DS-GVO als auch im neuen BDSG-2018 sowie sonstigen Datenschutzregelungen (z.B. den Landesdatenschutzgesetzen oder bereichsspezifischen Normen) für die Anwender rechtssicher bestimmt ist, werden noch sehr viele Jahre vergehen.