Die Datenschutz-Grundverordnung - erste Erkenntnisse und ihre Anwendung auf die anwaltliche Berufspraxis

Von Rechtsanwältin Dr. Susanne Offermann-Burckart
Beauftragte des Vorstands für Grundsatzfragen

I. Einleitung

Ab dem 25.05.2018 finden die in der europäischen Datenschutz-Grundverordnung (DS-GVO) niedergelegten Vorgaben in allen EU-Mitgliedstaaten unmittelbare Anwendung. Die Auswirkungen in der Praxis sind z.T. erheblich und betreffen u.a. auch Dienstleister, die - wie Rechtsanwälte - mit sensiblen Daten von Kunden bzw. Mandanten umgehen. Jede Rechtsanwältin und jeder Rechtsanwalt muss sich deshalb schon im ureigenen Interesse mit den Bestimmungen der DS-GVO und den daraus resultierenden Handlungsanforderungen vertraut machen.

Dabei ergibt sich eine Vielzahl neuer Fragen, wie z.B.:

Wie umfangreich sind die Erläuterungspflichten zu Beginn eines Mandats? Müssen auch Gegner, Zeugen und sonstige Drittbetroffene über die Verarbeitung ihrer Daten informiert werden? Erschweren die besonders hohen Schutzstandards, die die DS-GVO für die Verarbeitung der Daten von Kindern aufstellt, die Bearbeitung von familienrechtlichen Mandaten, in denen es um Minderjährige geht? Wie „vertragen“ sich die DS-GVO und das deutsche anwaltliche Berufsrecht? Wie lassen sich die strengen Löschungspflichten mit den Anforderungen einer wirksamen Kollisionskontrolle oder der Abwehr spät geltend gemachter Schadensersatzansprüche in Einklang bringen? Was gilt bei der Hinzuziehung von freien Mitarbeitern und externen Dienstleistern?

Der folgende Beitrag klärt über die neue Rechtslage auf und liefert erste Lösungsansätze für diese und weitere Fragestellungen. Dabei werden notwendigerweise auch die neuen Bestimmungen über anwaltliche Handakten und über das Outsourcing von Dienstleistungen durch Berufsgeheimnisträger beleuchtet und zur DS-GVO in Beziehung gesetzt.

II. Zu Entstehungsgeschichte und Besonderheiten der DS-GVO

Schon seit 1995 gilt auf Ebene der EU und des Europäischen Wirtschaftsraums mit der EU-Datenschutz-Richtlinie ein gemeinsames Datenschutz-Niveau. Al-

lerdings hat sich gezeigt, dass die Richtlinie in den einzelnen Mitgliedstaaten sehr unterschiedlich ausgelegt wird. Außerdem hat sich seither in der digitalen Welt viel verändert. Zwar gab es 1995 schon das Internet, aber Facebook, Google und Twitter waren noch nicht geboren und eBay und Amazon noch keine zwei Jahre alt. Die massiven Probleme, die die Digitalisierung und Vernetzung mit sich brachten, traten erst nach und nach zu Tage und machten ein neues Datenschutzrecht erforderlich.

Deshalb wurde von der EU-Kommission im Januar 2012 zur Modernisierung des Datenschutzrechts in Europa eine EU-Datenschutzreform vorgestellt. Im zuständigen LIBE-Ausschuss des EU-Parlaments wurden über 3.100 Änderungsanträge zu dem ursprünglichen Entwurf der EU-Kommission eingebracht. Generell setzten sich die meisten sozialdemokratischen und grünen Abgeordneten für eine Verschärfung oder zumindest Präzisierung des Entwurfs ein, während die meisten konservativen und liberalen Abgeordneten eine liberalere, die Interessen der IT-Wirtschaft stärker in den Blick nehmende Lösung favorisierten.

Schon am 21.10.2013 nahm der Innen- und Justizausschuss des Europäischen Parlaments die durch den Grünen-Europaabgeordneten *Jan-Phillip Albrecht* ausgearbeitete Verhandlungsposition mit überwältigender Mehrheit an. Ihre Bestätigung durch das Plenum erfolgte am 12.03.2014. Der EU-Ministerrat benötigte ein Jahr länger, um seinen Standpunkt zu finden. Die anschließenden Trilog-Verhandlungen (zwischen Kommission, Parlament und Rat) dauerten noch einmal knapp zwei Jahre und endeten am 15.12.2015 schließlich mit einer Einigung. Am 14.04.2016 passierte die *„Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“* das EU-Parlament und am 04.05.2016 erfolgte ihre Veröffentlichung im Amtsblatt der Europäischen Union. Zwanzig Tage später, also am 25.05.2016, trat die Verordnung offiziell in Kraft (Art. 99 Abs. 1 DS-GVO). Gem. Art. 99 Abs. 2 „gilt“ sie ab dem 25.05.2018.

Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung (die anders als eine Richtlinie keines innerstaatlichen Umsetzungsaktes bedarf, vgl. Art. 288 Abs. 2 AEUV) entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die DS-GVO wird ab dem 25. Mai 2018 ohne Umsetzungsakt in allen ihren Teilen verbindlich sein und in jedem EU-Mitgliedstaat unmittelbar gelten. Den Mitgliedstaaten wird es daher grundsätzlich nicht möglich sein, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken.

Mit Wirksamwerden der DS-GVO treten das (alte) deutsche Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Länder außer Kraft. Auch die zahlreichen, in Deutschland beispielsweise im Bereich des Sozial- und Versicherungsrechts, vorzufindenden sondergesetzlichen Regelungen werden ab dem 25.05.2018 nur noch bedingt anwendbar sein.

Dennoch ist die DS-GVO - anders als ursprünglich geplant - doch kein Instrument der „Vollharmonisierung“ geworden. Denn es gibt Bereiche, in denen die Mitgliedstaaten die Regelungen der DS-GVO konkretisieren dürfen und auf diese Weise nach wie vor länderspezifische Regelungen schaffen können. Die DS-GVO stellt also auch wieder eine Kompromisslösung dar und wird deshalb von manchen etwas abschätzig als „Verordnung light“ bezeichnet.[1] Der den Mitgliedstaaten eingeräumte Spielraum wurde in Deutschland mit der Verabschiedung des sog. Datenschutz-Anpassungs- und Umsetzungsgesetzes (DSAnpUG-EU)[2] genutzt, das im Wesentlichen eine Neufassung des BDSG beinhaltet. Der deutsche Gesetzgeber hielt es für erforderlich, ein „reibungsloses Zusammenspiel“ u.a. der DS-GVO mit dem „stark ausdifferenzierten deutschen Datenschutzrecht“ sicherzustellen.

III. Leitfaden und Online-Tool der EU-Kommission

Ganz aktuell sei auf einen Leitfaden und ein Online-Tool[3] verwiesen, den bzw. das die EU-Kommission am 25.01.2018 in Vorbereitung auf das Inkrafttreten der DS-GVO veröffentlicht hat. Auf diese Weise soll Bürgern, Organisationen und Unternehmen dabei geholfen werden, die neuen Bestimmungen einzuhalten und richtig zu nutzen.

Der Leitfaden fasst die wichtigsten Änderungen, die die Verordnung im Datenschutz vorsieht, zusammen und erklärt allen Akteuren die Vorteile und Chancen, die diese Bestimmungen für den Europäischen Markt mit sich bringen. Bis jetzt haben nur zwei Mitgliedstaaten - darunter Deutschland - ihre nationalen Datenschutzbestimmungen an die Verordnung angepasst. Daher fordert die Kommission die Mitgliedstaaten auf, dafür zu sorgen, dass ihre nationalen Behörden mit den notwendigen finanziellen und personellen Mitteln ausgestattet sind, um deren Unabhängigkeit und Effizienz zu gewährleisten. Sie stellt zudem

---

[1] *Kazemi/Lenhard*, Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei, 3. Aufl. 2017, Rdn. 190.
[2] BGBl. 2017 I S. 2097.
[3] Https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

1,7 Mio Euro für die Finanzierung der Datenschutzbehörden sowie für Schulungen von Datenschutz-Fachkräften bereit.

IV. Zum Inhalt der DS-GVO

Die DS-GVO bringt zum Teil weitreichende Änderungen des Datenschutzrechts mit sich und zwingt in vielen Bereichen zu einem (datenschutz-)rechtlichen Umdenken im Rechtsverständnis und vor allem in der Rechtsanwendung.

1. Gegenstand und Ziele

Art. 1 DS-GVO definiert als „Gegenstand und Ziele“, dass

- die Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten enthält,

- die Verordnung die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützt

und

- der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf.

2. Sachlicher Anwendungsbereich

Gem. Art. 2 Abs. 1 gilt die Verordnung

> „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“.

Die DS-GVO findet keine Anwendung u.a. auf die Verarbeitung personenbezogener Daten

> „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ (Abs. 2 lit. c).

3. Definitionen

Art. 4 DS-GVO klärt - wie dies in Verordnungen und Richtlinien der EU üblich ist - umfassend die Begrifflichkeiten.

a) Neue Begriffe

Dabei finden sich auch einige neue Termini.

aa) Verarbeitung

So gibt es für jeden „Umgang“ mit Daten im weitesten Sinne jetzt nur noch den Oberbegriff der „Verarbeitung“ (Art. 4 Ziff. 2). Dieser bezeichnet

> „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

bb) Verantwortlicher

Statt wie früher von „verantwortlicher Stelle“ ist jetzt von „Verantwortlicher“ (§ 4 Ziff. 7) die Rede. Dies ist

> „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

cc) Auftragsverarbeiter

Der „Auftragsverarbeiter“ (§ 4 Ziff. 8) - früher „Auftragnehmer“ - ist

> „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

b) Personenbezogene Daten

Der zentrale Begriff der DS-GVO ist der der „personenbezogenen Daten“ (Art. 4 Ziff. 1).

Dies sind

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“,

wobei als identifizierbar eine natürliche Person angesehen wird,

> „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Der unter Ziff. III. erwähnte Leitfaden der EU-Kommission stellt klar, dass auch verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, personenbezogene Daten darstellen. Personenbezogene Daten, die anonymisiert, verschlüsselt oder pseudonymisiert worden seien, aber zur erneuten Identifizierung einer Person genutzt werden könnten, blieben personenbezogene Daten und fielen in den Anwendungsbereich der Verordnung. Dagegen handele es sich bei personenbezogenen Daten, die in einer solchen Weise anonymisiert worden seien, dass die betroffene Person nicht oder nicht mehr identifiziert werden könne, nicht mehr um personenbezogene Daten. Damit die Daten wirklich anonymisiert seien, müsse die Anonymisierung unumkehrbar sein. Die Verordnung schütze personenbezogene Daten unabhängig von der zur Datenverarbeitung verwendeten Technik. Sie sei „technologieneutral“ und gelte für die automatisierte wie für die manuelle Verarbeitung, sofern die Daten nach bestimmten Kriterien (z.B. in alphabetischer Reihenfolge) geordnet seien. Außerdem sei nicht entscheidend, wie die Daten gespeichert würden – in einem IT-System, mittels Videoüberwachung

oder auf Papier. In all diesen Fällen fielen die personenbezogenen Daten unter die in der DS-GVO dargelegten Datenschutzklauseln.

Als Beispiele für personenbezogene Daten nennt der Leitfaden:

- Name und Vorname
- eine Privatanschrift
- eine E-Mail-Adresse wie (vorname.nachname@unternehmen.com)
- eine Ausweisnummer
- Standortdaten (z.B. die Standortfunktion bei Mobiltelefonen)
- eine IP-Adresse
- eine Cookie-Kennung
- die Werbekennung des Telefons
- Daten, die in einem Krankenhaus oder bei einem Arzt vorliegen, die zur eindeutigen Identifizierung einer natürlichen Person führen können.

Nicht zu den personenbezogenen Daten zählen laut Leitfaden:

- Handelsregisternummern
- eine E-Mail-Adresse wie (info@unternehmen.com)
- anonymisierte Daten.

4. Räumlicher Anwendungsbereich

Der - ausufernd weite - räumliche Anwendungsbereich ergibt sich aus Art. 3 DS-GVO. Es gilt das sog. „Marktortprinzip“,[4] welches besagt, dass jedes Unternehmen, das - von innerhalb oder außerhalb Europas - auf einen in der EU Ansässigen einwirkt, beim Umgang mit den Daten der „betroffenen Person“ die DS-GVO zu beachten hat. Ein Unternehmen, das auf EU-Ansässige einwirkt,

[4] Vgl. *Herb*, BRAK-Mitt. 2017, 209, 210.

ohne einen Sitz in Europa zu haben, muss nach Art. 27 DS-GVO einen Vertreter bestellen.

5. Handlungsanforderungen

Art. 5 DS-GVO legt die „Grundsätze für die Verarbeitung personenbezogener Daten“ fest.

Das sind - wie bisher:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Abs. 1 lit. a)
- Zweckbindung (Abs. 1 lit. b)
- Datenminimierung (Abs. 1 lit. c)
- Richtigkeit (Abs. 1 lit. d)
- Speicherbegrenzung (Abs. 1 lit. e)
- Integrität und Vertraulichkeit (Abs. 1 lit. f).

Neu und brisant ist, dass der Verantwortliche gem. Art. 5 Abs. 2 DS-GVO für die Einhaltung des Abs. 1 nicht nur verantwortlich ist, sondern

> einer „Rechenschaftspflicht“ unterliegt, d.h. die Einhaltung von Abs. 1 „nachweisen“ können (muss).

Auf die „sichere Seite“ kann sich dabei bringen, wer etwa die Verhaltensregeln eines (Berufs-)Verbandes (Art. 40, 41 DS-GVO) beherzigt und sich selbst zertifizieren lässt (Art. 42, 43 DS-GVO) und/oder ausschließlich mit anderen zertifizierten Anbietern zusammenarbeitet.

6. Verbot mit Erlaubnisvorbehalt

Das auch bislang schon geltende Verbot mit Erlaubnisvorbehalt wurde beibehalten. Nach Art. 6 Abs. 1 DS-GVO ist die Verarbeitung von Daten (vgl. oben Ziff. IV. 3. a aa) nur rechtmäßig, wenn

- die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat, und/oder

- die Verarbeitung für die Erfüllung eines Vertrags, dessen Partei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen, und/oder

- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt, und/oder

- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, und/oder

- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, und/oder

- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (nicht: von Behörden in Erfüllung ihrer Aufgaben) erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person (in Sonderheit eines Kindes), die den Schutz personenbezogener Daten erfordern, überwiegen.

Die Erfüllung **einer** dieser Voraussetzungen reicht aus.

7. Anforderungen an eine Einwilligung

Beruht die Datenverarbeitung auf einer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) trifft gem. Art. 7 Abs. 1 DS-GVO wiederum den Verantwortlichen die Pflicht des Nachweises, dass die Einwilligung tatsächlich vorliegt.

Außerdem müssen im Falle einer schriftlichen Einwilligung, die den Nachweis ja grundsätzlich erleichtern würde, bestimmte weitere Voraussetzungen (Verständlichkeit des Ersuchens um die schriftliche Einwilligung, klare Trennung von anderen Sachverhalten, Koppelungsverbot - Art. 7 Abs. 2 DS-GVO) erfüllt sein.

Die Einwilligung kann, worauf die betroffene Person auch ausdrücklich hinzuweisen ist, gem. Art. 7 Abs. 3 DS-GVO jederzeit widerrufen werden.

Nicht leicht „verdaulich“ ist Art. 7 Abs. 4 DS-GVO, der lautet:

> „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“

Hier fühlt man sich unweigerlich an die „Opt-in“- und „Opt-out“-Diskussionen bei der seinerzeitigen Neufassung des UWG und an die immer noch praktizierte „Friss oder stirb-Methode“ vieler Internetanbieter und Suchmaschinen-Betreiber erinnert. Wer hat schon Lust und Zeit, sich mit den Feinheiten von Nutzungsbedingungen zu befassen, wenn er dringend etwas „googeln“ möchte, ihn von der Anzeige der erwünschten Suchergebnisse aber ein paar (lästige) datenschutzrechtliche Kenntnisnahmen und Zustimmungserklärungen trennen, die in Ermangelung einer Alternative routinemäßig abgegeben werden?

Buchner/Kühling[5] führen denn auch aus, dass mit Art. 7 Abs. 4 DS-GVO nicht generell untersagt sei, dass Anbieter ihre Leistung im Sinne eines „take it or leave it“ davon abhängig machten, dass die betroffene Person auch in die Verarbeitung ihrer personenbezogenen Daten einwillige. Als unfreiwillig und damit unwirksam sei eine solchermaßen eingeholte Einwilligung vielmehr „tendenziell“ nur dann einzuordnen, wenn sie eine Datenverarbeitung legitimieren solle, die über das hinausgehe, was für eine Vertragserfüllung erforderlich sei. Zwingend sei allerdings auch dies keineswegs, da dieser Erforderlichkeitszusammenhang „lediglich maßgeblich“ zu berücksichtigen sei, nicht aber zwingend zum Ausschluss der Freiwilligkeit führe. Zulässig sei es daher insbesondere, die Leistungserbringung von der Erteilung einer Einwilligung in die Datenverarbeitung abhängig zu machen, wenn erst diese Datenverarbeitung die notwendige Entscheidungs- und Kalkulationsgrundlage für das konkrete Rechtsgeschäft biete.

8. Rechte und Pflichten

Die Rechte der betroffenen Personen, deren Persönlichkeitsrecht geschützt werden soll, und damit korrespondierend die Pflichten des Verantwortlichen sind in Kapitel III der DS-GVO (also in den Art. 12 bis 23) dezidiert niedergelegt.

---

[5] In: Kühling/Buchner, Kommentar zur Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 7 DS-GVO Rdn. 46 ff.

a) „Transparenz und Modalitäten“

Der 1. Abschnitt von Kapitel III enthält mit Art. 12 nur eine einzige Vorschrift, welche mit „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ überschrieben ist.

Nach Art. 12 Abs. 1 S. 1 DS-GVO muss der Verantwortliche geeignete Maßnahmen ergreifen, um der betroffenen Person alle für sie wesentlichen, auf die Datenverarbeitung bezogenen Informationen und Mitteilungen

> „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln.

Dies erfolgt grundsätzlich schriftlich oder in anderer Form, ggf. auch elektronisch (Abs. 1 S. 2). Auf Verlangen des Betroffenen kann die Information allerdings auch mündlich erteilt werden, sofern die Identität der betroffenen Person (also des Gesprächspartners) in anderer Form nachgewiesen wurde (Abs. 1 S. 3).

Auch die Verwendung von Bildsymbolen kommt in Betracht (Abs. 7), wobei die EU-Kommission hierzu (insbesondere zur Festlegung verbindlicher Bildsymbole) nähere Regelungen erlassen kann (Abs. 8).

b) Datenerhebung

Der 2. Abschnitt von Kapitel III regelt die konkreten Informationspflichten und Auskunftsrechte bei der Erhebung personenbezogener Daten, wobei zu unterscheiden ist zwischen der Datenerhebung unmittelbar bei der betroffenen Person und einer anderweitigen Erhebung.

aa) Erhebung bei der betroffenen Person

Werden - wie dies insbesondere im Rechtsanwalt/Mandanten-Verhältnis unerlässlich ist - „personenbezogene Daten bei der betroffenen Person erhoben“, trifft den Verantwortlichen nach Art. 13 DS-GVO die Pflicht zu einer Reihe besonderer Mitteilungen an den Betroffenen, deren wichtigste sind:

- der Name und die Kontaktdaten des Verantwortlichen (sowie ggf. seines Vertreters) (Abs. 1 lit. a)

- ggf. die Kontaktdaten eines zu bestellenden Datenschutzbeauftragten (Abs. 1 lit. b)

- die Zwecke, für welche die personenbezogenen Daten verarbeitet werden sollen, und die Rechtsgrundlage der Verarbeitung (Abs. 1 lit. c)

- die Dauer, für welche die Daten gespeichert werden (oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer) (Abs. 2 lit. a)

- das Bestehen eines Rechts auf Auskunft, auf Berichtigung oder Löschung, auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts (Abs. 2 lit. b)

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (Abs. 2 lit. d).

Die aktive, vollständige und rechtzeitige Unterrichtung der betroffenen Person (etwa des Mandanten) ist Voraussetzung einer ordnungsgemäßen Datenerhebung. Eine Verletzung der entsprechenden Pflichten kann gem. Art. 83 Abs. 5 lit. b DS-GVO eine Geldbuße (in beträchtlicher Höhe) zur Folge haben.[6]

Die Bestimmung der Reichweite der Informationspflichten kann im Einzelnen schwierig sein. So führt etwa *Bäcker*[7] zur in Art. 13 Abs. 1 lit. c DS-GVO geforderten Information über die Rechtsgrundlage der Datenverarbeitung aus, ein schlichtes Zitieren oder die wörtliche Wiederholung des jeweils einschlägigen Erlaubnistatbestands aus Art. 6 DS-GVO ermögliche es der betroffenen Person in der Regel nicht, ihre rechtliche Position gegenüber der Datenverarbeitung einzuschätzen. Denn zum einen seien die Erlaubnistatbestände in Art. 6 Abs. 1 DS-GVO durchweg sehr offen formuliert. Und zum anderen könne das Zusammenwirken von Art. 6 Abs. 1 lit. c (und e) DS-GVO mit den hierzu ergangenen Rechtsvorschriften komplexe Zuordnungsfragen aufwerfen. Die Informationspflicht sei darum weiter zu verstehen, damit sie ihren Zweck erfülle. Der Verantwortliche müsse der betroffenen Person zumindest dann, wenn es wegen der Komplexität der Rechtslage oder aufgrund der erkennbaren Eigenschaften und Kenntnisse der betroffenen Person geboten sei, die Rechtslage „einzelfallbezogen und vollständig“ darlegen. Dazu müsse der Verantwortliche die Rechtsgrundlage der Datenverarbeitung so erläutern, dass die betroffene Per-

[6] *Bäcker*, in: Kühling/Buchner, aaO, Art. 13 DS-GVO Rdn. 61.
[7] AaO, Art. 13 DS-GVO Rdn. 26.

son deren Anwendung auf ihren Fall nachvollziehen könne. Zumindest aber sei eine solche Erläuterung geboten, wenn die betroffene Person sie verlange.

In Erwägungsgrund 60 der DS-GVO heißt es, die Grundsätze einer fairen und transparenten Verarbeitung machten es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet werde. Der Verantwortliche sollte der betroffenen Person dabei alle „weiteren Informationen“ zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet würden, notwendig seien, um eine faire und transparente Verarbeitung zu gewährleisten. Wie so oft im EU-Recht sind die gewählten Formulierungen hinsichtlich ihres Grades an Abstraktion kaum zu überbieten.

Für den Rechtsanwalt kann es nicht schaden, wenn er den Mandanten etwa darüber aufklärt,

- dass er gem. § 50 BRAO (hierzu näher unter Ziff. VI. 1.) verpflichtet ist, Handakten zu führen und für eine bestimmte Dauer aufzubewahren

- welche Informationen in diesen Handakten gesammelt werden

- wie er die jeweilige Handakte führt (in Papierform und/oder elektronisch)

- wo und wie (z.B. in einem Mandantenregister) sonst noch mandatsbezogene Daten gespeichert und verarbeitet werden

- wer außer ihm selbst zu der jeweiligen Handakte und den außerhalb derselben gespeicherten und verarbeiteten Daten Zugang hat

- welche Maßnahmen er ergriffen hat, um sicherzustellen, dass sämtliche Personen, die mit der Handakte und den sonst gespeicherten und verarbeiteten Daten in Kontakt gelangen, sorgfältig ausgewählt, unterwiesen, überwacht und zur Verschwiegenheit verpflichtet (möglicherweise auch zertifiziert) sind (vgl. hierzu noch näher unter Ziff. VI. 2.)

- ob es ggf. dritte Stellen gibt, die er (z.B. im Rahmen eines Akteneinsichtsgesuchs bei einer Behörde) vom Bestehen des Mandatsverhältnisses unterrichten muss, um dieses verantwortlich führen zu können

- auf welche Weise und durch wen die Handakten etc. nach Ablauf der Aufbewahrungsfrist datensicher entsorgt werden.

Korrespondierend zur Informationspflicht des Verantwortlichen hat die betroffene Person das Recht auf Auskunft. Dieses umfasst gem. Art. 15 Abs. 1 Hs. 1 DS-GVO zunächst das Recht, zu erfahren, also von dem Verantwortlichen eine Bestätigung darüber zu erlangen, ob die eigene Person betreffende personenbezogene Daten verarbeitet werden.

Ist dies der Fall, besteht ferner das Recht auf Auskunft darüber, welche konkreten Daten dies sind, und auf u.a. folgende Informationen:

- die Verarbeitungszwecke (Abs. 1 lit. a)

- die geplante Dauer, für welche die Daten gespeichert werden (oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer) (Abs. 1 lit. d)

- das Bestehen eines Rechts auf Berichtigung oder Löschung, auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts (Abs. 1 lit. e)

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (Abs. 1 lit. f).

Dem besonderen Schutz der DS-GVO unterliegen bei alledem Kinder (vgl. Erwägungsgrund 38). Allerdings gilt dies in erster Linie dann, wenn sie selbst die Rolle von Konsumenten und „Datenlieferanten“ spielen.[8]

Für Rechtsanwälte gilt, dass die Verletzung einer gesetzlichen Pflicht immer auch einen Verstoß gegen die Generalklausel des § 43 BRAO darstellen kann, der eine berufsrechtliche Ahndung nach sich zieht.

bb) Anderweitige Erhebung

Werden die personenbezogenen Daten nicht bei der betroffenen Person selbst (sondern z.B. beim Gegner) erhoben, sind der betroffenen Person nach Art. 14 DS-GVO zusätzlich zu den unter lit. aa bereits aufgezählten Informationen u.a. mitzuteilen:

[8] Vgl. zu der in diesem Zusammenhang wichtigen Einbindung der „Träger der elterlichen Verantwortung“ *Buchner/Kühling*, in: Kühling/Buchner, aaO, Art. 8 DS-GVO Rdn. 20 f. u. 23 ff.

- (in jedem Fall) die Kontaktdaten des Datenschutzbeauftragten (Abs. 1 lit. b)

- u.U. (wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DS-GVO beruht) die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden (Abs. 2 lit. d)

- aus welcher Quelle die personenbezogenen Daten stammen (und ggf. ob sie aus öffentlich zugänglichen Quellen stammen) (Abs. 2 lit. f).

Art. 14 Abs. 5 DS-GVO benennt Ausschlusstatbestände, darunter in lit. d den Schutz des Berufsgeheimnisses, der nach *Bäcker*[9] etwa greift, wenn ein Arzt von einem Patienten therapeutisch bedeutsame Gesundheitsdaten über dessen Familienangehörige erhält.

Insgesamt schließen nach *Bäcker*[10] Berufsgeheimnisse, welche Vertrauensverhältnisse zwischen privaten Dienstleistern und ihren Kunden schützten, die Informationspflichten grundsätzlich vollumfänglich aus. Denn diesen Berufsgeheimnissen unterfalle regelmäßig bereits die Tatsache, dass der Berufsgeheimnisträger und der Begünstigte miteinander in vertraulichen Kontakt getreten seien. Zumeist würden bereits Teilinformationen Rückschlüsse auf diese Tatsache zulassen. Auch Rechtsanwälte haben demzufolge gegenüber Gegnern, Zeugen und sonstigen „Drittbetroffenen“, deren Daten sie im Rahmen einer Mandatsführung zwangsläufig verarbeiten (etwa in einen Schriftsatz einflechten) keine Informationspflichten. Dies ergibt sich auch aus § 29 Abs. 1 u. 2 BDSG-2018 (siehe hierzu näher unter Ziff.VI. 2. a aa) und nicht zuletzt aus den Zeugnisverweigerungsrechten und der Beschlagnahmefreiheit (also den sog. Anwaltsprivilegien), die andernfalls ihres Sinns entkleidet und weitgehend leerlaufen würden.

Soweit es in familienrechtlichen Mandaten um die Daten minderjähriger Kinder geht, sind die Eltern (bzw. ein Elternteil, u.U. auch ein Verfahrenspfleger) Garanten für den nach der DS-GVO erforderlichen besonderen Schutz. Der Rechtsanwalt ist hier nur ausnahmsweise zur Ergreifung weiterer Maßnahmen veranlasst, wenn er erkennt, dass die Eltern ihrer entsprechenden Fürsorgepflicht nicht gerecht werden.

Korrespondierend zur Informationspflicht ergibt sich das Auskunftsrecht der betroffenen Person, deren Daten vom Verarbeiter nicht bei ihr selbst erhoben wurden, wiederum aus Art. 15 DS-GVO (siehe zuvor unter lit. aa).

---

[9] In: Kühling/Buchner, aaO, Art. 14 DS-GVO Rdn. 68, 69.
[10] In: Kühling/Buchner, aaO, Art. 14 DS-GVO Rdn. 70.

c) Recht auf „Vergessenwerden“

Art. 17 DS-GVO sieht als - neues - Korrelat zu den allgemeinen Löschpflichten in bestimmten Situationen bzw. aus verschiedenen Gründen zum einen das Recht der betroffenen Person, die unverzügliche Löschung der sie betreffenden Daten zu verlangen, und zum anderen die Pflicht des Verantwortlichen vor, die Löschung unverzüglich vorzunehmen.

Der wichtigste Grund hierfür ist der Wegfall der Notwendigkeit des Vorhalts der Daten, also die Situation, dass die Daten „für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig (sind)“ (Abs. 1 lit. a).

Das ist eigentlich beim Ende der Mandatsbeziehung (aufgrund Erledigung des Auftrags oder einseitiger Kündigung einer der Vertragsparteien) der Fall. Allerdings trifft § 50 BRAO insofern Sonderregelungen, auf die später noch näher einzugehen sein wird (vgl. zur erforderlichen Öffnung für mitgliedstaatsspezifische Sonderregelungen Art. 17 Abs. 3 lit. b DS-GVO).

Auch die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen kann eine längere Aufbewahrung bzw. „Verarbeitung“ von Daten erforderlich machen (Art. 17 Abs. 3 lit. e).

d) Recht auf Einschränkung der Verarbeitung

Unterhalb der Schwelle des Löschens sieht Art. 18 DS-GVO unter bestimmten Voraussetzungen das Recht auf Einschränkung der Datenverarbeitung vor.

Das betrifft die Fälle, in denen aufgrund bestimmter Aufbewahrungsfristen (z.B. der deutschen Abgabenordnung) zwar ein Teil (etwa die Rechnungsunterlagen aus einem Mandat), nicht aber sämtliche Daten aufbewahrt werden müssen und folglich auch nicht aufbewahrt werden dürfen.

f) Recht auf Datenübertragbarkeit

Neu ist das in Art. 20 DS-GVO geregelte Recht der betroffenen Person, die sie betreffenden Daten „in einem strukturierten, gängigen und maschinenlesbaren Format“ zu erhalten und diese Daten entweder selbst an einen anderen „Ver-

antwortlichen“ weiterzuleiten oder den (bisherigen) Verantwortlichen zu veranlassen, den unmittelbaren Datentransfer an den neuen Verantwortlichen zu veranlassen.

Wie dabei die berechtigten Interessen (z.B. auf Erhalt der Vergütung und Geltendmachen eines Zurückbehaltungsrechts) des ursprünglich Verantwortlichen zu wahren sind, ist zweifelhaft. Im Anwaltsalltag stellt sich durchaus häufiger die Situation, dass ein unzufriedener Mandant einen neuen Rechtsanwalt beauftragt, die Gebühren des bisherigen Anwalts nicht zahlt, diesen aber gleichwohl auffordert, alle Mandatsunterlagen dem neu beauftragten Kollegen zu übermitteln. Das konnte und kann der „Alt-Anwalt“ (unter Hinweis auf sein berufs- und zivilrechtlich gewährleistetes Zurückbehaltungsrecht - § 50 Abs. 3 S. 1 BRAO, §§ 675, 273 Abs. 1 BGB) von Extremfällen abgesehen verweigern.

Lehnt ein Verantwortlicher i.S. der DS-GVO die Weiterleitung der Daten (auf elektronischem Wege und kostenlos) ab, muss er dies gegenüber der betroffenen Person begründen (Art. 12 Abs. 4 DS-GVO) und auf die weiteren Durchsetzungsmöglichkeiten, nämlich auf einen gerichtlichen Rechtsbehelf und vor allem auch auf die Beschwerde bei der zuständigen Aufsichtsperson, hinweisen.[11]

Welche Daten von dem Recht auf Übertragung im Einzelnen erfasst sind, ist nicht einfach festzustellen. Grundsätzlich geht es nur um Daten, die vom Anspruchsinhaber bereitgestellt wurden. Damit wären die in Anwalts-Unterlagen enthaltenen eigenen Aufzeichnungen des Sachbearbeiters ebenso wie Schriftsätze der Gegenseite, Entscheidungen von Gerichten und Behörden u.Ä. nicht umfasst.[12] Noch anders als Art. 20 DS-GVO zwischen den von der betroffenen Person bereitgestellten und sonstigen Daten unterscheidet, differenziert der neu gefasste § 50 BRAO zwischen „Dokumenten, die der Rechtsanwalt aus Anlass seiner beruflichen Tätigkeit von dem Auftraggeber oder für ihn erhalten hat“ (Letzteres sind auch Schriftstücke anderer) und den „Handakten“. Nur die Handakten im engeren Sinne müssen ein geordnetes und zutreffendes Bild über die Auftragsbearbeitung des Anwalts abgeben und sechs Jahre aufbewahrt werden (vgl. hierzu noch näher unter Ziff. VI. 1.).

9. Auftragsdatenverarbeitung

[11] *Herbst*, in: Kühling/Buchner, aaO, Art. 20 DS-GVO Rdn. 33.
[12] Vgl. *Herbst*, in: Kühling/Buchner, aaO, Art. 20 DS-GVO Rdn. 11, der ein vollständiges Chat-Protokoll, das neben Äußerungen der betroffenen Person auch Äußerungen anderer Personen enthält, nicht als Gegenstand des Anspruchs auf Datenübertragbarkeit bezeichnet.

Für die Auftragsdatenverarbeitung, also die Situation, dass sich der Verantwortliche eines Dritten bedient, stellt Art. 28 DS-GVO strenge Regelungen auf. Der Verantwortliche darf nur mit solchen Auftragsverarbeitern arbeiten,

> „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“ (Abs. 1).

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt gem. Art. 28 Abs. 3 DS-GVO in der Regel auf der Grundlage eines Vertrags, in dem festgelegt sind

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- die Art der personenbezogenen Daten
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen.

Der Vertrag muss u.a. vorsehen, dass der Auftragsverarbeiter

- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen (Abs. 3 lit. b)
- alle gem. Art. 32 erforderlichen Sicherheits-Maßnahmen ergreift (Abs. 3 lit. c)
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht oder dazu beiträgt (Abs. 3 lit. h).

Gem. Art. 29 DS-GVO dürfen der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, welche Zugang zu per-

sonenbezogenen Daten hat, diese Daten grundsätzlich ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Die besonderen Anforderungen an Auftragsverarbeiter, deren „Mitarbeiter“ (im weitesten Sinne) und Verantwortliche, welche Auftragsverarbeiter in Anspruch nehmen, sind inzwischen auch - jedenfalls weitgehend - in den neugefassten §§ 203 StGB, 43a Abs. 2 und 43e BRAO sowie 2 BORA abgebildet (siehe hierzu noch näher unter Ziff. VI. 2. b).

10. Melde- und Benachrichtigungspflichten bei Verletzung des Schutzes personenbezogener Daten

Geht „etwas schief“ (etwa weil ein Hackerangriff erfolgte, der Mitarbeiter eines Verantwortlichen unbefugt vertrauliche Daten offenbarte oder eine Akte unauffindbar ist), muss der Verantwortliche dies gem. Art. 33 Abs. 1 S. 1 DS-GVO grundsätzlich „unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde“, der zuständigen Aufsichtsbehörde melden.

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, hat er dies unverzüglich dem Verantwortlichen zu melden (Art. 33 Abs. 2 DS-GVO).

Für den Fall, dass die Verletzung des Schutzes personenbezogener Daten „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge (hat)“, muss gem. Art. 34 Abs. 1 DS-GVO der Verantwortliche die betroffene Person selbst unverzüglich „in klarer und einfacher Sprache“ (Art. 34 Abs. 2) von der Verletzung unterrichten.

11. Datenschutz-Folgenabschätzung

Art. 35 Abs. 1 S. 1 DS-GVO erlegt dem Verantwortlichen die Pflicht auf, vorab „eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ durchzuführen, sofern eine Form der Verarbeitung von Daten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Dabei ist der Rat des Datenschutzbeauftragten (soweit vorhanden) einzuholen (Art. 35 Abs. 2 DS-GVO).

Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Datenverarbeitung ein hohes Risiko zur Folge hätte, muss der Verantwortliche vor der Verarbeitung grundsätzlich die Aufsichtsbehörde konsultieren (Art. 36 Abs. 1 DS-GVO).

12. Datenschutzbeauftragte

Der vierte Abschnitt von Kapitel III der DS-GVO regelt Benennung (Art. 37), Stellung (Art. 38) und Aufgaben des Datenschutzbeauftragten (Art. 39).

Diese Regelungen werden in Deutschland durch nähere Bestimmungen im neuen BDSG-2018 (§§ 5 bis 7, 38) ergänzt, sodass sich gegenüber dem bisherigen Rechtszustand nichts ändert (siehe hierzu näher unter Ziff. V.).

Gem. § 38 Abs. 1 BDSG-2018 müssen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Mit der Datenverarbeitung ist jeder befasst, der „am PC sitzt“,[13] weshalb auch schon mittelgroße Anwaltskanzleien einen betrieblichen Datenschutzbeauftragten bestellen müssen.

Neu ist, dass nach Art. 37 Abs. 7 DS-GVO der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten (z.B. auf der Homepage) veröffentlichen und der Aufsichtsbehörde mitteilen muss.

13. Aufsichtsbehörden

[13] *Herb*, BRAK-Mitt. 2017, 209, 212.

Die in den Art. 51 bis 76 DS-GVO geregelten Aufgaben und Befugnisse der Aufsichtsbehörden wurden erheblich ausgeweitet.

Der Grundsatz findet sich in Art. 51 Abs. 1 DS-GVO, wonach jeder Mitgliedstaat vorsieht,

> „dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird".

1. Die Situation in Deutschland

In Deutschland ist - nicht zuletzt aufgrund seiner föderalen Struktur und anders als in den meisten übrigen Mitgliedstaaten, die nur eine einzige Aufsichtsbehörde eingerichtet haben - die Situation komplex. Es gibt den Bundesdatenschutzbeauftragten (zurzeit: die Bundesdatenschutzbeauftragte), der/die u.a. für die Bundesbehörden und die Postdienstleistungen zuständig ist, die Datenschutzbeauftragten der Länder und außerdem eigenständige „sektorale" Aufsichtsbehörden für bestimmte Bereiche (etwa die Kirchen).

2. Vorschlag der Bundesrechtsanwaltskammer

Die Anwaltschaft konnte sich mit ihrer Forderung nach einer eigenen Aufsichtsbehörde bislang noch nicht durchsetzen. Die Bundesrechtsanwaltskammer hatte die Einfügung eines § 191g („Datenschutzbeauftragter der Rechtsanwaltschaft") in die BRAO vorgeschlagen, der lauten sollte:[14]

> „(1) Der Datenschutzbeauftragte der Rechtsanwaltschaft ist für alle Mitglieder der Rechtsanwaltskammern die datenschutzrechtliche Kontrollstelle entsprechend den europarechtlichen Vorgaben. Die Kontrolle erstreckt sich auf alle datenschutzrechtlichen Vorschriften einschließlich derer im Bereich der Telemedien und Telekommunikation; auch insoweit tritt er an Stelle anderer Kontrollstellen. Für ihn gelten die für Kontrollstellen gesetzlich vorgesehenen Aufgaben sowie Rechte und Pflichten einschließlich der Zeugnisverweigerungsrechte. Er kann Bußgelder entsprechend den Bestimmungen des Bundesdatenschutzgesetzes erheben.

[14] BRAK-Stellungnahme 41/2016 aus Dezember 2016.

(2) Der Datenschutzbeauftragte der Rechtsanwaltschaft kann Maßnahmen zur Gewährleistung der Einhaltung datenschutzrechtlicher Vorschriften anordnen. Soweit damit auch berufsrechtliche Regelungen getroffen werden müssen, unterrichtet er die Rechtsanwaltskammern, damit diese tätig werden. Für individuell zurechenbare Amtshandlungen können nach Maßgabe einer von der Satzungsversammlung genehmigten Verordnung Gebühren und Auslagen festgesetzt werden.

(3) Der Datenschutzbeauftragte der Rechtsanwaltschaft wird bei der Bundesrechtsanwaltskammer eingerichtet und ist in Ausübung des Amtes völlig unabhängig, nur dem Gesetz unterworfen und unterliegt keiner Rechts-, Fach- oder Dienstaufsicht. Ihm ist die für die Erfüllung der Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen.

(4) Die Satzungsversammlung der Bundesrechtsanwaltskammer wählt mit Zustimmung der Hauptversammlung einen Datenschutzbeauftragten der Rechtsanwaltschaft. Der Datenschutzbeauftragte der Rechtsanwaltschaft muss eine mindestens fünfjährige Berufserfahrung als Rechtsanwalt besitzen.

(5) Die Amtszeit beträgt fünf Jahre; eine Wiederwahl ist einmalig zulässig.

(6) Der Datenschutzbeauftragte der Rechtsanwaltschaft bestellt mit Zustimmung der Satzungsversammlung und der Hauptversammlung einen Vertreter.

(7) Der Datenschutzbeauftragte der Rechtsanwaltschaft kann vorzeitig mit 2/3 Mehrheit von der Satzungsversammlung aus dem Amt entlassen werden, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Beendigung des Amtsverhältnisses rechtfertigen.

(8) Der Datenschutzbeauftragte der Rechtsanwaltschaft darf seinen Beruf als Rechtsanwalt nicht ausüben. Er darf auch keiner anderen abhängigen Beschäftigung nachgehen oder einem Vorstand einer Rechtsanwaltskammer, der Satzungsversammlung oder einem Anwaltsgericht angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten in Datenschutzangelegenheiten abgeben.

(9) Der Datenschutzbeauftragte der Rechtsanwaltschaft veröffentlicht alle zwei Jahre einen Bericht über die Tätigkeit.

(10) Der Datenschutzbeauftragte der Rechtsanwaltschaft ist, auch nach Beendigung seiner Tätigkeit, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren.“

In der Begründung ihres Vorschlags führt die BRAK aus, die Schaffung einer eigenständigen, sektoralen Datenschutzaufsicht sei zur Gewährleistung des Datenschutzes und insbesondere des Mandatsgeheimnisses zwingend erfor-

derlich. Anstelle von 16 staatlichen Aufsichtsbehörden solle mit § 191g BRAO-E eine anwaltsspezifische Kontrollstelle, der Bundesdatenschutzbeauftragte für die Rechtsanwaltschaft, errichtet werden. Sektorale Kontrollstellen gebe es ja auch bereits im Bereich der Medien und der Kirchen.

Mit § 191g Abs. 1 BRAO-E werde klargestellt, dass die oder der Bundesdatenschutzbeauftragte für die Rechtsanwaltschaft eine Kontrollstelle entsprechend dem aktuellen Art. 28 EG-Datenschutz-Richtlinie (bzw. eine Kontrollstelle nach der EU-Datenschutz-Grundverordnung) sei und für sie oder ihn die dortigen Anforderungen gölten. Ihre/seine Kontrollkompetenz solle umfassend für alle anwaltlichen Tätigkeiten gelten. Damit wären weder die Konkurrenz mit anderen allgemeinen Datenschutz-Kontrollorganen (wie z.B. den Bundes- oder Landesdatenschutzbeauftragten) noch mit spezifischen Aufsichtsorganen (wie z.B. der Bundesnetzagentur für den Bereich der Telekommunikation) vereinbar, weshalb es einer entsprechenden Klarstellung in Satz 2 bedürfe.

Wie bereits erwähnt, war dem Vorstoß der BRAK bislang kein Erfolg beschieden.

3. Befugnisse der Aufsichtsbehörde(n)

Art. 58 DS-GVO stattet die jeweilige Aufsichtsbehörde mit umfangreichen Untersuchungs-, Abhilfe- und Genehmigungs-Befugnissen aus, die es ihr u.a. gestatten,

- den Verantwortlichen, den Auftragsverarbeiter und ggf. den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind (Abs. 1 lit. a)

- Untersuchungen in Form von Datenschutzprüfungen durchzuführen (Abs. 1 lit. b)

- von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten (Abs. 1 lit. e)

- einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstoßen hat (Abs. 2 lit. b)

- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge ggf. auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen (Abs. 2 lit. d)

- den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen (Abs. 2 lit. e)

- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen (Abs. 2 lit. f)

- eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle zur Vornahme entsprechender Maßnahmen anzuweisen (Abs. 2 lit. h)

- eine Geldbuße (gem. Art. 83 DS-GVO) zu verhängen (Abs. 2 lit. i)

- Zertifizierungsstellen (gem. Art. 43 DS-GVO) zu akkreditieren (Abs. 3 lit. e)

- (im Einklang mit Art. 42 Abs. 5 DS-GVO) Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen (Abs. 3 lit. f).

14. Haftung und Sanktionen

Kapitell VIII der DS-GVO regelt in Art. 77 bis 84 die „Rechtsbehelfe, Haftung und Sanktionen“.

Gem. Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter.

Und nach Art. 82 Abs. 2 S. 1 haftet jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wurde. Es wird im Vergleich zur bisherigen Rechtslage mit einem Anstieg der Haftungsfälle und der - insbesondere auch für immaterielle Schäden - zugesprochenen Haftungssummen gerechnet. Dies wirke sich auch auf die Zielvorgaben von Projekten aus. Künftig müsse es eines der wesentlichen Projektziele sein, die Verteidigung des jeweiligen Unternehmens (=

Verarbeiters) gegen Schadensersatzforderungen oder Ermittlungen von Datenschutzbehörden vorzubereiten.[15]

Ein Auftragsverarbeiter haftet nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten nicht nachgekommen ist oder unter Nichtbeachtung der regelmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat (Art. 82 Abs. 2 S. 2 DS-GVO).

Art. 83 DS-GVO sieht die Verhängung von Geldbußen vor, die „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein muss.

Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde (gem. Art. 58 Abs. 2 DS-GVO) können Geldbußen von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist.

V. Deutsches Datenschutzrecht

Unter Ausnutzung der in der DS-GVO (zahlreich) enthaltenen Öffnungsklauseln für eigene legislative Aktivitäten einerseits und in Erfüllung der konkreten, an die Mitgliedstaaten gerichteten Regelungsaufträge andererseits und schließlich auch in Umsetzung der Richtlinie (EU) 2016/680[16] hat der deutsche Gesetzgeber das *„Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“*[17] geschaffen.

Sein wesentlicher Bestandteil, das BDSG-2018, soll dabei grundsätzlich auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes Anwendung finden, die von der nur für die Privatwirtschaft geltenden DS-GVO nicht erfasst werden.

Auch in den Ländern müssen die notwendigen Anpassungen vorgenommen werden - in Nordrhein-Westfalen etwa durch das in Vorbereitung befindliche

---

[15] *Wybitul/Haß/Albrecht*, NJW 2018, 113, 115, 117.

[16] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates - Abl. L 119 v. 04.05.2016, S. 89.

[17] BGBl. 2017 I S. 2097 - in der Kurzfassung: Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU).

„Nordrhein-Westfälische Datenschutz-Anpassungs- und Umsetzungsgesetz EU (NRWDSAnpUG-EU)“.

VI. Deutsches anwaltliches Berufsrecht

Für Rechtsanwälte ist und bleibt natürlich auch die Bundesrechtsanwaltsordnung maßgeblich. Berührungspunkte mit der DS-GVO gibt es insbesondere bei den Themen Handaktenführung, Verschwiegenheit und (Legal) Outsourcing.

1. Handakten

Nach § 50 Abs. 1 BRAO n.F. ist der Rechtsanwalt nicht nur berechtigt, sondern ausdrücklich verpflichtet, die Daten seiner Mandanten zu erfassen, zu bearbeiten und für eine bestimmte Zeitdauer aufzubewahren. Er muss „durch das Führen von Handakten ein geordnetes und zutreffendes Bild über die Bearbeitung seiner Aufträge geben können“ (Abs. 1 S. 1).

Damit wurde die Vorschrift durch das *„Gesetz zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Berufe“* („kleine BRAO-Reform“) vom 12.05.2017[18] gegenüber dem früheren Rechtszustand sogar noch verschärft und - zumindest vom Ansatz her - der für Wirtschaftsprüfer geltenden Regelung des § 51b WPO angepasst. Der Gesetzgeber spricht in diesem Zusammenhang von der Notwendigkeit, die Tätigkeit des Rechtsanwalts „im Wege der Aufsicht überprüfen zu können“, ohne allerdings zu sagen, was er konkret meint.[19]

Die Dauer der Pflicht zur Aufbewahrung der Handakten ist jetzt in § 50 Abs. 1 S. 2 BRAO (statt wie früher in Abs. 2 S. 1) geregelt und von fünf Jahren auf sechs Jahre verlängert worden. Aus der „Standort-Verschiebung“ ergibt sich zugleich, dass der Anwalt von der Pflicht zur Aufbewahrung der Handakte als solcher nicht mehr durch seinen Mandanten entbunden werden kann, indem der Mandant die Handakte abholt oder auf eine Aufforderung zur Abholung nicht binnen sechs Monaten reagiert. Für die Dauer von sechs Jahren muss die Handakte im engeren Sinne – unabhängig von diesbezüglichen Wünschen des Mandanten – „zum Zweck der Aufsicht zur Verfügung stehen“.[20] Selbst wenn der Mandant den Anwalt ausdrücklich auffordert, sämtliche Mandatsunterlagen

[18] BGBl. 2017 I S. 1121.
[19] BT-Drucks. 18/9521, S. 115. Zu einer Reihe ungeklärter Fragen in Zusammenhang mit § 50 BRAO n.F. vgl. *Offermann-Burckart*, AnwBl. Online 2017, 238, 244 f.
[20] BT-Drucks. 18/9521, S. 115.

zu vernichten, bleibt die Aufbewahrungspflicht des § 50 Abs. 1 S. 2 BRAO bestehen. Gleiches gilt für Aufbewahrungspflichten nach der Abgabenordnung (z.B. nach § 147 Abs. 1 Nr. 1, 4 u. 4a, Abs. 3 S. 1 AO - zehn Jahre) und dem Geldwäschegesetz (§ 8 Abs. 4 S. 1 GWG - fünf Jahre). Die streng aufbewahrungspflichtige Handakte im engeren Sinne ist zu unterscheiden von den Dokumenten, „die der Rechtsanwalt aus Anlass seiner beruflichen Tätigkeit von dem Auftraggeber oder für ihn erhalten hat“ (§ 50 Abs. 2 S. 1 BRAO). Diese Dokumente hat der Anwalt grundsätzlich auch weiterhin auf Verlangen des Mandanten (also unabhängig von Zeitvorgaben des Gesetzgebers) herauszugeben.

Die Aufbewahrungsfrist beginnt gem. § 50 Abs. 1 S. 3 BRAO jetzt nicht mehr mit Beendigung des Auftrags, sondern mit Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde. Diese Neuerung soll es laut amtlicher Begründung den Rechtsanwälten ermöglichen, nur einmal am Jahresende die Vernichtung aller in einem bestimmten Kalenderjahr abgeschlossener Handakten vorzunehmen, statt diese tagesgenau sieben Jahre nach Beendigung des Mandats vernichten zu müssen, was außerordentlich aufwändig wäre. Der Gesetzgeber macht also im Zuge der „kleinen BRAO-Reform“ erstmals eine klare zeitliche Vorgabe für die (nach dem bisherigen § 35 Abs. 2 S. 2 Nr. 3 BDSG auch jetzt schon geltende und) ab dem 25.05.2018 aus Art. 17 DS-GVO sowie dem neu gefassten § 35 BDSG resultierende datenschutzrechtliche Löschungsverpflichtung (und das sogenannte „Recht auf Vergessenwerden“).

In der amtlichen Begründung zur „kleinen BRAO-Reform“ heißt es hierzu:[21]

> „Die sich derzeit noch aus § 35 Absatz 2 Satz 2 Nummer 3 BDSG ergebende datenschutzrechtliche Löschungsverpflichtung wird sich zukünftig voraussichtlich unmittelbar aus der kurz vor der Verabschiedung stehenden Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung) ergeben. Gerade im Hinblick auf die dort sehr allgemeinen Regelungen zu Löschungspflichten erscheint es sinnvoll und erforderlich, dass nicht jeder einzelne Rechtsanwalt im Hinblick auf den Gegenstand jeder einzelnen Handakte gegenüber der Datenschutzaufsichtsbehörde begründen muss, warum die Aufbewahrung dieser Handakte zum Zweck der Aufsicht noch erforderlich ist, sondern für einen bestimmten Zeitraum für alle Beteiligten die Erforderlichkeit und Zulässigkeit der Aufbewahrung zu diesem Zweck gesetzlich klargestellt ist. Anschließend sind die Handakten, da sie wohl immer personenbezogene Daten enthalten werden, aufgrund der datenschutzrechtlichen Vorgaben zu vernichten, soweit sich nicht aus anderen Gründen eine Pflicht oder Befugnis zu ihrer weiteren Aufbewahrung ergibt.“

[21] Wie zuvor.

Der Rechtsanwalt, der fürchtet, auch nach Verstreichen eines längeren Zeitraums (die regelmäßige Verjährungsfrist beginnt gem. § 199 Abs. 1 Nr. 2 BGB bekanntlich erst mit dem Schluss des Jahres, in dem der Gläubiger Kenntnis von den anspruchsbegründenden Umständen erlangt) vom Mandanten in Regress genommen zu werden, und diese Befürchtung einigermaßen schlüssig darlegen kann, wird sich hier im Zweifel noch auf „andere Gründe“ berufen können.

Über ein Thema scheint sich der Gesetzgeber aber bislang gar keine Gedanken gemacht zu haben: Wenn Handakten (und überhaupt alle Mandanten-Daten) nur bis zum Ablauf von sechs Jahren aufbewahrt werden dürfen, können sich für den Rechtsanwalt bei der Kollisionskontrolle erhebliche Schwierigkeiten ergeben, ein neues Mandat im alten bzw. ein altes im neuen wiederzuerkennen. Die Kollisionsbefangenheit und damit die Gefahr eines Verstoßes gegen § 356 StGB, § 43a Abs. 4 BRAO und § 3 BORA währt bekanntlich ewig und kann den Anwalt deshalb auch noch nach weit mehr als sieben Jahren erheblich in die Bredouille bringen. Problematisch ist das insbesondere bei größeren Kanzleieinheiten und Kanzleiwechseln. Denn während sich der Sachbearbeiter eines Mandats möglicherweise noch lange an Namen und Fakten erinnert, sind die nach § 3 Abs. 2 u. 3 BORA mit befangenen Kollegen zwingend auf die Durchforstung eines vorhandenen Datenbestands angewiesen.

Hilfreich könnte in diesem Zusammenhang die Entscheidung des LG Karlsruhe vom 06.10.2016[22] sein, in der das Landgericht die Klage auf Rückzahlung von Anwaltshonorar richtigerweise u.a. deshalb ablehnt, weil die beklagte Rechtsanwältin weder die Möglichkeit hatte, von dem an einem entfernten Standort der Großkanzlei, für die sie früher einmal tätig war, geführten Kollisions-Mandant konkrete Kenntnis zu erlangen noch im Nachhinein irgendeine Form der Kollisionskontrolle auszuüben. Denn vom Anwalt darf im Hinblick auf die Vermeidung von Interessenkollisionen natürlich nichts Unmögliches, also auch kein übersteigertes Erinnerungsvermögen und schon gar nicht die Fähigkeit des „Hellsehens“ verlangt werden.

Die Umsetzung des „Rechts auf Vergessenwerden“ erfordert ebenso wie die anwaltliche Schweigepflicht zwingend auch eine absolut sichere Vernichtung der Daten. Papierakten müssen (durch Kanzleipersonal oder eine Fachfirma) im „Reißwolf“ entsorgt und dürfen nicht einfach der Altpapier-Sammlung überantwortet werden und bei PCs, Mobiltelefonen und vergleichbarer Hardware müssen sämtliche Speicher unwiederbringlich gelöscht oder zerstört werden.

[22] Vgl. AnwBl. 2017, 91.

2. Verschwiegenheit und (Legal) Outsourcing

Inwieweit die anwaltliche Schweigepflicht und die Anforderungen der DS-GVO in Einklang stehen, einander ergänzen oder auch in Widerspruch zueinander treten, werden erst die Einzelfälle der Zukunft vollends zeigen.

a) Grundsätze der anwaltlichen Schweigepflicht

Nach § 43a Abs. 2 S. 2 BRAO bezieht sich die Verpflichtung des Rechtsanwalts zur Verschwiegenheit „auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist“. Allerdings besteht nach ganz h.M. die Schweigepflicht nur gegenüber dem eigenen Mandanten.

aa) Informationspflichten gegenüber Drittbetroffenen?

Rechte Dritter (des Gegners, von Zeugen etc.) muss und darf (!) der Anwalt ganz grundsätzlich nicht schützen. Deshalb könnten die Informationspflichten, die gem. Art. 14 DS-GVO für den Fall gelten, dass die Erhebung personenbezogener Daten nicht bei der betroffenen Person selbst erfolgt, aus anwaltlicher Sicht und aus Sicht nahezu aller einer Berufsverschwiegenheit unterliegenden Geheimnisträger bei buchstabengetreuer Anwendung fatal sein.

Der deutsche Gesetzgeber hat hier allerdings von der nach Art. 14 Abs. 5 lit. d DS-GVO geltenden Öffnungsklausel zur Wahrung von Berufsgeheimnissen (vgl. hierzu schon oben Ziff. IV. 8. b bb) Gebrauch gemacht und in § 29 Abs. 1 u. 2 BDSG-2018 (unter der Überschrift „Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten“) festgeschrieben:

> „(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die

> Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.
>
> (2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt."

Die Formulierung „sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt" in § 29 Abs. 2 a.E. ist allerdings auslegungsfähig.

Herb,[23] der Vorsitzende des BRAK-Ausschusses Datenschutzrecht, formuliert hierzu etwas sibyllinisch, durch § 29 Abs. 1 u. 2 BDSG-2018 werde die Pflicht zur Information des Gegners (oder sonstiger Dritter) „eingeschränkt", die Interessen des Mandanten hätten „insoweit grundsätzlich Vorrang" und das gelte „auch im Hinblick auf eventuelle Auskunftsansprüche des Gegners". Als vollständige Entwarnung können diese vorsichtigen Formulierungen eher nicht verstanden werden.

In der amtlichen Begründung zum DSAnpUG-EU[24] heißt es, auf der Grundlage der Öffnungsklausel des Art. 23 Abs. 1 lit. i der DS-GVO beschränke § 29 Abs. 1 wie bisher nach dem BDSG a.F. gegenüber Geheimnisträgern das Recht auf Information und Auskunft. Abs. 1 S. 2 beschränke die Betroffenenrechte auch für die Fälle, in denen Informationen „nach einer Rechtsvorschrift" geheim gehalten werden müssten. S. 1 beziehe sich nicht auf diese nach Rechtsvorschriften bestehenden Geheimhaltungspflichten, da die Informationspflicht hier bereits unmittelbar durch Art. 14 Abs. 5 lit. d DS-GVO beschränkt werde. Die Sätze 3 und 4 bezögen sich auf eine Beschränkung der Benachrichtigungspflicht nach Art. 34 DS-GVO.

---

[23] BRAK-Mitt. 2017, 209, 211.
[24] BT-Drucks. 18/11325, S. 100 f.

§ 29 Abs. 2 BDSG-2018 diene dem Schutz der ungehinderten Kommunikation zwischen Mandant und Berufsgeheimnisträger. Wirtschaftsprüfer und Rechtsanwälte würden oftmals nicht (nur) mit der Verfolgung von Rechtsansprüchen, sondern mit vielfältigen Beratungsdienstleistungen (Steuerberatung, Begleitung von Unternehmenstransaktionen, Gutachter- und Sachverständigentätigkeit etc.) beauftragt. Es widerspräche dem besonderen Schutz des Mandatsverhältnisses, wenn der Mandant in jedem Fall sämtliche durch die Datenübermittlung an den Berufsgeheimnisträger betroffenen Personen über die Zwecke der Datenübermittlung, die Identität der beauftragten Berufsgeheimnisträger etc. informieren müsste. Durch die in Abs. 2 letzter Hs. eingefügte „Abwägungsklausel“ werde den Rechten der Betroffenen angemessen Rechnung getragen.

Auf die Bedeutung der Anwaltsprivilegien (Zeugnisverweigerungsrechte, Beschlagnahmefreiheit u.a.) wurde im Übrigen unter Ziff. IV. 8. b bb bereits hingewiesen.

bb) Informationspflichten gegenüber Aufsichtsbehörden

Nach Art. 33 und 34 DS-GVO müssen über Datenschutzverletzungen grundsätzlich („es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“) sowohl die Aufsichtsbehörde (innerhalb von 72 Stunden) als auch die betroffene Person selbst informiert werden.

Die Zeitvorgabe und die Pflicht, den Betroffenen zu unterrichten, sind neu, die grundsätzliche Informationspflicht galt auch bislang schon.

In einer Anwaltskanzlei sind verschiedene „Datenlecks“ denkbar - vom Hackerangriff, über ein gestohlenes Mobiltelefon oder den verlorenen USB-Stick bis hin zur Indiskretion eines Mitarbeiters. Ob es in all diesen Fällen im Interesse des betroffenen Mandanten liegt, dass über das „Missgeschick“ und also auch über das Mandatsverhältnis als solches (man denke nur an die Beratung in einer Steuerhinterziehungs-Angelegenheit) nun auch noch staatliche Behörden informiert werden, ist - ebenso wie die Frage des Nutzens für den Mandanten - zweifelhaft. Da der Mandant der Betroffene und (möglicherweise) Geschädigte und außerdem der alleinige „Herr des Geheimnisses“ ist, müsste es seiner Entscheidungsgewalt unterliegen, ob der Anwalt die Aufsichtsbehörde informiert oder nicht.

Fraglich ist auch, was in welcher Zeit zu veranlassen ist, wenn gar nicht feststeht, ob tatsächlich eine Datenschutzverletzung eingetreten ist. So können ein

Mobiltelefon oder USB-Stick auch schlicht verlegt oder eine Papierakte falsch einsortiert worden sein und später wieder auftauchen und ein Einhalten der 72-Stunden-Regelung dazu führen, dass völlig unnötiger Weise „die Pferde scheu gemacht“ und wertvolles Vertrauen des Mandanten aufs Spiel gesetzt wurden.

b) Neue Regeln zum (Legal) Outsourcing etc.

Zu langjährigen Diskussionen auf verschiedenen Ebenen (Gesetzgeber, Satzungsversammlung der Anwaltschaft etc.) hat die Frage geführt, ob und unter welchen Voraussetzungen zur Geheimhaltung verpflichtete Berufsträger außer ihren schon lange gesetzlich mit erfassten und mit geschützten „Hilfspersonen“ (z.B. Rechtsanwalts- und Notarfachangestellten) sonstigen „Unterstützern“, etwa den Erbringern von Büroservice- oder IT-Dienstleistungen Zugang zu geschützten Informationen verschaffen dürfen.

Für Rechtsanwälte erfolgten erste Klarstellungen in § 2 BORA. Allerdings fehlte diesen zunächst der legislative Unterbau, weil es einerseits an einer Strafbarkeit der unterstützenden Dienstleister (im Unterschied zu den „berufsmäßig tätigen Gehilfen“) im Rahmen von § 203 StGB und damit korrespondierend am Privileg des Zeugnisverweigerungsrechts mangelte.

Hier ist der deutsche Gesetzgeber inzwischen tätig geworden. Das *„Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“* vom 30.10.2017,[25] das in seinen wesentlichen Teilen am 09.11.2017 in Kraft getreten ist, enthält jetzt u.a. für Rechtsanwälte eine Fülle von - beinahe schon wieder zu stark ausdifferenzierten - Regelungen.

Im Einzelnen sind folgende Vorschriften maßgeblich:

aa) § 203 Abs. 3 bis 5 StGB

> „(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich

[25] BGBl. 2017 I S. 3618.

ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart."

bb) § 43a Abs. 2 BRAO

„Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Rechtsanwalt hat die von ihm beschäftigten Personen in schriftlicher Form zur Verschwiegenheit zu verpflichten und sie dabei über die strafrechtlichen Folgen einer Pflichtverletzung zu belehren. Zudem hat er bei ihnen in geeigneter Weise auf die Einhaltung der Verschwiegenheitspflicht hinzuwirken. Den von dem Rechtsanwalt beschäftigten Personen stehen die Personen gleich, die im Rahmen einer berufsvorbereitenden Tätigkeit oder einer sonstigen Hilfstätigkeit an seiner beruflichen Tätigkeit mitwirken. Satz 4

gilt nicht für Referendare und angestellte Personen, die im Hinblick auf die Verschwiegenheitspflicht den gleichen Anforderungen wie der Rechtsanwalt unterliegen. Hat sich ein Rechtsanwalt mit anderen Personen, die im Hinblick auf die Verschwiegenheitspflicht den gleichen Anforderungen unterliegen wie er, zur gemeinschaftlichen Berufsausübung zusammengeschlossen und besteht zu den Beschäftigten ein einheitliches Beschäftigungsverhältnis, so genügt auch der Nachweis, dass eine andere dieser Personen die Verpflichtung nach Satz 4 vorgenommen hat."

cc) § 43e BRAO („Inanspruchnahme von Dienstleistungen") - neu

„(1) Der Rechtsanwalt darf Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 43a Absatz 2 Satz 1 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Rechtsanwalt im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.

(2) Der Rechtsanwalt ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Er hat die Zusammenarbeit unverzüglich zu beenden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.

(3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist

1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,

2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und

3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.

(4) Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.

(5) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat.

(6) Die Absätze 2 und 3 gelten auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet hat.

(7) Die Absätze 1 bis 6 gelten nicht, soweit Dienstleistungen auf Grund besonderer gesetzlicher Vorschriften in Anspruch genommen werden. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.

(8) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt."

dd) § 2 Abs. 3 bis 8 BORA

„(3) Ein Verstoß ist nicht gegeben, soweit das Verhalten des Rechtsanwalts

a) mit Einwilligung erfolgt oder

b) zur Wahrnehmung berechtigter Interessen erforderlich ist, z.B. zur Durchsetzung oder Abwehr von Ansprüchen aus dem Mandatsverhältnis oder zur Verteidigung in eigener Sache, oder

c) im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz).

(4) Der Rechtsanwalt hat seine Mitarbeiter zur Verschwiegenheit schriftlich zu verpflichten und anzuhalten, auch soweit sie nicht im Mandat, sondern in sonstiger Weise für ihn tätig sind.

(5) Abs. 4 gilt auch hinsichtlich sonstiger Personen, deren Dienste der Rechtsanwalt in Anspruch nimmt und

a) denen er verschwiegenheitsgeschützte Tatsachen zur Kenntnis gibt oder

b) die sich gelegentlich ihrer Leistungserbringung Kenntnis von verschwiegenheitsgeschützten Tatsachen verschaffen können. Nimmt der

Rechtsanwalt die Dienste von Unternehmen in Anspruch, hat er diesen Unternehmen aufzuerlegen, ihre Mitarbeiter zur Verschwiegenheit über die Tatsachen gemäß Satz 1 zu verpflichten. Die Pflichten nach Satz 1 und 2 gelten nicht, soweit die dienstleistenden Personen oder Unternehmen kraft Gesetzes zur Geheimhaltung verpflichtet sind oder sich aus dem Inhalt der Dienstleistung eine solche Pflicht offenkundig ergibt.

(6) Der Rechtsanwalt darf Personen und Unternehmen zur Mitarbeit im Mandat oder zu sonstigen Dienstleistungen nicht hinzuziehen, wenn ihm Umstände bekannt sind, aus denen sich konkrete Zweifel an der mit Blick auf die Verschwiegenheitspflicht erforderlichen Zuverlässigkeit ergeben und nach Überprüfung verbleiben.

- neu

(7) Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit des Datenschutzrechts dessen Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen. Abs. 3 lit. c) bleibt hiervon unberührt.[26]

(8) Die Bestimmungen des Datenschutzrechts zum Schutz personenbezogener Daten bleiben unberührt."

Der neu eingefügte Abs. 7 wurde - nach kontroverser Diskussion - in der 4. Sitzung der Sechsten Satzungsversammlung am 19.05.2017 beschlossen und ist Anfang 2018 in Kraft getreten.

Welche „organisatorischen und technischen Maßnahmen" vom Rechtsanwalt zu ergreifen sind und welche Standards hierbei beachtet werden müssen, liegt noch weitgehend im Dunkeln.

Der Ausschuss 6 („Verschwiegenheitspflicht und Datenschutz") der Sechsten Satzungsversammlung ist seit längerem mit dieser Problematik befasst. In der 5. Sitzung der Sechsten Satzungsversammlung am 01.12.2017 trug der Ausschuss-Vorsitzende *Gasteyer* zu dem Thema vor, der Ausschuss habe es sich zur Aufgabe gemacht, den Rechtsanwälten im Hinblick auf den neuen § 2 Abs. 7 BORA Hilfestellungen zu der Frage zu geben, welche Maßnahmen in den Kanzleien ergriffen werden müssten. Dieses Unterfangen habe sich allerdings als schwieriger herausgestellt als zunächst angenommen. Man stehe hierüber

[26] Abs. 7 ist am 01.01.2018 in Kraft getreten.

auch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in regem Austausch.

Der Ausschuss habe u.a. mit der Diskussion über die Fragen begonnen,

- welche Formulierungen in § 2 BORA durch das Geheimnisschutzgesetz obsolet geworden seien, weil sie hinter ihm zurückblieben,
- oder weil sie zu ihm im Gegensatz stünden,
- welche Formulierungen ggf. eine eigene Daseinsberechtigung hätten und ggf. angepasst werden sollten und
- welche Formulierungen unverändert bestehen bleiben könnten und müssten.

Im Ausschuss seien die Auffassungen hierzu kontrovers gewesen.[27]

Alleine diese Diskussion zeigt, wie schwierig es ist, die Themen Verschwiegenheit und Datenschutz und damit auch die neue DS-GVO aufzubereiten und in gleichermaßen verlässliche wie praxistaugliche „Nutzer-Hinweise“ zu gießen.

VII. Vorläufige Schlussfolgerungen und Handlungsempfehlungen

Was folgt aus alledem für die Tätigkeit des Rechtsanwalts ab dem Mai 2018?

Für verbindliche Leitlinien ist es - das zeigt nicht zuletzt die soeben dargestellte Diskussion in der Satzungsversammlung - noch zu früh, wenn es sie denn überhaupt jemals geben kann.

Folgende Eckpunkte sollten beherzigt werden:

1. Auch wenn die Erhebung bestimmter Daten und Fakten beim Auftraggeber zu Beginn des Mandats zwangsläufig ist und sich (auch dem Mandanten) ihre Notwendigkeit geradezu aufdrängt, verlangt Art. 13 DS-GVO, den Mandanten als „betroffene Person“ mit einer Reihe von Informationen (siehe hierzu oben Ziff. IV. 8 b aa) zu versehen. Der Vorsitzende des BRAK-Ausschusses Datenschutz *Herb*[28] rät, dem Mandanten im

[27] Protokoll der 6. Sitzung der Sechsten Satzungsversammlung am 01.12.2017, S. 4 ff.
[28] BRAK-Mitt. 2017, 209, 211.

Zusammenhang mit der Vollmachtserteilung die entsprechenden Informationen auf einem „Merkblatt“ zu geben.

Nur die Erfüllung der Informationspflichten führt zu einer ordnungsgemäßen Datenerhebung und bewahrt vor Geldbußen und sonstigen Weiterungen.

2. Gegner und andere Drittbetroffene müssen grundsätzlich nicht informiert werden. Fallbeispiele für Ausnahmesituationen (vgl. § 29 Abs. 2 BDSG-2018 a.E.) müssen sich erst herausbilden.

3. Das Recht auf „Vergessenwerden“, welches auch im neuen § 50 Abs. 1 S. 2 BRAO seinen Niederschlag findet, zwingt künftig zu konsequenter (natürlich sicherer) Akten- und Datenvernichtung nach dem Ablauf von sechs Jahren (vorbehaltlich längerer, in Spezialnormen geregelter Aufbewahrungspflichten für bestimmte Arten von Daten).

4. Auch Anwaltskanzleien von durchschnittlicher Größe (mindestens zehn Mitarbeiter „am PC“) benötigen einen betrieblichen Datenschutzbeauftragten. Sein Name und seine Kontaktdaten gehören zu den „mitteilungspflichtigen“ Informationen.

5. Für die Auswahl und den Umgang mit Mitarbeitern und Dienstleistern gelten schon aufgrund des *„Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“* strenge Anforderungen, deren Einhaltung den Rechtsanwalt auch im Hinblick auf die DS-GVO „auf die sichere Seite bringt“.

6. Datenschutzverletzungen müssen der Aufsichtsbehörde (innerhalb kurzer Frist von nur 72 Stunden) und der betroffenen Person angezeigt werden. Aus Gründen äußerster Vorsicht sollte der Rechtsanwalt den Mandanten auch über seine Informationspflicht gegenüber der Aufsichtsbehörde informieren.

   Inwieweit es hier einen Dispens geben kann, sofern schützenswerte Interessen des Mandanten einer offiziellen Anzeige entgegenstehen, wurde noch nicht erörtert.

7. Ein Rechtsanwalt, der gegen Bestimmungen der DS-GVO verstößt, setzt sich erheblichen Bußgeldforderungen und möglicherweise zusätzlich aufsichtsrechtlichen Maßnahmen aus.

Und zu guter Letzt:

> „Die bisherige deutsche Datenschutzgesetzgebung wird (durch die DS-GVO) 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.“

Dieser - nicht wirklich ermutigenden - Feststellung des Vorsitzenden des BRAK-Ausschusses Datenschutzrecht *Herb*[29] ist nichts hinzuzufügen.

gez. Dr. Offermann-Burckart
Düsseldorf, den 09.02.2018/Off-B

[29] BRAK-Mitt. 2017, 209, 214.