Anwaltsbüro Dr. Stebner
Arzneimittel- und Medizinrecht

Anwaltsbüro Dr. Stebner · Reitling 3 · 38228 Salzgitter

Dr. jur. Frank A. Stebner
Rechtsanwalt
Fachanwalt für Medizinrecht

Reitling 3
38228 Salzgitter

Tel.: 0 53 41/85 31-0
Fax: 0 53 41/85 31-50
Email: info@drstebner.de
Internet: www.DrStebner.de

Basisinformationen für Mitglieder des VFP mit der Berufsausübung „Psychologischer Berater/Coach“

Salzgitter, den 27.03.2019
Rechtsanwalt Dr. Stebner

Datenschutz im Berufsalltag:
Praktische Hinweise für Psychologische Berater/Coaches (PB)

Am 25. Mai 2018 traten die Datenschutz-Grundverordnung/VO (EU) 2016/679 (**DS-GVO**) (https://dsgvo-gesetz.de/) und das neue Bundesdatenschutzgesetz (**BDSG-N**) (https://dsgvo-gesetz.de/bdsg-neu/) in Kraft. Die vollständig neu geordnete Rechtslage brachte gravierende Änderungen, die aber zu Unrecht von vielen als katastrophal für die berufliche Organisation und das PB-Klienten-Verhältnis wahrgenommen wurden. Die sachliche und juristisch fundierte Auseinandersetzung mit dem neuen Recht sowie die ersten praktischen Erfahrungen im zweiten Halbjahr 2018 ergeben ein anderes Bild: Vieles wurde dramatisiert, und wenngleich das neue Recht nicht einfach ist, so lässt es sich doch mit Augenmaß und Wohlwollen praktisch handhabbar im Alltag umsetzen, ohne übertriebenen Organisationsaufwand und Störung der Beratungen.

Die Informationen über das neue Recht sind insbesondere im Internet vielfältig, aber oft rudimentär und teilweise widersprüchlich. Deshalb will diese Basisinformation für

VFP-Mitglieder die neue Rechtslage verständlich beschreiben sowie praktische Empfehlungen für die Organisation und den Beratungsalltag mit Klienten geben.

1. Das neue Recht

Die DS-GVO ist als EU-Verordnung unmittelbar geltendes Recht in den Mitgliedsstaaten. Der Deutsche Bundestag beschloss ergänzend das BDSG-N. Das neue Recht ist von den Berufsträgern seit dem 25.05.2018 verbindlich zu beachten. Die DS-GVO ist datenschutzrechtlich denkbar weit gefasst und wird ergänzend ausgelegt im BDSG-N. Es besteht also seit dem 25.05.2018 ein Nebeneinander von europäischem und deutschem Datenschutzrecht. Die DS-GVO wirft nach ersten juristischen Analysen zahlreiche Auslegungsfragen auf, die voraussichtlich durch den Europäischen Gerichtshof in den nächsten Jahren zu klären sein werden.

2. Anwendungsbereich

Das neue Recht gilt für alle Betriebe, die automatisiert Daten verarbeiten. Jede Benutzung von Computer, Internet, E-Mail kann also zur Anwendung führen, wenn personenbezogene Daten betroffen sind.

Erfasst wird auch die nicht automatisierte Verarbeitung, insbesondere bei handschriftlichen Aufzeichnungen, wenn die Absicht besteht, dass personenbezogene Daten (später) in ein Dateisystem aufgenommen werden (Art. 2 Abs. 2 DS-GVO). Handschriftlich geführte Dokumentationen über Klienten können also unter die nicht automatisierte Verarbeitung fallen und damit der automatisierten Datenverarbeitung gleichstehen.

Verarbeitung ist ein zentraler Begriff und in Art. 4 Nr. 2. DS-GVO definiert. Zu den Definitionsmerkmalen gehört die „Speicherung" der personenbezogenen Daten. Erfolgt keine Speicherung, sondern die Löschung nach der Datenerhebung, ist der Anwendungsbereich des Datenschutzrechts nicht eröffnet.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Werden von Klienten eingegangene E-Mails beantwortet, beide mit Papierausdruck zur Akte genommen und die Daten im Rechner gelöscht, erfolgt keine Speicherung. Wenn während der Beratung eine Dokumentation mit Hilfe des Rechners erfolgt, ein

Papierausdruck gefertigt und die Daten gelöscht werden, ist ebenfalls der Anwendungsbereich des Datenschutzrechts nicht eröffnet. Die Beispielsfälle wären nur anders zu beurteilen, wenn die „Absicht" bestehen würde, die Papierausdrucke später noch elektronisch zu verarbeiten. „Absicht" ist freilich ein innerer Vorgang, der als subjektiver Bereich des PB im Allgemeinen nicht von außen verifizierbar ist.

3. Personenbezogene Daten

Der Begriff der personenbezogenen Daten ist in Art. 4 Nr. 1. DS-GVO sehr weit gefasst und bleibt auch dadurch unscharf. Darunter fallen beispielsweise Informationen wie Name, Adresse, Telefonnummer oder aber auch die IP-Adresse einer Person. Ausreichend ist bereits, wenn die Informationen einer Person lediglich irgendwie zugeordnet und damit ein Personenbezug hergestellt werden kann.

Es ist davon auszugehen, dass sämtliche Dokumentationen und schriftliche Kommunikation des PB über Klienten personenbezogen sind.

4. Datenschutzbeauftragter

Nach Art. 37 Abs. 1 b) und c) DS-GVO muss ein Datenschutzbeauftragter unter den genannten Voraussetzungen bestellt werden. Diese sind:

> Der Verantwortliche benennt auf jeden Fall einen Datenschutzbeauftragten, wenn
> b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
> c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht.

Für PB dürften diese Voraussetzungen grundsätzlich nicht zutreffen.

Allerdings müssen Verantwortliche nach § 38 Abs. 1 Satz 1 BDSG-N unabhängig von der vorgenannten Vorschrift einen Datenschutzbeauftragten bestellen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Maßgebend ist also nicht die Menge der

Mitarbeiter, sondern die Anzahl der Mitarbeiter, die „ständig“ in der automatisierten Datenverarbeitung tätig sind.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Große PB-Unternehmen mit zehn und mehr Mitarbeitern (der Betriebsinhaber wird dabei mitgezählt) sollten in einem **Organisationsplan** festlegen, welche Personen „ständig“ mit der automatisierten Verarbeitung der Klientenendaten beschäftigt sind. Nach den Organisationsabläufen wird es möglich sein, die Anzahl dieser Mitarbeiter auf höchstens neun Personen zu begrenzen, sodass ein Datenschutzbeauftragter nicht engagiert werden muss. Rechtlich unerheblich ist es, wenn andere Mitarbeiter gelegentlich untergeordnet in der elektronischen Datenverarbeitung mitwirken.

5. Datenschutz-Folgenabschätzung (DSFA)

Art. 35 Abs. 1 DS-GVO verpflichtet unter den genannten Voraussetzungen Unternehmen zur Erstellung einer Datenschutz-Folgenabschätzung. Die Norm lautet:

> Hat eine Form der Verarbeitung, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

„Der Begriff Rechte und Freiheiten natürlicher Personen ist weit gefasst und bezieht sich deshalb nicht nur auf den Schutz von personenbezogenen Daten. Die Erwägungsgründe 83 und 85 zählen beispielhaft denkbare Risiken für natürliche Personen auf, die bei dieser Betrachtung eine Rolle spielen können. Dazu zählen u. a. physische, materielle oder immaterielle Schäden aufgrund der Vernichtung, des Verlustes oder der Veränderung der personenbezogenen Daten, Einschränkungen von Rechten, Diskriminierung, Identitätsdiebstahl, Betrug, finanzielle Verluste, unbefugte Aufhebung einer Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für besondere natürliche Personen“ (Gola, DS-GVO, 2. Auflage München 2018, Rdnr. 12 zu Art. 35).

Eine Umfrage des Anwaltsbüros Dr. Stebner im Auftrag des VFP bei Datenschutzbeauftragten des Bundes und der Bundesländer ergab, dass in Heilpraktikerpraxen eine stets zu aktualisierende DSFA nicht zu erstellen sei. Dieses Ergebnis kann auf PB-Betriebe übertragen werden, sodass bei normalem Betrieb keine DSFA erstellt werden muss.

6. Technische und organisatorische Maßnahmen der Datensicherheit

Art. 32 DS-GVO verpflichtet jedes Unternehmen zu Maßnahmen, die die Integrität und Vertraulichkeit der Datenverarbeitung gewährleisten. Eine interne Checkliste ist empfehlenswert, die bei rechtlichen Auseinandersetzungen vorgelegt werden kann. Der VFP stellt seinen PB-Mitgliedern die **Checkliste „Technische und organisatorische Maßnahmen der Datensicherheit"** zur Verfügung (**Anlage 1**). Die Checkliste ist ein Grundmuster, das den individuellen Gegebenheiten des Unternehmens angepasst werden muss.

7. Verzeichnis von Verarbeitungstätigkeiten

Nach Art. 30 Abs. 1 DS-GVO ist in Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Es ist Änderungen in der Organisation permanent anzupassen.

Der VFP hält für seine PB-Mitglieder zwei Muster bereit:

- Verzeichnis von Verarbeitungstätigkeiten (**Anlage 2**);
- Ausfüllhinweise zum „Verzeichnis von Verarbeitungstätigkeiten" (**Anlage 3**). (Das Muster ist beispielhaft ausgefüllt; aufgeführt sind zwei Verarbeitungstätigkeiten.)

8. Informationspflichten / Einwilligungserklärung

Zu unterscheiden sind Informationspflichten bei der Erhebung personenbezogener Daten direkt beim Betroffenen (Art. 13 DS-GVO) und bei der Erhebung aus vorhandenen Datensammlungen (Art. 14 DS-GVO).

Die Verantwortlichen für die Datenerhebung müssen nach Art. 13 DS-GVO künftig eine Reihe von Auskünften bereitstellen. Nach Art. 13 Abs. 1 DS-GVO wird angeordnet: Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt

der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Der Verantwortliche muss nach Art. 13 Abs. 2 a) DS-GVO der betroffenen Person die Dauer mitteilen, für die die personenbezogenen Daten gespeichert werden.

Ferner ist nach Art. 13 Abs. 2 b) DS-GVO die betroffene Person zu informieren über

> das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit.

Nach Art. 6 Abs. 1 Satz 1a) DS-GVO ist die Verarbeitung nur rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Das neue Recht bringt hier eine rechtliche Erleichterung, weil das grundsätzliche Schriftformerfordernis entfallen ist (Koreng/Lachenmann – Bergt, Datenschutzrecht, 2. Auflage München 2018, S. 937). Aus Gründen einer juristisch sicheren Nachweisprüfung ist jedoch zu einer schriftli-

chen Einwilligung der Klienten zu raten, zumindest sollte eine eindeutige Dokumentation in der Akte erfolgen. Der VFP rät seinen Mitgliedern zu einer **schriftlichen Einwilligungserklärung** und stellt ihnen ein **Muster** zur Verfügung.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Es ist juristisch ausreichend, den Klienten das Formular zur Unterschrift vorzulegen, wenn sie erstmals seit Mai 2018 wieder einen Beratungstermin wahrnehmen. Die Aushändigung einer Kopie ist nicht verpflichtend, muss aber auf Nachfrage des Klienten erfolgen. Da den Klienten eine Datenschutzinformation ausgehändigt werden muss (siehe Nr. 14.), ist das Musterformular als **Datenschutzinformation und Erklärung zur Einwilligung in die Datenverarbeitung kombiniert** (**Anlage 4**). Durch seine Unterschrift bestätigt der Klient auch den Erhalt der Datenschutzinformation. Wird das Kombinationsformular verwendet, muss dem Klienten zur Erfüllung der Informationspflichten eine Kopie ausgehändigt werden.

Für **Organisationsgemeinschaften** bestehen besondere Anforderungen für die Einhaltung der Schweigepflicht und die Einwilligung der Klienten. Das Musterformular „Datenschutzinformation und Erklärung zur Einwilligung in die Datenverarbeitung" (Anlage 4) ist deshalb speziell für Organisationsgemeinschaften erweitert worden als Musterformular **„Datenschutzinformation und Erklärung zur Einwilligung (1) in die Organisationsgemeinschaft und (2) in die Datenverarbeitung"** (**Anlage 5**). In Einzelunternehmen ist lediglich das Musterformular Anlage 4 zu verwenden.

Die Musterformulare erfüllen die Anforderung, inhaltlich „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache ... (zu) erfolgen" (Art. 7 Abs. 2 Satz 1 DS-GVO). Nicht ausreichend sind deshalb fiktive Einwilligungserklärungen auf der Website oder ein Aushang im Wartezimmer.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Manche PB möchten ihren Klienten personenbezogene Daten via WhatsApp übermitteln. Das juristische Problem ist, ob Klienten **wirksam in die WhatsApp-Nutzung einwilligen** können.

WhatsApp ist ein Instant-Messenger-Dienst, der in die Kategorie „Over-the-top“ (OTT)-Kommunikationsdienste gefasst wird (Spindler/Schmitz, TMG, 2. Auflage München 2018, Rdnr. 26). Der Dienstleister „on the top“ leitet mindestens die in der jeweiligen Kontakte-App gespeicherten Rufnummern vollständig an die Anbieter in den USA weiter (Koreng/Lachenmann, Datenschutzrecht, 2. Auflage München 2018, Seite 380), und WhatsApp wird bei Nutzung der Zugriff auf das Adressbuch gegeben. Das juristische Problem dabei ist die Wirksamkeit der Einwilligung des Klienten in die WhatsApp-Nutzung, konkret in die Nutzung der Kontaktdaten durch den Dienstleister. Wenn wir davon ausgehen, dass unkontrolliert Daten abgeschöpft werden, geschieht dies nicht durch den PB, sondern durch den Dienstleister (on the top), der von PB und Klient genutzt wird. Es wird deshalb auch die Ansicht vertreten, dass das datenschutzrechtliche Problem eigentlich bei dem Dienstleister „on the top“ liegt.

Zu einer wirksamen Einwilligung nach Art. 7 Abs. 1 DS-GVO gehört das Erfordernis der ausreichenden Informiertheit des Einwilligenden. Die erforderliche Informiertheit ist gegeben, wenn die Einwilligung auf der Kenntnis aller hierfür erforderlichen Umstände beruht (Ehmann/Selmayr, DS-GVO, 2. Auflage München 2018, Rdnr. 58 zu Art. 7). Es bleibt festzuhalten, dass nach dem Erwägungsgrund 32 eine ausreichende Informiertheit für die Einwilligung erforderlich ist und der Einwilligende für den konkreten Fall und in Kenntnis der Sachlage die Einwilligung abgeben muss, d. h., die betroffene Person muss wissen, was mit den Daten geschehen soll (Gola, DS-GVO, 2. Auflage München 2018, Rdnr. 34 zu Art. 7). Die ausreichende Informiertheit wird bei der WhatsApp-Einwilligung von Datenschutzbehörden infrage gestellt.

Alles in allem handelt es sich bei der Einwilligung des Klienten in die WhatsApp-Nutzung um eine streitige Angelegenheit, sodass zumindest den PB, die einen „vorsichtigen Weg“ verfolgen, von der WhatsApp-Nutzung abzuraten ist. Anderen PB, die trotz der Umstrittenheit der wirksamen Einwilligung WhatsApp nutzen wollen, ist zu raten, die Aufklärung in der schriftlichen Einwilligung so ausführlich wie möglich zu halten.

9. E-Mail-Adressen im Datenbestand von Stammkunden

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:

Manche PB haben einen großen Datenbestand von Klienten, die gegenwärtig nicht betreut werden. Zu den Daten können auch E-Mail-Adressen gehören. Es stellt sich die Frage, ob PB diese E-Mail-Adressen zur Kommunikation (z. B. für allgemeine Informationen oder für die Bestätigung telefonisch vereinbarter Termine) nutzen können, auch dann, wenn (noch) keine schriftliche Einwilligung der Klienten in die Nutzung vorliegt.

Die Verarbeitung von Daten ist nur rechtmäßig, wenn mindestens eine der in Art. 6 Abs. 1 DS-GVO aufgeführten Bedingungen erfüllt ist. In Betracht kommt hier Art. 6 Abs. 1 lit. a) DS-GVO:

> Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.

Die Zwecke der Verarbeitung müssen nach Erwägungsgrund 32 zur DS-GVO für den bestimmten Fall, d. h. so konkret wie möglich, benannt werden. Blankoeinwilligungen oder pauschale Einwilligungen genügen dieser Vorgabe nicht.

Die Einwilligung kann zunächst schriftlich, elektronisch oder mündlich erfolgen. Möglich sind auch konkludente Einwilligungen, sofern die betroffene Person darüber eindeutig signalisiert, dass sie mit der Datenverarbeitung einverstanden ist (Gola, DS-GVO, 2. Auflage München 2018, Rdnr. 42 zu Art. 7). Erwägungsgrund 32 zur DS-GVO bestimmt, dass Stillschweigen, standardmäßig angekreuzte Kästchen oder Untätigkeit nicht als Einwilligung gewertet werden können.

Konkludentes (schlüssiges) Handeln ist das Verhalten, das eine Zielsetzung nicht unmittelbar durch eine ausdrückliche Erklärung, sondern nur mittelbar erkennen lässt. Ob ein schlüssiges Handeln vorliegt, ist durch Auslegung zu ermitteln.

Wenn ein Klient seine E-Mail-Adresse bekannt gibt, kann von seinem konkludenten Einverständnis ausgegangen werden, dass der PB die E-Mail-Adresse in der Kommunikation auch nutzen darf. Es sollte jedoch das ausdrückliche schriftliche Einver-

ständnis mit Verwendungszwecken vorliegen, weshalb bei nächster Gelegenheit die Einwilligungserklärung zur Unterschrift vorgelegt werden sollte. Die Einwilligungserklärung sollte genau festlegen, wozu die E-Mail-Adresse genutzt werden darf.

10. Datenschutzerklärung für die Website

Das neue Datenschutzrecht verlangt eine umfassende Datenschutzerklärung auf der Website. Jeder PB, der eine Website unterhält, sollte sehr großen Wert auf eine korrekte Datenschutzerklärung legen. Nach den Erfahrungen im zweiten Halbjahr 2018 besteht in der Umsetzung des neuen Datenschutzrechts mehr oder weniger allein bei der Datenschutzerklärung der Website das Abmahnrisiko. Die Website kann von jedem Ort jederzeit kontrolliert werden, was beispielsweise bei der den Klienten auszuhändigen Datenschutzinformation nicht der Fall ist. So erklärt sich die hohe juristische Komplikationsdichte bei der Website insbesondere bei der Datenschutzerklärung.

Der VFP hält für seine PB-Mitglieder das **Grundmuster einer Datenschutzerklärung für die Website** bereit (**Anlage 6**). Sie ist unbedingt dem Aufbau und der Gestaltung der Website individuell anzupassen. Das Grundmuster ist sehr weit gefasst. Ggf. müssen z. B. Dienste, die nicht genutzt werden, herausgenommen werden. Angaben zu zurzeit nicht genutzten Diensten können jedoch belassen werden, um für zukünftige Veränderungen der Website durch z. B. die Einbindung von Social Media eine Absicherung zu bieten.

Weiter erhalten Mitglieder des VFP ein Muster für die erforderliche **Ergänzung des Impressums** (**Anlage 7**).

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:

Muss eine Website, auf der (potentielle) Klienten ein Kontaktformular nutzen können, eine Verschlüsselung haben? Inzwischen liegen die ersten Erfahrungen und weiteren Beurteilungen zum neuen Datenschutzrecht vor. Nach Art. 32 Abs. 1 a) DS-GVO ist eine Verschlüsselung personenbezogener Daten bei Versendung erforderlich. Erfasst wird hier eine Website, die ein Kontaktformular hat. Hier ist eine SSL-Transportverschlüsselung für die Kontaktaufnahme seitens des Nutzers mit dem PB zwingend erforderlich, jedoch auch ausreichend.

11. „Cookie-Hinweis“ oder „Cookie-Einverständnis“ auf der Website

Beim Betrieb der Website stellt sich die Frage, ob ein „Cookie-Hinweis“ oder ein „Cookie-Einverständnis“ eingerichtet werden muss.

Cookies sind kleine Dateien, die von einem Internetanbieter auf dem Computer des Nutzers – zumeist ohne dessen Kenntnis – abgelegt werden. Anhand dieser Informationen kann der Webserver den Computer immer wieder identifizieren. Dadurch wird zum einen ein bequemes Surfen im Internet gewährleistet, z. B. dadurch, dass Waren, die bereits in den Warenkorb eines Onlineshops gelegt wurden, beim Weitersurfen dort gespeichert bleiben. D. h. also, Voreinstellungen bleiben bestehen, sodass man diese nicht immer wieder neu eingeben muss. Mit der Cookie-Technik können aber auch Profile über Surfgewohnheiten des Nutzers erstellt werden, da Informationen über das Verhalten des Nutzers gesammelt werden. Das hat zur Folge, dass z. B. dem Nutzer zu seinem Surfverhalten passende Werbung eingeblendet wird.

Es handelt sich bei Cookies um eine Kennung, die in Erwägungsgrund 30 zur DS-GVO ausdrücklich Erwähnung findet. Art. 4 Abs. 1 2. Halbsatz DS-GVO legt die Deutung nahe, dass jede „Kennung“ per se Personenbezug haben soll. Es ist somit zu erwarten, dass sich nach Inkrafttreten des DS-GVO die Auffassung durchsetzen wird, dass es sich bei Cookies stets und ausnahmslos um personenbezogene Daten handelt (Härting, Internetrecht, 6. Auflage Köln 2017, Rdnr. 227).

Die Frage ist, ob nach der DS-GVO eine Einwilligungserklärung vom Nutzer durch z. B. ein Pop-up-Fenster einzuholen ist. Gemäß Erwägungsgrund 32 sollen Einwilligungserklärungen, die auf elektronischem Wege eingeholt werden, „in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung abgegeben wird, erfolgen.“ Ob eine Einwilligungserklärung für Cookies erforderlich ist, wird in juristischen Fachkreisen unterschiedlich beurteilt. Die Rechtslage erscheint nach Recherche unklar (die Juristen sagen „non liquet“), weshalb den Mitgliedern nicht die Änderung der Website mit Aufnahme einer „Einwilligung in das Setzen von Cookies durch ein Pop-up-Fenster“ empfohlen werden muss. Aus juristischer Sicht ist ein Abwarten gerechtfertigt. Wer will, kann den Website-Nutzern durch ein Banner die Information zur Verwendung von Cookies geben.

Die DS-GVO und das neue Bundesdatenschutzgesetz regeln also die Frage der Cookies nicht ausdrücklich. Voraussichtlich wird 2019 eine EU-Verordnung zu ePrivacy erlassen. Dort wird es voraussichtlich Bestimmungen über Cookies geben. Auch aus diesem Aspekt heraus ist es gerechtfertigt, derzeit abzuwarten.

12. Datenschutzinformation / Datenschutzerklärung

Zu unterscheiden sind Datenschutzinformation und Datenschutzerklärung:

- **Datenschutzinformation**

  Die Datenschutzinformation muss allen Klienten ausgehändigt werden. Rechtlich noch ungeklärt ist, ob Aushänge ausreichend sind. Empfehlenswert ist die schriftliche Datenschutzinformation, am besten kombiniert im **Musterformular „Datenschutzinformation und Erklärung zur Einwilligung in die Datenverarbeitung“** (**Anlage 4**) für Einzelunternehmen.

  Für Organisationsgemeinschaften ist das spezielle **Musterformular „Datenschutzinformation und Erklärung zur Einwilligung (1) in die Organisationsgemeinschaft und (2) in die Datenverarbeitung“** (**Anlage 5**) entwickelt worden.

  Den Mitgliedern wird empfohlen, das VFP-Musterformular dem eigenen Unternehmen angepasst zu verwenden.

- Die **Datenschutzerklärung** bezieht sich auf die Unterhaltung einer Website. Es handelt sich dabei um Informationen im Sinne von Art. 12 Abs. 1 DS-GVO.

  Bei der Datenschutzerklärung ist zu unterscheiden, ob die Website lediglich betrachtet werden kann, oder ob darüber hinaus eine Kommunikation mit Kontaktformular möglich ist, also eine Datenverarbeitung. Erfolgt keine Datenverarbeitung, ist eine einfachere Information ausreichend. Erfolgt eine Datenverarbeitung, ist eine umfassende Information mit Einwilligungserklärung erforderlich.

Der VFP stellen seinen PB-Mitgliedern eine **Muster-Datenschutzerklärung** (**Anlage 6**) für die Website zur Verfügung. Dabei ist zu beachten, dass es sich um ein Grundmuster handelt, welches den individuellen Gegebenheiten der Website angepasst werden muss.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Wenn ein Klient trotz Erinnerung die Rechnung nicht begleicht, kann der PB dann eine Inkassobüro oder einen Rechtsanwalt mit dem Forderungseinzug beauftragen?

Ein Inkassobüro ist Dritter im Sinne von Art. 4 Nr. 10 DS-GVO. Die Datenweitergabe darf nur mit ausdrücklicher Einwilligung des Klienten erfolgen. Die überlegte Erweiterung der allgemeinen Einwilligungserklärung wird bei kritischer Prüfung als nicht wirksam einzustufen sein. Es ist deshalb von der Zusammenarbeit mit einem Inkassobüro (Bürgel, Creditreform usw.) abzuraten.

Ein Rechtsanwalt ist nicht Dritter im Sinne von Art. 4 Nr. 10 DS-GVO. Er ist Organ der Rechtspflege, unterliegt der strafbewehrten berufsrechtlichen Schweigepflicht und kann jederzeit zur zweckentsprechenden Rechtsverfolgung eingeschaltet werden. Der Zustimmung des Klienten bedarf es nicht. Voraussetzung ist allein, dass die Beauftragung des Rechtsanwalts notwendig ist. Befindet sich der Klient im Zahlungsverzug, ist die Beauftragung des Rechtsanwalts gerechtfertigt. Sicherheitshalber sollte eine zweite Mahnung an den Klienten vor Beauftragung des Rechtsanwalts gesendet werden. Die zeitliche Verzögerung ist hinzunehmen, da bereits bei Eintritt des Verzuges die Forderung verzinst wird. Die Verzinsung beträgt derzeit nach § 288 BGB rund 5 %.

13. Auskunftserteilung an anfragende Klienten

Nach Art. 15 Abs. 1 DS-GVO haben Klienten das Recht auf Auskunft über gespeicherte personenbezogene Daten und auf die explizit in Abs. 1 genannten Informationen.

Von dem Auskunftsrecht nach Art. 15 DS-GVO ist das Einsichtsrecht in die Dokumentation zu unterscheiden. Wird lediglich eine Auskunft nach Art. 15 DS-GVO verlangt, ist dies keine Geltendmachung einer Einsichtnahme in die Dokumentation.

Die Aufklärung des Klienten über seine Rechte nach Datenschutzrecht ist erforderlich. Für die PB ist es am einfachsten, wenn sie das VFP-Muster „Datenschutzerklärung" beifügen. Unverzichtbar im Anschreiben ist der Hinweis auf die Datenschutzbehörde/den Datenschutzbeauftragten (Koreng/Lachenmann, Datenschutzrecht, 2. Auflage München 2018, Seite 585). Die Kommunikationsdaten der Datenschutzbehörde des Bundeslandes, in dem das Unternehmen liegt, kann problemlos im Internet ermittelt werden.

Der VFP stellt seinen PB-Mitgliedern das **Musterformular – Auskunftserteilung an Klienten** zur Verfügung (**Anlage 8**).

14. Rechenschaftspflicht / Löschen und Vernichten von Daten

Die Rechenschafts- bzw. Nachweispflicht (Art. 5 Abs. 2 DS-GVO) kann Auswirkungen auf die Prozesse und Abläufe in den Unternehmen haben. Die verantwortliche Stelle muss nach Art. 5 Abs. 1 DS-GVO jederzeit nachweisen können, dass die Datenverarbeitung rechtmäßig erfolgt, etwa durch Einwilligungen mit den Klientenn. Die Verarbeitung darf nur für bestimmte und festgelegte Zwecke erfolgen, und erhoben werden dürfen dafür nur die notwendigen Daten. Darüber hinaus muss es Maßnahmen geben, damit unrichtige Daten unverzüglich berichtigt oder gelöscht werden.

Der Grundsatz der Rechenschaftspflicht wird durch die Regelung des Art. 24 Abs. 1 Satz 1 DS-GVO konkretisiert. Danach sind es in erster Linie „geeignete technische und organisatorische Maßnahmen", durch die sichergestellt werden soll, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt. Art. 24 DS-GVO bildet eine Generalklausel, die immer dann relevant wird, wenn die Verordnung keine spezielleren Normen enthält. Die Bedeutung dürfte erheblich sein, denn „geht irgendwo etwas schief", dürfte dies zumindest auf eine Verletzung von Art. 24 DS-GVO hindeuten (Schantz/Wolff, Das neue Datenschutzrecht, München 2017, Rdnr. 822).

Technik meint Maßnahmen, die sich automatisch vollziehen und insbesondere Programme oder Instrumente und Maschinen betreffen; hierzu gehören etwa Steuerung des Software- und des Hardwareprozesses der Verarbeitung, ebenso Verschlüsselungs- und Passwortsicherungen (Schantz/Wolff, a. a. O., Rdnr. 825). Organisatori-

sche Maßnahmen beziehen sich vor allem auf den äußeren Rahmen der Verarbeitung und betreffen den Ablauf sowie die Einbettung in Organisation und Personal, wozu etwa Zugriffs- und Zugangskontrollen, Aufsichtsstrukturen, Protokollierungspflichten gehören (Schantz/Wolff, a. a. O.).

Daten dürfen nicht mehr gespeichert bleiben, wenn sie nicht mehr benötigt werden. Für PB kann es von erheblicher juristischer Bedeutung sein, dass sie wegen der Strafbarkeitsandrohung in § 5 Heilpraktikergesetz nachweisen können, die Grenze zur Heilbehandlung nicht überschritten zu haben. Diese Grenzziehung kann auch für mögliche Schadensersatzansprüche der Klienten bzw. Rechtsnachfolger nach dem Tod von Bedeutung sein. Deshalb ist die Verjährung möglicher Ansprüche Maßstab für das Ende der Aufbewahrungsfrist. Es gilt die allgemeine Verjährungsfrist von drei Jahren (§ 195 BGB). Der Lauf der Frist beginnt allerdings erst nach Kenntnis der (möglichen) Ansprüche mit einer Kappungsgrenze von 10 Jahren (§ 199 Abs. 3 Satz 1 Nr. 1. BGB). Wer sichergehen will, speichert somit die Dokumentation nach dem Ende der Beratung max. 10 Jahre.

15. Datenlöschkonzept

Gespeicherte personenbezogene Daten müssen gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden. Frist hierfür enthält die DS-GVO nicht, sodass es für PB auf die Verjährung ankommt. Bitte vergleichen Sie hierzu im Einzelnen Nr. 14. Rechenschaftspflicht/Löschen und Vernichten von Daten.

Die DS-GVO definiert nicht den Vorgang des Löschens. In Art. 4 Nr. 2. DS-GVO werden das **Löschen** und die Vernichtung in einem Zuge als unterschiedliche Elemente der Verarbeitung erwähnt („das Löschen oder die Vernichtung“). Hieraus kann jedenfalls entnommen werden, dass es sich um zwei unterschiedliche Tatbestände handeln muss, die Vernichtung jedenfalls also nicht zwingend erforderlich ist, um den Tatbestand des Löschens zu erfüllen. Das Löschen ist mithin ein Minus zur Vernichtung. Für das Löschen reicht es aus, die Daten für den gewöhnlichen Gebrauch unbenutzbar zu machen (Auernhammer – Stollhoff, DS-GVO, BDSG, 6. Auflage Köln 2018, Rdnr. 9).

Jegliche Art der Unkenntlichmachung soll danach erfasst sein. Vorausgesetzt, die Daten sind unlesbar geworden bzw. stehen nicht mehr zur Verfügung. Eine Löschung auf allen verfügbaren Datenträgern und eine Löschung sämtlicher Zwischen- und Sicherheitskopien sind hierfür nicht erforderlich; auch muss der Löscherfolg nicht strikt irreversibel sein; es genügt die technische Löschung von elektronischen Daten (Auernhammer – Stollhoff, a. a. O., Rdnr. 9 mit weiteren Hinweisen).

Die **Vernichtung** der personenbezogenen Daten in Beratungsdokumentationen bedeutet dann z. B. die Zerstörung der Festplatte, idealerweise wenn die Datensicherung auf einer externen Festplatte erfolgt. Hier kann durch zeitlich gestaffelte Verwendung von externen Festplatten, z. B. in einem 10-Jahres-Zeitraum, eine praktikable Organisation ohne großen Aufwand erfolgen.

Es existieren vielfältige Empfehlungen für die Erstellung eines Löschkonzepts. Analysiert man diese, lässt sich feststellen, dass eine weitgehende Übereinstimmung mit dem Verarbeitungsverzeichnis besteht. Eine praktikable Handhabung ist deshalb die Erweiterung des Verarbeitungsverzeichnisses (**Anlage 2**) um ein Löschkonzept, wie zuvor beschrieben.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Für PB ist es zweckmäßig, lediglich das Verarbeitungsverzeichnis um eine Spalte „Löschkonzept“ zu erweitern, wobei sich aufgrund der maximalen 10-Jahres-Frist für Löschung oder Vernichtung bei Dokumentationen der Aufwand in Grenzen halten dürfte. Andere personenbezogene Daten müssen nach Ablauf der kurzen Verjährungsfristen (z. B. aus Arbeitsrecht oder Mietrecht) nach Ablauf dieser verhältnismäßig kurzen Fristen gelöscht oder vernichtet werden. Hier kann sicherlich für viele PB die Lösung darin liegen, die Daten nicht elektronisch zu verarbeiten. Beispiel: Ein gespeicherter Basisarbeitsvertrag wird im Rechner für die Einstellung einer neuen Mitarbeiterin angepasst. Der Vertrag wird ohnehin ausgedruckt und persönlich unterzeichnet. Werden im Rechner die Daten des Arbeitsvertrages sofort gelöscht, ergibt sich keine Lösch- oder Vernichtungsfrist nach einem Löschkonzept.

16. Abschluss eines Vertrages über Auftragsdatenverarbeitung mit Steuerberatern

Eine explizite gesetzliche Regelung über Auftragsdatenverarbeitung und Dienstleistungen von Steuerberatern fehlt, weshalb Art. 28 DS-GVO ausgelegt werden muss. Ob die Dienstleistungen eines Steuerberaters Auftragsverarbeitung sind oder nicht, wird unterschiedlich beurteilt, teilweise wird nach den Aufträgen differenziert. Die Bundessteuerberaterkammer als Körperschaft des öffentlichen Rechts und offensichtlich auch alle Landessteuerberaterkammern vertreten ebenso wie das Bundesfinanzministerium und das Bundesinnenministerium die Auffassung, die Dienstleistungen eines Steuerberaters seien **keine Auftragsdatenverarbeitung**, weshalb ein entsprechender Vertrag nach Art. 28 Abs. 3 DS-GVO nicht abgeschlossen werden müsse.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:

Solange die Auslegungen der Bundesministerien und der Steuerberaterkammern Bestand haben, brauchen PB nicht auf den Abschluss eines Auftragsverarbeitungsvertrages zu bestehen, selbst wenn die Datenschutzbehörde/Datenschutzbeauftragten des jeweiligen Bundeslandes eine andere Rechtsauffassung vertreten sollten. In einem theoretisch fernliegenden Ordnungswidrigkeitenverfahren wären sie auf jeden Fall durch die Rechtsauffassungen der Bundesministerien und Steuerberaterkammern exkulpiert. Will ein Steuerberater einen Auftragsdatenverarbeitungsvertrag abschließen, ist zu raten, ihn routinemäßig anhand der Vorgaben von Art. 28 Abs. 3 DS-GVO zu prüfen und zu unterzeichnen. Im Übrigen sei angemerkt, dass die inhaltlichen Vorgaben für einen Auftragsverarbeitungsvertrag in Art. 28 Abs. 3 DS-GVO bei sachlicher, distanzierter Betrachtung an und für sich lediglich Punkte enthalten, die im Umgang mit sensiblen, besonders schutzwürdigen personenbezogenen Daten selbstverständlich sein sollten.

17. Bußgelder / persönliche Risikobewertung

Der Bußgeldrahmen bei Verstößen gegen die Rechenschaftspflicht endet bei 20.000.000,-- € (Art. 83 Abs. 5 DS-GVO). Der gleiche Bußgeldrahmen kommt auch zur Anwendung bei Verstößen gegen die Betroffenenrechte (Informationspflicht, Auskunftsrecht, Recht auf Berichtigung und Löschung).

Art. 83 Abs. 2 DS-GVO enthält Kriterien, nach denen in jedem Einzelfall die Höhe eines Bußgeldes zu bilden ist. Der maximale Rahmen von 20 Mio. € ist festgelegt worden, weil die DS-GVO auch zur Anwendung kommt im Datenschutz international agierender Konzerne. Welcher Bußgeldrahmen für PB bei Verletzungen relevant wird, ist offen. Möglicherweise wird sich ein „Bußgeldkatalog" der Aufsichtsbehörden herausbilden. Jedenfalls ist nach Sinn und Zweck von Art. 83 DS-GVO davon auszugehen, dass auch gegen PB relativ hohe Bußgelder festgesetzt werden können. Wie die Verwaltungspraxis mit der Einleitung von Bußgeldverfahren, deren Handhabung und der Verhängung von Bußgeldern letztlich aussieht, ist völlig offen.

Aufsichtsbehörden werden nicht von sich aus tätig, sondern nach Anzeige, beispielsweise von einem Klienten, der meint, in dem Unternehmen des PB werde der Datenschutz verletzt. In dem Fall müssen dann gegenüber der Behörde Nachweise über die Einhaltung des Datenschutzes erfolgen.

Aus der Beratungspraxis des Anwaltsbüros für VFP-Mitglieder:
Das neue Datenschutzrecht ist kompliziert, und es mangelt manchmal an der notwendigen Transparenz. Mit Hilfe dieses oder eines anderen Wegweisers sollten PB prüfen, welche Punkte auf ihren Betrieb zutreffen, und rechtzeitig agieren. Die Verwendung der VFP-Musterformulare – individuell dem eigenen Unternehmen angepasst – ist unbedingt zu empfehlen.

Klar ist, dass zur eigenen Absicherung im Datenschutz einiges unternommen werden muss. Zweckmäßig ist eine **individuelle Risikobewertung**, bei der unterschieden werden sollte:

- Welche Einhaltung von Datenschutzbestimmungen kann von außen mehr oder weniger einfach kontrolliert werden?

  Hierzu gehört die Website, weshalb besonders auf eine korrekte und umfassende Datenschutzerklärung Wert gelegt werden sollte. Im Zweifel sollte zur eigenen Absicherung hier eher mehr als weniger getan werden.

- Welche Nachweise müssen ggf. in einer – eher unwahrscheinlichen – zivilrechtlichen Auseinandersetzung mit einem Klienten oder in der Auseinandersetzung mit einer Aufsichtsbehörde erfolgen?

  Hier handelt es sich fast ausschließlich um interne Festlegungen, Pläne usw., die im Konfliktfall vorzulegen sind und zuvor noch aktualisiert werden können.

Rechtsstand Januar 2019.

Dr. jur. Frank A. Stebner
Rechtsanwalt
Fachanwalt für Medizinrecht

Anlagen:

1. Checkliste „Technische und organisatorische Maßnahmen der Datensicherheit“
2. Verzeichnis von Verarbeitungstätigkeiten
3. Ausfüllhinweise zum „Verzeichnis von Verarbeitungstätigkeiten“
4. Datenschutzinformation und Erklärung zur Einwilligung in die Datenverarbeitung
5. Datenschutzinformation und Erklärung zur Einwilligung (1) in die Organisationsgemeinschaft und (2) in die Datenverarbeitung
6. Datenschutzerklärung
   (Grundmuster einer Datenschutzerklärung für die Website)
7. Ergänzung des Impressums
8. Auskunftserteilung an Klienten