RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU) • Salzburg

Datenschutz für Anwaltskanzleien*

» jusIT 2018/42

Datenschutzrecht; Berufsausübung, anwaltliche; Rechtsanwaltskanzlei als Auftraggeber; Datenschutzbeauftragter; Bestellungspflicht; Datensicherheit; Meldepflicht, Wegfall der; Verarbeitungsverzeichnis; Datenschutz-Folgenabschätzung; Data Breach Notification; Daten, personenbezogene; Daten, strafrechtsbezogene; Daten, sensible; Strafverteidiger; Kerngeschäft, anwaltliches; Datenmanagementsystem

§ DSG 2000: §§ 4, 7, 8, 10, 11, 17, 18, 19; VO (EU) 2016/679: Art 4, Art 13 ff, Art 28, Art 30, Art 37, Art 38, Art 39, Art 83

Spätestens mit Wirksamwerden der Datenschutz-Grundverordnung[1] (DS-GVO) am 25. 5. 2018 ist auch für die anwaltliche Berufsausübung eine „GDPR Compliance" zu erzielen. Der vorliegende Beitrag gibt – ohne Anspruch auf Vollständigkeit – ausgehend vom derzeitigen Stand des Datenschutzrechts für österreichische Rechtsanwaltskanzleien einen Überblick über die voraussichtlichen Neuerungen durch die DS-GVO. Änderungen der Gesetzeslage, Spruchpraxis der Behörden oder Gerichte bleiben selbstverständlich vorbehalten.

1. Einleitung

Bereits einmal stand die österreichische Rechtsanwaltschaft vor einer Zeitenwende im Datenschutzrecht. Zum Inkrafttreten des DSG 1978[2] mit 1. 1. 1980 bemerkte bereits RA *Bednar* treffend: *„Dass auch Freiberufler bisher so achtlos am Datenschutz vorübergegangen sind, hat mehrere Ursachen. Sicher ist die völlig fehlende Aufklärung durch Gesetzgeber und Administration eine Hauptursache. Der Gesetzestext ist auch keine Hirnweide, obwohl fast ein Jahrzehnt herumgedoktert wurde. Die äußerst unglückliche Vollziehung tut ein Übriges."*[3] Im Jahr 2018 ist es wieder soweit, dass ein mittlerweile sehr gut entwickeltes, aber gerade von den RechtsanwältInnen in ihren eigenen Unternehmen, eben den Kanzleibetrieben, bislang wenig beachtetes Rechtsgebiet grundlegend reformiert wird. Lediglich die genaue Kenntnis der DS-GVO und des DSG (2018)[4] kann zu einer nutzbringenden Umsetzung führen. Was (auch) heute noch zu tun ist, war schon bei Einführung des DSG 1978 bekannt: *„Es liegt wiederum an den Meinungsbildnern, sich auch über Datenschutz zu informieren, sich darüber eine Meinung zu bilden und diese in ihrem täglichen Handeln spürbar zu machen. Um unsere Zukunft zu bewältigen, brauchen wir den Schutz unserer Daten."*[5] Der vorliegende Artikel möge dazu einen Beitrag leisten.

2. Grundlagen und Grundbegriffe

2.1. Schutz der Privatsphäre

Zum Schutz der Privatsphäre einer natürlichen oder juristischen Person gewährt das Datenschutzrecht vor allem ein Recht auf Geheimhaltung personenbezogener Daten, soweit ein schutzwürdiges Interesse daran besteht.[6] Dieses Recht kann insb mit Zustimmung des Betroffenen oder zur Wahrung berechtigter Interessen eines anderen eingeschränkt werden. Daneben treten die weiteren Rechte auf Auskunft, Richtigstellung und Löschung. Das Grundrecht auf Datenschutz gem § 1 DSG 2000 (§ 1 DSG [2018]) bedeutet demzufolge:

- umfassender Geheimhaltungsanspruch,
- Verbotsprinzip (mit Ausnahmen),
- unmittelbare Wirkung auch gegenüber Privaten.

Sowohl die Datenschutz-RL[7] als auch § 7 DSG 2000 und die DS-GVO gehen vom Verbotsprinzip als tragendem Grundsatz des Datenschutzrechts aus. Dazu kommt ein erhöhtes Maß an unternehmerischer Eigenverantwortung im Umgang mit personenbezogenen Daten in Form einer umfassenden Rechenschaftspflicht („privacy accountability") nach Art 5 Abs 2 iVm Art 24 DS-GVO.

Gleiches gilt für den Vorschlag einer E-Datenschutz-Verordnung[8] (ePrivacy-VO; EDS-VO), welche die derzeit gültige Elek-

* Dieser Beitrag wurde bereits auch veröffentlicht in Bergauer/Jahnel/Mader/Staudegger (Hrsg), jusIT Spezial: DS-GVO (2018) 203 und erscheint hier in aktualisierter Form.

1 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 (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF L 2016/314, 72.

2 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG 1978), BGBl 565/1978, mehrfach novelliert, zuletzt idF BGBl 632/1994.

3 *Bednar*, Datenschutz für Rechtsanwälte, AnwBl 1981, 55 (56).

4 Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), BGBl I 120/2017 idF 23/2018 und 24/2018, in Kraft mit 25. 5. 2018.

5 *Bednar*, Datenschutz für Rechtsanwälte, AnwBl 1981, 55 (56).

6 Vgl § 1 Abs 1 DSG 2000; sinngemäß auch Art 16 Abs 1 AEUV; Art 8 EMRK; Art 8 GRC.

7 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

8 Derzeit als Entwurf der EU-Kommission KOM (2017) 10 final, 2017/0003 (COD) vom 10. 1. 2017 idF 27. 10. 2017 (über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG [Verordnung über Privatsphäre und elektronische Kommunikation]).

tronische Datenschutz-RL[9] ablösen soll. Sie sollte ebenfalls mit 25. 5. 2018 wirksam werden und unmittelbar anwendbar sein. Sie verweist auf zahlreiche Definitionen in anderen Rechtsakten, insb in der DS-GVO und in dem Vorschlag für einen neuen EU-Kodex für die elektronische Kommunikation. Dadurch sollen künftig alle Definitionen der DS-GVO auch im Rahmen der EDS-VO gelten. Eine endgültige Fassung fehlt bislang.

2.2. Personenbezogene Daten

Das Datenschutzrecht bezieht sich ausschließlich auf die Verarbeitung personenbezogener Daten. Es regelt den Umgang mit Daten von Menschen. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Es handelt sich also um Informationen, die eine Person identifizieren können. Für die Einstufung einer Information als „personenbezogenes Datum" iSv Art 4 Z 1 DS-GVO ist nicht erforderlich, dass die Information für sich genommen die Identifizierung der betreffenden Person ermöglicht und dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden.

Die DS-GVO erfasst als *„personenbezogene Daten"* nach Art 4 Z 1 *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [sog ‚betroffene Person'] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu*

- *einer Kennung wie einem Namen,*
- *einer Kennnummer,*
- *Standortdaten,*
- *einer Online-Kennung oder*
- *einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,*

identifiziert werden kann".

Keine dem DSG (2018) bzw der DS-GVO unterliegenden „Daten" sind anonyme Daten, also solche, die niemand auf eine Person zurückführen kann, oder ganz generell Daten ohne Personenbezug.

Die in einer Anwaltskanzlei verarbeiteten Daten sind vielfältig. Sie fallen in Form von Klienten-, Mitarbeiter- oder sonstigen Daten der Beteiligten in den Zivil-, Verwaltungs- oder Strafcausen einer berufsmäßigen Parteienvertretung sehr zahlreich an.

Bei den Daten über einen Asylwerbenden, die in einer verwaltungsbehördlichen „Entwurfsschrift" wiedergegeben sind, handelt es sich um „personenbezogene Daten". Dazu zählen auch die dargelegten Gründe des Sachbearbeiters, auf denen der Entscheidungsentwurf beruht, und jene Daten, die Teil der in der Entwurfsschrift enthaltenen rechtlichen Analyse sind. Diese Einstufung gilt allerdings nicht für die Analyse als solche.[10]

Die von § 4 Z 2 DSG 2000 bisher als besonders schutzwürdig angesehenen Daten erfasst nunmehr Art 9 DS-GVO als besondere Kategorien von Daten und erweitert diese um die biometrischen und genetischen Daten. Nach Art 9 Abs 1 DS-GVO ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person untersagt.

Art 9 Abs 2 DS-GVO hält (taxativ) bestimmte Ausnahmen vom Verarbeitungsverbot für „kategorisierte Daten" bereit, zB für den Fall der (ausdrücklichen) Einwilligung des Betroffenen oder zum Schutz lebenswichtiger Interessen Dritter oder des Betroffenen.[11]

So gehört zB die Angabe, dass sich eine Person den Fuß verletzt hat und partiell krankgeschrieben ist, zu den personenbezogenen Daten über die Gesundheit iSv § 4 Z 2 DSG 2000 (Art 4 Z 15 DS-GVO); also zu den besonders geschützten oder „kategorisierten" Daten.[12] Diese Informationen sind in jedem Haftpflichtprozess wegen zB Schmerzengeld nach einem Verkehrsunfall durch den Kanzleibetrieb zu ermitteln, zu speichern oder zu übermitteln. MaW, es liegt ein verantwortliches Verarbeiten personenbezogener Daten iSv Art 4 Z 2 DS-GVO vor.

Schließlich sind strafrechtliche Vorwürfe zwar keine sensiblen Daten; durch ihre Einordnung als Strafdaten unter die Sonderregel des § 8 Abs 4 DSG 2000 (nunmehr: § 4 Abs 3 DSG [2018]) sind sie im Hinblick auf das Geheimhaltungsinteresse jedoch klar „sensibler" als das bloße Geburtsdatum und daher ebenfalls besonders zu behandeln.[13] Für die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sieht Art 10 DS-GVO eigene (strenge) Verarbeitungsvoraussetzungen vor. Nach hM[14] ist davon auszugehen, dass bei Verarbeitung sensibler (besonders kategorisierter) und gleichzeitig strafrechtlich relevanter Daten die Verarbeitungsvoraussetzungen nach Art 10 DS-GVO vorgehen, dh, dass die zulässige Verarbeitung strafrechtsbezogener Daten insgesamt für deren Verwendung ausreicht. § 4 Abs 3 DSG (2018) gestattet ebenso wie vormals § 8 Abs 4 DSG 2000 nicht-staatlichen Einrichtungen, also primär Unternehmen, aber auch Privatpersonen, die Verarbeitung von

9 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37.

10 EuGH 17. 7. 2014, C-141/12 (YS ua) = jusIT 2014/107, 227 (*Thiele*) = Dako 2015/53, 97 (*Haidinger*).

11 Näher *Schiff* in Ehmann/Selmayr, DSGVO (2017) Art 9 Rz 27 ff.

12 EuGH 6. 11. 2003, C-101/01 (Lindqvist) = MR 2004, 83 (*Kronegger*) = ÖJZ 2004/45, 741 (*Hörlsberger)*.

13 DSK 14. 12. 2012, K121.872/0010-DSK/2012 (RSa-Zustellung von Strafverfügungen) = Dako 2014/22, 44 (*Haidinger*); 17. 12. 2010, K121.636/0010-DSK/2010 (Straferkenntnis mit Geburtsdatum) = jusIT 2011/11, 23 (*König*).

14 *Schiff* in Ehmann/Selmayr, Art 10 Rz 2; *Kampert* in Sydow (Hrsg), Europäische Datenschutzgrundverordnung Handkommentar (2017) Art 10 Rz 9 f; *Gola* in Gola (Hrsg), DS-GVO (2017) Art 10 Rz 7; unklar *Paal/Pauly*, Datenschutz-Grundverordnung[2] (2018) Art 9 Rz 49 f.

strafrechtsbezogenen Daten unter Einhaltung der Vorgaben der DS-GVO, wenn

- eine ausdrückliche gesetzliche Ermächtigung/Verpflichtung dazu besteht oder
- sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist

und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DS-GVO und dem DSG (2018) gewährleistet.

Gewissermaßen umgekehrt kann auch der/die Rechtsanwalt/Rechtsanwältin von einer Datenverarbeitung Dritter betroffen sein. *„Betroffener"* iSd Datenschutzrechts war gem § 4 Z 3 DSG 2000 jede natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet wurden und die vom Auftraggeber verschieden war. Art 4 Z 1 DS-GVO definiert demgegenüber als „betroffene Person" lediglich eine identifizierte oder identifizierbare *natürliche* Person. Ein/e Anwalt/Anwältin kann daher durchaus – auch und gerade wegen seiner/ihrer Berufsausübung – Betroffene/r einer Datenverarbeitung sein. Dies gilt insb im Umgang mit der Standesvertretung.

So hat die Datenschutzpraxis[15] schon früh festgehalten, dass keine Verletzung im Grundrecht auf Geheimhaltung nach § 1 Abs 1 DSG 2000 (unverändert § 1 Abs 1 DSG [2018]) durch den Auftrag der zuständigen Rechtsanwaltskammer bewirkt wird, einen Lebenslauf und Tätigkeitsbericht anlässlich des Verfahrens zur Wiedereintragung in die Liste der Rechtsanwaltsanwärter vorzulegen (nunmehr ausdrücklich § 20 DSt idF Art 102 des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl I 32/2018).

Gleichermaßen hat die Rsp[16] in der Datenübermittlung an die anwaltliche Disziplinarbehörde keinen Verstoß gegen das Grundrecht auf Datenschutz des betroffenen Rechtsanwaltskollegen erkannt. Wenn bei einer Disziplinaranzeige an eine Standesbehörde Daten des Angezeigten weitergegeben werden, kann dies wegen überwiegender öffentlicher Interessen an der Verfolgung nicht verjährter Disziplinarvergehen gerechtfertigt sein. Dabei kommt es – wie nahezu immer im Datenschutzrecht – auf eine umfassende Interessenabwägung an.

2.3. Datenschutzrechtliches Verbotsprinzip

Das Datenschutzrecht ist von einem Regel-Ausnahme-Prinzip geprägt. Um keine Datenschutzverletzung zu begehen, muss sich der Verantwortliche vergewissern, eine der genannten Rechtfertigungen zu erfüllen.

Ausnahmen vom Verbot der personenbezogenen Datenverarbeitung, also Rechtfertigungsgründe einer Datenverwendung, bestehen für unkategorisierte und nicht strafrechtsbezogene Daten nach Art 6 Abs 1 DS-GVO, bei:

- Einwilligung des Betroffenen,
- Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene ist,
- Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt,
- Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe, zB Behördenhandeln,
- Wahrung überwiegender bzw zumindest gleichwertiger Interessen des Verantwortlichen bzw Dritter,
- lebenswichtigen Interessen des Betroffenen oder eines Dritten.

Die nach österr Recht bisher normierte Rechtfertigung der Datenverarbeitung wegen „allgemeiner" Verfügbarkeit der Daten[17] besteht in dieser Form nicht mehr.

Im Unterschied dazu ist die Verarbeitung sensibler Daten künftig unter strengere Voraussetzungen gestellt als derzeit. Art 9 DS-GVO geht von einem grundsätzlich weiter reichenden Verbot aus:

- *keine* Interessenabwägung
- *keine* Vertragserfüllung
- Ausnahmen:
  - *ausdrückliche* Einwilligung des Betroffenen,
  - exakte Rechtsgrundlage (Art 9 Abs 2 lit g DS-GVO),
  - lebenswichtige Interessen des Betroffenen *oder eines anderen Menschen,*
  - offensichtlich durch Betroffenen selbst veröffentlicht.

Darüber hinaus ist im Rahmen sog „besonderer Verarbeitungssituationen" bei Einhaltung der sonstigen Zulässigkeitskriterien auch die Verarbeitung sensibler Daten gestattet, nämlich (vgl Art 9 Abs 2 DS-GVO):

- im Arbeitsrechtskontext (Art 88 DS-GVO: Beschäftigtendatenschutz),
- für Kirchen, religiöse Vereinigungen oder bestimmte Vereine (Art 91 DS-GVO),
- bei Geltendmachung von Rechtsansprüchen (Art 9 Abs 2 lit f DS-GVO),
- in der Gesundheitsvorsorge (Art 9 Abs 2 lit h und Abs 4 DS-GVO),
- für Forschung, Statistik oder Archive (Art 89 DS-GVO).

Generell ist also die Verarbeitung einfach personenbezogener Daten unter leichteren Voraussetzungen möglich als die Verarbeitung sensibler Daten.

2.4. Anwendbares Datenschutzrecht

Art 3 DS-GVO hält eine autonome Anknüpfungsgrundlage für internationale Sachverhalte bereit: Für Datenverarbeitungen innerhalb der EU gilt das Niederlassungsprinzip; entscheidend ist der Sitz der verantwortlichen Stelle, dh des Verantwortlichen, uU innerhalb dieser Verarbeitung die Sachnähe.

Die (rechtlichen) Möglichkeiten der Umgehung des Datenschutzrechts durch Auslagerung einer Datenverarbeitung außerhalb der

15 DSK 28. 2. 2003, K120.806/002-DSK/2003 (ARAK) = RIDA-Nr 0154094.
16 OGH 12. 3. 1997, 6 Ob 2228/96g (Disziplinaranzeige) = SZ 70/42.

17 Diese generelle Privilegierung für veröffentlichte Daten ist nach dem Urteil des EuGH 16. 12. 2008, C-73/07 (Satakunnan/Satamedia) = jusIT 2009/13, 28 (*Jahnel*) = MR-Int 2009, 14 (*Wittmann*) für das österreichische Datenschutzrecht nicht mehr aufrechtzuerhalten.

EU sind geringer, als es auf den ersten Blick scheint. Der Begriff der Verarbeitung von Daten iSv Art 4 Z 2 DS-GVO ist nämlich sehr weit und umfasst das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Übermitteln, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten.

Die Verarbeitung personenbezogener Daten durch ein im elektronischen Geschäftsverkehr tätiges Unternehmen unterliegt dem Recht jenes Mitgliedstaats, auf den das Unternehmen seine Geschäftstätigkeit ausrichtet, wenn sich zeigt, dass das Unternehmen die fragliche Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung iSv Art 3 Abs 1 DS-GVO vornimmt, die sich in diesem Mitgliedstaat befindet. Es ist Sache des nationalen Gerichts, zu beurteilen, ob dies konkret der Fall ist.[18]

Gegenüber Verbrauchern – und damit haben es RechtsanwältInnen oftmals zu tun – muss eine datenschutzrechtliche Rechtswahlklausel sowie eine Einwilligungserklärung des Klienten zusätzlich noch den Anforderungen des § 6 Abs 3 KSchG genügen.[19]

2.5. RechtsanwältInnen als datenschutzrechtlich Verantwortliche

Die DS-GVO hält an der bisherigen Rollenverteilung fest. Demnach sind der datenschutzrechtliche Auftraggeber („Verantwortlicher"), der Betroffene und der datenschutzrechtliche Dienstleister („Auftragsverarbeiter") voneinander abzugrenzen.

Derjenige, der für die Datenverarbeitung verantwortlich ist, wird im Datenschutzrecht als Auftraggeber bzw Verantwortlicher bezeichnet (§ 4 Z 4 DSG 2000 bzw Art 4 Z 7 DS-GVO). Dies ist jede natürliche oder juristische Person oder Personengemeinschaft, die die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten.

Als Faustregel gilt: Verantwortlicher ist derjenige, der die tatsächliche Verfügungsgewalt über die Daten hat („Herr der Datenverarbeitung"). Er bleibt selbst dann Verantwortlicher, wenn er einem anderen Daten zur Herstellung eines von ihm aufgetragenen Werkes überlässt. Maßgeblich ist, wer die rechtliche Entscheidungsbefugnis hat, die konkrete Datenverarbeitung zu beenden.

Nur derjenige, der mit seinem rechtlichen oder tatsächlichen Einfluss die Datenverarbeitung auch jederzeit stoppen kann, kann Verantwortlicher sein.[20] Nach bisheriger Spruchpraxis in Österreich[21] bewirkt die berufliche Selbstständigkeit eines berufsmäßigen Parteienvertreters idR bereits, dass dieser bei der Besorgung von Geschäften für einen Mandanten gem Art 4 Z 7 letzter Halbsatz DS-GVO „eigenverantwortlich" vorgeht und damit datenschutzrechtlich gesehen Verantwortlicher ist. Insoweit garantiert die (bloß) gesetzesgebundene Ausübung des dem Rechtsanwalt übertragenen Mandats nach § 9 RAO, kein bloßer Auftragsverarbeiter iSv Art 28 DS-GVO zu sein.

Vorstellbar sind Konstellationen und Situationen, in denen die Anwaltskanzlei als reiner Auftragsverarbeiter eingesetzt wird. Zu denken ist zB an die Tätigkeit eines Rechtsanwalts als reiner Rechtsberater für ein Unternehmen. In diesem Fall, aber auch im Fall eines anderen Verantwortlichen nimmt der Rechtsanwalt (auch) die Rolle eines Empfängers iSv Art 4 Z 9 DS-GVO ein. In diesen Fällen muss auf eine klare, mit den Erfordernissen nach Art 28 DS-GVO abgestimmte, vertragliche Regelung geachtet werden, einschließlich einer entsprechenden Dokumentation im (separaten) Verarbeitungsverzeichnis.

3. Kurzer Aufriss der Datenschutzgrundsätze nach der DS-GVO

3.1. Rechenschaftspflicht ersetzt Meldepflicht

Die Grundsätze der Datenverarbeitung sind nunmehr in Art 5 DS-GVO festgelegt. Im Wesentlichen bestehen kaum Änderungen zur Rechtslage nach dem DSG 2000. Es sind daher auch künftig folgende Grundsätze zu beachten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit,
- Rechenschaftspflicht.

Der zuletzt aufgezählte Grundsatz der *Accountability* prägt die Verantwortlichkeit des datenverarbeitenden Unternehmens. Der Zweckbindungsgrundsatz ist im Vergleich zur Strenge des DSG 2000 etwas gelockert worden, da eine Datenverarbeitung zu einem anderen Zweck (alternativ) nicht nur bei Einwilligung der Betroffenen iSv Art 7 DS-GVO oder bestehender Rechtsgrundlage zulässig ist, sondern auch bei Bestehen des sog „Kompatibilitätstests" nach Art 6 Abs 4 DS-GVO, dh in demonstrativer Aufzählung bei:

- Verbindung zwischen den Zwecken,
- Zusammenhang der Datenerhebung,
- Folgen der Weiterverwendung,
- Verschlüsselung oder Pseudonymisierung.

Die datenschutzrechtlichen Verpflichtungen des Rechtsanwalts bei seiner Berufsausübung ergeben sich primär aus seiner Funktion als Verantwortlicher für die in seinem Kanzleibetrieb anfallenden Datenverarbeitungen. Darunter versteht man – vereinfacht – alles, was man mit Daten elektronisch oder manuell machen kann, also insb ein bloßes Speichern, Vervielfältigen, Über-

18 EuGH 28. 7. 2016, C-191/15 (VKI/Amazon EU) = ZIIR 2016, 458 (*Thiele*) = ÖJZ 2016/121, 894 (*Brenn*) = ecolex 2016, 939 (*Vidmar*) = ZfRV 2016/34, 268 (*Dorfmayr/Komuczky*) = jusIT 2016/96, 217 (*Thiele*) = VbR 2016/115, 168 (*Stadler*) = MR 2016, 343 (*Riede/Pöchhacker*) = VbR 2017/6, 17 (*Reichholf*).

19 Vgl OGH 14. 12. 2017, 2 Ob 155/16g (Amazon-AGB) = jusIT 2018/21, 54 (*Mader/Thiele*); 21. 12. 2017, 4 Ob 228/17h (Zalando-AGB).

20 Zutreffend *Fritz*, Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, in Schweighofer/Kummer/Saarenpää/Schafer (Hrsg), Datenschutz & Legal Tech, IRIS Tagungsband 2018 (2018) 19 (21 f).

21 DSB 27. 10. 2014, DSB-D122.215/0004-DSB/2014 (F-Rechtsanwalts KG) = ZIR 2015, 47 = jusIT 2015/11, 32 (*König*); DSK 13. 7. 2012, K121.810/0013-DSK/2012 (Netventure Plattform) = RIDA-Nr 0284179.

spielen oder sonstiges Verwenden. Eine Datenverarbeitung stellt dabei nach Art 4 Z 2 DS-GVO jeder Vorgang dar, der personenbezogene Daten verwendet, gleich ob in automatisierten oder nicht-automatisierten Verfahren.[22]

Jeder Kanzleibetrieb, dh bei Einzelanwälten der betreffende Rechtsanwalt, bei Sozietäten – gleich welcher Rechtsform – die Personenmehrheit, musste bis zum 25. 5. 2018 beim Datenverarbeitungsregister eingetragen sein, da keine generelle Ausnahme von der Meldepflicht für berufsmäßige Parteienvertreter bestand.

Achtung: Die Registrierung (DVR-Nummer) an sich sanierte bereits nach bisheriger Rechtslage nicht die Rechtmäßigkeit der Datenanwendung, die im Einzelfall nach dem in § 7 DSG 2000 enthaltenen Stufenkonzept zu prüfen war. Die Registrierungsmöglichkeit ist weggefallen.

Nach dem Konzept der DS-GVO ist eine Datenverarbeitung erst dann rechtskonform, wenn sowohl die Verarbeitungsgrundsätze des Art 5 DS-GVO als auch die Rechenschaftspflicht iSv Art 24 DS-GVO (einschließlich der Datensicherheit) erfüllt und die Betroffenenrechte nach den Art 12 ff DS-GVO beachtet werden.

Im Zuge der Meldung der Datenanwendungen einer Anwaltskanzlei waren auch entsprechende Datensicherheitsmaßnahmen nach § 14 DSG 2000 offenzulegen und tatsächlich in die IT-Systeme zu integrieren.[23] Die Anmeldung selbst war seit September 2012 zwingend auf elektronischem Weg durchzuführen.[24]

Mit Wirksamwerden der DS-GVO entfällt allerdings die Meldepflicht. Ab diesem Zeitpunkt trifft den für die Führung des Kanzleibetriebs Verantwortlichen die volle Rechenschaftspflicht. Bis Ende des Jahres 2019 bleibt aber das DVR einerseits als Meldearchiv abrufbar, andererseits besteht für bereits gemeldete RechtsanwältInnen weiterhin die Möglichkeit, die eigenen Datenanwendungen über eine technische Schnittstelle in ihr aktuelles Verarbeitungsverzeichnis zu übernehmen.[25]

Im Wesentlichen weiter bestehen bleibt das Datengeheimnis nach § 6 DSG (2018) (ex § 15 DSG 2000). Dieses ist daher ebenso wie die Verschwiegenheitsverpflichtung qua Anwaltsgeheimnis auch von bloß im Betrieb tätigen Nicht-AnwältInnen zu wahren, also insb von SekretärInnen, PraktikantInnen, VolontärInnen oder EDV-BetreuerInnen. Eine entsprechend angepasste schriftliche Festlegung im Dienst- oder Werkvertrag ist unerlässlich.

3.2. Auskunftspflicht der RechtsanwältInnen über betrieblich verarbeitete Daten

Die Auskunftspflicht der RechtsanwältInnen als Verantwortliche ihrer Datenanwendungen im Kanzleibetrieb gilt zugunsten von betroffenen Klienten, Gegnern oder sonst Beteiligten gleichermaßen. Das Auskunftsrecht selbst ist verfassungsrechtlich in § 1 Abs 3 DSG 2000 verankert[26] und sowohl unionsrechtlich durch Art 16 Abs 1 AEUV, Art 8 GRC als auch konventionsrechtlich durch Art 8 EMRK abgesichert.[27] Bereits im Anwendungsbereich des DSG 2000 zeigten sich dabei ungerechtfertigte Auskunftsverweigerungen. Ein pauschaler Verweis auf die anwaltliche Verschwiegenheitspflicht nach § 9 Abs 2 RAO kann jedenfalls ein Absehen von der Auskunftserteilung nicht rechtfertigen, zumal es sich bei dieser Verschwiegenheitspflicht um keine absolute handelt.

Im Anlassfall[28] begehrte die spätere Beschwerdeführerin vom belangten Rechtsanwalt X und der Y-Rechtsanwalts-KG Auskunft darüber, welche personenbezogenen Daten im Zuge einer Mietrechtsklage der Z-Bauen und Wohnen GesmbH gegen die Beschwerdeführerin verarbeitet würden. Die Z-GmbH wurde nämlich durch Rechtsanwalt X und seine Y-KG vertreten. Der – aus Sicht der Rechtsanwälte – Prozessgegnerin im Mietverfahren wurde die Auskunft unter „pauschalem Verweis auf die anwaltliche Verschwiegenheitspflicht nach § 9 Abs 2 RAO“ schlichtweg verweigert. Die DSB stellte zunächst fest, dass die belangte Rechtsanwaltskanzlei und Rechtsanwalt X für die Verarbeitung der personenbezogenen Daten der Gegnerin im Mietprozess ebenfalls datenschutzrechtliche Auftraggeber sind, dh eigenverantwortlich agiert haben. Die Auskunftsverweigerung ist durch die bloße anwaltliche Verschwiegenheitspflicht nach § 9 Abs 2 RAO nicht zu rechtfertigen.

Ebenfalls mit einer Verurteilung des Rechtsanwalts wegen Verletzung des Auskunftsrechts eines Betroffenen endete die Anfrage eines potenziellen Mandanten, den der Anwalt unter seiner privaten Geheimnummer kontaktiert hatte. Für die DSB war in beiden Fällen nicht nachvollziehbar, weshalb die Interessen des Beschwerdegegners sowie des – nicht näher spezifizierten – Mandanten das Interesse des Beschwerdeführers jedenfalls zur Gänze überwogen und deshalb keine Auskunft erteilt werden konnte.[29]

Hätten die belangten Rechtsanwälte unter Nennung der in jedem Schriftsatzrubrum ablesbaren Daten des Gegners (vgl § 75 Z 1 ZPO) entweder lapidar Auskunft erteilt (Fall 1) oder besondere Umstände dargetan, die ein überwiegendes Interesse des Auftraggebers oder des Dritten an der Nichterteilung der Auskunft über die eigenen Daten des Betroffenen begründet hätten (Fall 2), wäre es nicht zu einer Verletzung des Auskunftsrechts gekommen.[30]

Die DSB vertritt auch bezüglich anderer beruflicher oder amtlicher Verschwiegenheitspflichten die Auffassung, dass ein bloß pauschaler Verweis darauf den Geheimnisträger nicht davon entbindet, Auskunft zu erteilen. Der ÖRAK ist an die DSB herangetreten und hat sich um eine Lösung iSd Rechtsstaatlichkeit und aller

22 Zur früheren Datenanwendung iSv § 58 DSG 2000 siehe *Thiele*, Die anwaltliche Datenverarbeitung de lege lata und de lege ferenda, ZIIR 2017, 370 (374).

23 Bereits *Thiele*, ZIIR 2017, 370 (373).

24 Näheres unter <https://dvr.dsk.gv.at/> (5. 3. 2018).

25 Näher dazu *Seiser*, Von der Meldepflicht nach dem DSG 2000 zur Verzeichnisführungspflicht des Art 30 DS-GVO, jusIT 2018/26, 71 bzw in Bergauer/Jahnel/Mader/Staudegger (Hrsg), jusIT Spezial: DS-GVO (2018) 107.

26 Aufgrund legistischer Untätigkeit besteht allerdings derzeit (5. 3. 2018) ein massives Ausführungsdefizit; vgl *Anderl/Hörlsberger/Müller*, Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018/3, 14 (16).

27 EGMR (Große Kammer) 27. 6. 2017, 931/13 (Satakunnan Markkinapörssi Oy and Satamedia Oy) = jusIT 2017/68; dazu *Thiele*, Kein SMS-Dienst mit Steuerdaten – vom Straßburger Ende für finnische Geschäftsmodelle, jusIT 2017/64, 149 mwN.

28 DSB 27. 10. 2014, DSB-D122.215/0004-DSB/2014 = jusIT 2015/11, 32 (*König*).

29 DSB 9. 3. 2015, DSB-D122.299/0003-DSB/2015, RIDA-Nr 0300579.

30 So bereits *Thiele*, ZIIR 2017, 370 (374).

KollegInnen bemüht.[31] Im Ergebnis sieht nunmehr § 9 Abs 3a RAO idF Art 108 des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl I 32/2018, ausdrücklich einen Vorrang (a) der anwaltlichen Verschwiegenheit zur Sicherstellung des Schutzes der Partei oder (b) der Rechte und Freiheiten anderer Personen oder (c) der Durchsetzung zivilrechtlicher Ansprüche vor. Darauf dürfen und sollen sich demnach RechtsanwältInnen berufen, die mit Ansprüchen nach Art 11–22 oder Art 34 DS-GVO konfrontiert werden.

3.3. Im Kanzleibetrieb zu beachtende Verpflichtungen nach neuem Datenschutzregime

Die RechtsanwältInnen treffen insb – ohne Anspruch auf Vollständigkeit – folgende wesentliche Pflichten[32] als (eigenverantwortliche) Verantwortliche:

- Offenlegung der Identität des Verantwortlichen bei Datenverarbeitungen,[33]
- Nachweis der Zulässigkeit der Datenverwendung gemäß anwaltlicher Berufsausübung,
- Dokumentation und Aktualisierung der ergriffenen Datensicherheitsmaßnahmen,[34]
- Verpflichtung der Kanzleimitarbeiter auf das Datengeheimnis nach § 6 DSG (2018),
- Überbindung von Verschwiegenheits- und Leistungspflichten an IT-Dienstleister der Kanzlei,[35]
- Informationspflicht an Klienten: Informationspflicht anlässlich direkter Ermittlung über Zweck und Auftraggeber gem § 13 DS-GVO; spätestens zum Zeitpunkt der Übermittlung bei indirekter Datenerhebung nach Art 14 DS-GVO; umfasst auch notwendige weitere Informationspflichten; entfällt unter gewissen Bedingungen,[36]
- Data Breach Notification (Art 33 und 34 DS-GVO): besondere Informationspflicht bei Datenmissbrauch an die Behörde und/oder an Betroffene zur Vermeidung von Vermögensschäden,[37]
- Richtigstellung unrichtiger Daten,
- Ermöglichung der eingeschränkten Verarbeitung,
- Gewährung von Datenportabilität,
- Beauskunftung von verarbeiteten Daten nach Art 15 DS-GVO,
- Löschung unzulässig verarbeiteter oder nicht mehr gebrauchter Daten.

Wenn der Rechtsanwalt diesen Pflichten nicht nachkommt, kann der Betroffene seine durch die DS-GVO gewährten Rechte bei der Datenschutzbehörde nach § 24 DSG (2018) geltend machen. Im Unterschied zur bisherigen Rechtslage[38] sind die Zwangsbefugnisse der DSB nach Art 58 DS-GVO erheblich erweitert worden. Neben der Verhängung abschreckender Bußgelder[39] sanktioniert § 62 DSG (2018) die Verletzung des Datengeheimnisses, der Voraussetzungen der Bildverarbeitung (ehemals Videoüberwachung) und die Verweigerung der behördlichen Einschau nach § 22 DSG (2018) mit einer Verwaltungsstrafe in Höhe von bis zu € 50.000. Daneben hat die DSB das Recht, im Fall eines begründeten Verdachts einer Pflichtverletzung Datenanwendungen zu untersagen.

4. DS-GVO: Erhöhte Compliance für die anwaltliche Datenverarbeitung

4.1. Drakonische Strafen

Die datenverarbeitenden Unternehmen – einschließlich der Anwaltskanzleien – müssen ungeachtet ihrer berufsrechtlichen Verschwiegenheitsverpflichtung jederzeit nachweisen können, dass sie alle Vorschriften der DS-GVO einhalten (sog *„Privacy Accountability"*). Gelingt der Nachweis nicht, droht nach Art 83 DS-GVO die Verhängung eines Bußgeldes in Höhe von bis zu € 20,000.000 oder 4 % vom Jahresumsatz, je nachdem, welcher Betrag höher ist. Rechtsanwaltskanzleien sind deshalb verpflichtet, nachweisen zu können, dass die eingesetzte IT sowie die Verarbeitung der Klienten- und Mitarbeiterdaten den datenschutzrechtlichen Standards der DS-GVO entsprechen.

4.2. Verarbeitungsverzeichnis

Im Betrieb ihrer/seiner Rechtsanwaltskanzlei nimmt jede/r österreichische Anwältin/Anwalt Datenverarbeitungen iZm ihrer/seiner Berufsausübung nicht bloß gelegentlich vor. Damit besteht die zwingende gesetzliche Verpflichtung für jede Anwaltskanzlei, ein Verzeichnis von Verarbeitungstätigkeiten (VVZ) nach Art 30 DS-GVO zu führen. Die Anwaltskanzlei verarbeitet zwangsläufig auch strafrechtsbezogene und sensible Daten von Klienten oder Dritten. Daher benötigt auch der Einzelanwalt ein Verarbeitungsverzeichnis.[40] Dabei handelt es sich – vereinfacht formuliert – um eine Liste von im Betrieb geführten Datenanwendungen.[41]

Der verantwortliche Anwalt/die verantwortliche Anwältin hat die im Verarbeitungsverzeichnis enthaltenen Angaben – sofern etabliert – dem Datenschutzbeauftragten zur Prüfung zur Verfügung zu stellen; über individuelle Aufforderung der Datenschutzbehörde im Kontrollfall muss das VVZ vorgelegt werden. Dies gilt auch für Verarbeitungstätigkeiten, die von anderen Stellen im

31 *ÖRAK*, Wahrnehmungsbericht 2016/17, AnwBl 2017, 14.
32 So bereits *Thiele*, ZIIR 2017, 370 (374) zum DSG 2000.
33 Die Angabe der DVR-Nummer ist in der Übergangszeit bis Ende 2019 weiterhin ausreichend.
34 UU in enger Zusammenarbeit mit den Herstellern für die eingesetzte Kanzleisoftware.
35 Vgl § 6 DSG (2018) iVm § 9 RAO und Art 28 Abs 3 und Art 32 Abs 4 DS-GVO.
36 Vgl Art 13 Abs 4 DS-GVO bzw Art 14 Abs 5 lit d DS-GVO: „die personenbezogenen Daten dem […] Berufsgeheimnis […] unterliegen".
37 Vgl zur derzeitigen Rechtslage die Empfehlung der DSB 24. 5. 2016, DSB-D213.462/0001-DSB/2016 (Patientenserviceprogramm) = RIDA-Nr 0313953; instruktiv *Pachinger*, „Datenvorfall" – was tun?, ZIR 2013, 244.
38 Dazu bereits *Thiele*, ZIIR 2017, 370 (374).
39 Siehe gleich unten Punkt 4.1.
40 Zur praktischen Erstellung bei ordnungsgemäßer DVR-Meldung vgl *Seiser*, DVR adé: Das österreichische Datenverarbeitungsregister entfällt ab Mai 2018, ZIIR 2018, 380.
41 Ausführlich bereits *Horn*, Die Dokumentationspflichten im Verarbeitungsverzeichnis nach Art 30 DS-GVO. Regulatorische Mindestinhalte, Gestaltung, operative Führung und Verantwortlichkeit, jusIT 2017/49, 106 mwN.

Wege der Auftragsdatenverarbeitung durchgeführt werden (erweiterte Rechenschaftspflicht). Insoweit enthält § 36 Abs 1a RAO idF BGBl I 32/2018 eine ausdrückliche Klarstellung für die Registerführungen durch den Österreichischen Rechtsanwaltskammertag (ÖRAK), der kraft Gesetzes allein verantwortlich dafür zeichnet.

4.3. Privacy Impact Assessment

Die Verpflichtung zur sog „Datenschutz-Folgenabschätzung" (*Privacy Impact Assessment* – PIA) bedeutet, vereinfacht formuliert, anhand eines risikobasierten Ansatzes die Wahrscheinlichkeit der Gefährdung von Betroffenen einer bestimmten Datenanwendung des Verantwortlichen zu bewerten.[42]

Die DSB erstellt dazu sog „schwarze Listen" (Datenschutz-Folgenabschätzung immer durchzuführen) und „weiße Listen" (Datenschutz-Folgenabschätzung nie durchzuführen) von Verarbeitungen.[43] Die anwaltliche Datenverarbeitung im Kanzleibetrieb von „einzelnen Rechtsanwälten" hat in die Whitelist (DSFA-AV, BGBl II 108/2018) Eingang gefunden. Dessen ungeachtet ist nicht für jede Datenanwendung einer mehrgliedrigen Rechtsanwaltskanzlei oder jede anwaltliche Berufsausübung eine PIA zwingend erforderlich.

4.4. Gesteigerte Informationspflichten gegenüber Mandanten

Für die anwaltliche Berufsausübung ändert sich vor allem der Umgang mit Klientendaten bei der Erstinformation. Art 7 und 8 DS-GVO unterscheiden nämlich zwischen einer Datenerfassung direkt bei der betroffenen Person und einer sonstigen Datenerfassung. Im ersten Fall, also typischerweise bei der ersten anwaltlichen Auskunft bzw Besprechung der Causa mit den MandantInnen, sind die Informationen über

- die zu verarbeitenden Datenarten (samt Erforderlichkeit),
- den Verarbeitungszweck (samt Speicherdauer),
- den Verantwortlichen (samt Rechtsgrundlagen),
- die Datenempfänger(kreise) sowie
- eine Aufklärung über die Betroffenenrechte

unaufgefordert zu erteilen, dh, es ist insoweit keine Anfrage der betroffenen Person erforderlich, und zu dokumentieren. Die davon allein bestehende Ausnahme des Art 13 Abs 4 DS-GVO, wonach der Mandant ohnehin ganz genau weiß, welche Daten zu welchen Zwecken wie verarbeitet werden, greift in der Praxis mE nicht.

Bei indirekter Ermittlung, zB durch Beschaffung aus Grundbuch-, Firmenbuch oder von Sozialversicherungsträgern, sind die oben genannten Informationen ebenfalls zur Verfügung zu stellen. Sie sind allerdings binnen angemessener Frist, dh höchstens einem Monat oder bei früherer Verarbeitung im Zeitpunkt der ersten Kommunikation mit der betroffenen Person oder bei Übermittlung der Daten an andere Empfänger, zu erteilen.[44] Die gesetzliche Ausnahme der Wahrung des anwaltlichen Berufsgeheimnisses nach Art 14 Abs 5 lit d DS-GVO greift in Fällen indirekter Ermittlung regelmäßig zugunsten der AnwältInnen ein.

4.5. Etablierung von Datenschutzbeauftragten

Es ist für anwaltliche Unternehmer nicht einfach zu entscheiden, ob sie einen DSBA zwingend benötigen. Exorbitant hohe Bußgelder drohen aber für den Fall, dass ein DSBA nach Art 37 DS-GVO zu benennen war, dies aber für den Kanzleibetrieb unterlassen wurde.

Entscheidende Voraussetzung einer DSBA-Pflicht für AnwältInnen ist die „umfangreiche Verarbeitung" iSv Art 37 Abs 1 lit c DS-GVO. Dass *„processing on a large scale"*, so die deutlichere englische Fassung, durchaus von kleineren Rechtsanwaltskanzleien erreicht werden kann, wenn sie (einzelne) Fälle mit großen Datenmengen bearbeiten, bestätigt die Empfehlung des Rates der Europäischen Anwaltschaften (CCBE): *„However, it may be easy to argue, on the basis of recital 91 that this requirement will not apply to solo practitioners"*.[45] Es ist daher anzunehmen, dass eine Anwaltsgemeinschaft (zB GesBR, GmbH oder KG), die aus zwei oder mehr Rechtsanwälten besteht, idR eine umfangreiche Datenverarbeitung durchführt und daher einen Datenschutzbeauftragten zwingend benötigt. Ob diese Verpflichtung auch den „Einzelkämpfer" trifft, ist durchaus umstritten.[46]

Besonderes Augenmerk verdient in diesem Zusammenhang die Position des Rechtsanwalts als Insolvenzverwalter. Dieser wird nämlich vom Insolvenzgericht bestellt und ihm obliegt die praktische Durchführung des Insolvenzverfahrens. Bei Einordnung dieser – als Verantwortlicher oder Auftragsverarbeiter – zu erfüllenden Tätigkeit als die einer „öffentlichen Stelle" iSv Art 37 Abs 1 lit a und Abs 3 DS-GVO besteht DSBA-Pflicht für die Anwaltskanzlei. Der Begriff der „öffentlichen Stelle" geht ausweislich ErwGr 45 davon aus, dass es sich dabei um unter das öffentliche Recht des jeweiligen Mitgliedstaates fallende natürliche oder juristische Personen handeln kann.[47] RechtsanwältInnen als natürliche Personen sind demnach dann öffentliche Stellen, wenn ihre Beleihung auf öffentlich-rechtlicher Grundlage beruht.[48] Der stets ad personam bestellte Masse- oder Sanierungsverwalter[49] ist aber ein Organ des Insolvenzgerichts, dessen Bestellung öffentlich kundgemacht ist.[50] Es handelt sich also um eine justizielle Tätigkeit, die unter die

42 Vgl die Stellungnahme der Art 29-Gruppe zur Datenschutz-Folgenabschätzung vom 4. 4. 2017, WP 248 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137> (5. 3. 2018).

43 Vgl die Ermächtigung in § 21 Abs 2 DSG (2018).

44 Vgl *Graf/Križanac*, Checkliste DS-GVO Compliance, ecolex 2017, 925 (928 f) samt Checklisten.

45 CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR) vom 19. 5. 2017 <http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf> (5. 3. 2018).

46 Vgl zum Meinungsstand *Thiele*, ZIIR 2017, 370 (376 f) mwN.

47 *Heberlein* in Ehmann/Selmayr, Art 37 Rz 19.

48 Vgl *Heberlein* in Ehmann/Selmayr, Art 37 Rz 20.

49 Vgl *Riel*, Wer ist Insolvenzverwalter?, ZIK 2012, 47.

50 OGH 3. 8. 2006, 8 Ob 80/06g (Amtsausübung des Masseverwalters) = ZIK 2006/275, 207 = RdW 2007/104, 92.

Bereichsausnahme für Gerichte nach Art 37 Abs 1 lit a letzter Halbsatz DS-GVO fällt. Insoweit bedürfen auch Insolvenzverwalter kraft ihrer Stellung keines DSBA. Es bleibt daher bei der str Klärung des Begriffes „umfangreich" nach Art 37 Abs 1 lit c leg cit.[51]

Ungeachtet der Frage einer DSBA-Pflicht ist auch für AnwältInnen eine unzutreffende Erwartungshaltung zu vermeiden: Die datenschutzrechtliche Haftung als Verantwortlicher nach außen trifft stets den Inhaber des Kanzleibetriebs; eine Zurechnung nach § 9 VStG an den DSBA ist ausgeschlossen, da ihm exekutive Befugnisse fehlen.

Für RechtsanwältInnen abschließend bemerkenswert erscheint die CCBE-Empfehlung zur Rolle des Anwalts als externem Datenschutzbeauftragten, diese Position für den Mandanten lediglich dann einzunehmen *„if they have neither acted as a lawyer in matters which might fall within the DPO's responsibility nor will act, during their term as DPO, as a lawyer in matters they were or are involved in as DPO"*.[52]

5. Zusammenfassung

Jede Rechtsanwaltskanzlei ist ein datenverarbeitender Betrieb iSd DS-GVO. Auf die/den für dieses Unternehmen verantwortliche/n Rechtsanwältin/Rechtsanwalt kommen daher all jene Aufgaben zu, die auch sonstige Datenschutzverantwortliche treffen. Ein Datenschutzbeauftragter unterstützt dabei, verantwortet aber nicht nach außen. Die besondere Verpflichtung zum sorgsamen Datenumgang für und durch RechtsanwältInnen in eigenen Angelegenheiten resultiert aber auch aus der unverzichtbaren Bedeutung der juristisch versierten berufsmäßigen Parteienvertreter im Rechtsstaat.

Die einzelnen Umsetzungsschritte in Anwaltskanzleien umfassen daher die vollständige Erfassung der IT-Systeme, die Bildung von Awareness der Mitarbeiter (Schulung), die Auswertung der Erfassungsergebnisse in technischer und juristischer Hinsicht, das Vorbereiten des Verarbeitungsverzeichnisses einschließlich der rechtlichen Prüfung (Speicherdauer, Löschfristen, Rechtsgrundlagen) mit dem Ziel, ein IT-basiertes Datenmanagementsystem zu verwirklichen. Die unverzügliche und rechtssichere Reaktion auf eine Datenpanne muss ebenso vorbereitet sein wie ein professioneller und rascher Umgang mit Betroffenen- und Mitarbeiterrechten.

51 Für eine DSBA-Pflicht auch bei Einzelanwaltskanzleien *Thiele*, ZIIR 2017, 370 (377).

52 CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR) vom 19. 5. 2017 <http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf> (5. 3. 2018).

Der Autor:

RA Hon.-Prof. Dr. **Clemens Thiele**, LL.M. Tax (GGU) studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

Publikationen des Autors:

Standardkommentar zum RATG[3] (2011); Werbeabgabegesetz Praxiskommentar[2] (2012); gemeinsam mit Elisabeth Staudegger Mitherausgeber des Jahrbuchs Geistiges Eigentum 2012 bis 2017; Co-Autor in Ciresa (Hrsg), Österreichisches Urheberrecht Kommentar; zahlreiche Beiträge in Fachzeitschriften zu Datenschutzthemen.

Anwalt.Thiele@eurolawyer.at

lesen.lexisnexis.at/autor/Thiele/Clemens

Foto: D. Wild

Dr. Raffaela Zillner, LL.M. • Wien

Informationspflichten bei der Erhebung von Daten nach der DS-GVO*

» jusIT 2018/43

Datenschutzrecht, Informationspflicht, Transparenz, Modalitäten der Informationserteilung, Datenverarbeitung, Erhebung von Daten, personenbezogene Daten, DS-GVO

§ VO (EU) 2016/679: Art 5, Art 12, Art 13, Art 14

Bei der Erhebung personenbezogener Daten müssen nach der DS-GVO künftig zahlreiche Informationspflichten erfüllt werden. Neben konkreten Vorgaben, welche Informationen erteilt werden müssen, gibt die DS-GVO auch vor, auf welche Art und Weise die Informationserteilung zu erfolgen hat. Dabei wird grundsätzlich unterschieden, ob die Daten bei der betroffenen Person selbst erhoben werden oder aus anderer Quelle stammen. Diesen erhöhten Informationspflichten liegt der Grundsatz der Transparenz zugrunde, aufgrund dessen betroffene Personen genau

* Dieser Beitrag wurde auch publiziert in Bergauer/Jahnel/Mader/Staudegger (Hrsg), jusIT Spezial: DS-GVO (2018) 67.