

**Die neue Datenschutzgrundverordnung
im Betreuungsbüro**

**Musterverzeichnisse und Formblätter
gegen Abmahnmissbrauch**



von

Martin Weber

www.beck-fernkurse.de



1. Auflage



Verlag C.H. Beck im Internet:
www.beck.de

www.beck-fernurse.de/berufsbetreuertage

© 2018/2019 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München

Druck: Druckhaus Nomos
In den Lissen 12, 76547 Sinzheim

Satz: PhotoSatz Pfeifer, Krailling

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)



Über den Autor:

Martin Weber ist als Rechtsanwalt, zertifizierter Testamentsvollstrecker und Verfahrenspfleger mit eigener Kanzlei in Passau tätig. Er publiziert regelmäßig zu aktuellen Fragen des Familien- und Betreuungsrechts sowie über Fristen, Verjährung und Datenschutz.



Inhaltsverzeichnis

Abkürzungsverzeichnis	8
Vorwort	10
I. Geltendes Datenschutzrecht	12
II. Wesentliche Grundsätze	12
1. Grundsatz der Datenminimierung	13
2. Integrität und Vertraulichkeit	14
3. Betroffenenrechte	14
III. Relevante Neuerungen	14
1. Einwilligungserfordernisse	14
2. Verarbeitungsverzeichnis	16
3. Informationspflichten, Art. 13, 14 DS-GVO	16
4. IT-Sicherheit, Art. 32 DS-GVO	18
5. Datenschutzbeauftragter, Art. 37 DS-GVO	19
6. Zwischenfazit	20
IV. Sozialdatenschutz	20
Rechtssicheres Muster-Verarbeitungsverzeichnis (Art. 30 DS-GVO)	22
Rechtssichere Muster-Erhebung personenbezogener Daten (Art. 13 f. DS-GVO)	31
Suchwortregister	34



Abkürzungsverzeichnis

Abs.	Absatz
a.F.	alte Fassung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BVfB	Bundesverband freier Berufsbetreuer e.V.
BdB	Bundesverband der Berufsbetreuer/innen e.V.
DGSVO	Datenschutzgrundverordnung
f.	Folgende
ff.	Fortfolgende
GG	Grundgesetz
Ggf.	gegebenenfalls
GRCH	Grundrechtecharta
EMRK	Europäische Menschenrechtskonvention
lit.	littera (Buchstabe)
i.S.d.	im Sinne des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
SGB	Sozialgesetzbuch
TOM	Technisch-organisatorische Maßnahme





Vorwort

Datenschutz hat Hochkonjunktur! Spätestens seit Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) am 25.05.2018 ist die Sicherheit personenbezogener Daten in aller Munde. Vor wenigen Jahren war dies eher zum juristischen Nischengebiet, als zum Gegenstand öffentlichen Diskurses verkommen. Das kollektive Interesse an einer zuletzt wieder recht stiefmütterlich behandelten Rechtsmaterie rührt aber nicht primär aus dem gesellschaftlich gewachsenen Bedürfnis nach Datensicherheit oder gar einem generell gewandelten Bild vom Datenschutz her. Vielmehr haben vorrangig die drakonischen Strafen für Verstöße gegen die weithin gänzlich unspezifisch gefassten Bestimmungen – die faktisch jeden treffen können – für blanke Panik und (in der Folge) zu einer erzwungenen Befassung mit der DS-GVO geführt.

Insofern sind auch Sie als Berufsbetreuer(in) gehalten, sich mit einem der schlechtesten – da überzogenen und in seinem Aussagegehalt vagen bis ambivalenten – Gesetz jüngster Zeit zu befassen. Die Europäische Kommission, das Europäische Parlament und der Europäische Rat haben uns damit beglückt und bedauerlicherweise das bisherige, sehr durchdachte nationale Datenschutzrecht zu Makulatur verkommen lassen.

Die weithin schwammig gefasste DS-GVO – die der Münsteraner Informationsrechtsprofessor Thomas Hoeren als „hirnlos“ und „eines der schlechtesten Gesetze des 21. Jahrhunderts“ charakterisiert hat – schafft erhebliche Rechtsunsicherheiten. Diese können wohl erst in den kommenden Jahren in mühseliger Kleinarbeit durch die Rechtspraxis und die Rechtsprechung ausgemerzt werden. Die Entwicklungslinien sind hier allenfalls grob prognostizierbar.

Rosig klingt dies alles nicht – doch trösten Sie sich: Wenn Sie einige einfache Grundregeln beachten, minimieren Sie Ihr Risiko, in Konflikt mit der DS-GVO und insbesondere mit den über ihre Einhaltung wachenden Behörden zu geraten, ganz erheblich. Diese Grundregeln gibt Ihnen dieser Ratgeber an die Hand.

Bedenken Sie auch immer: Als Berufsbetreuer(in) stehen Sie – anders etwa als multinationale Unternehmen – nicht vorrangig im Fokus der personell weithin unterbesetzten und überlasteten Datenschutzbehörden, die über die Einhaltung der DS-GVO wachen. Auch die Gefahr einer **Abmahnung** ist – wenn Sie sich an einige grundsätzliche Aspekte halten, die im Folgenden dargestellt sind, gering.

Die nachfolgenden Ausführungen geben Ihnen zunächst einen Überblick über die Rechtsgrundlagen des seit 25.05.2018 geltenden Datenschutzrechts (I.), dessen wesentliche Grundsätze (II.) sowie die besonders relevanten Neuerungen im allgemeinen Datenschutz (II.) und beim Sozialdatenschutz (III.).

Ihr

Martin Weber



I. Geltendes Datenschutzrecht

Am 25. Mai 2018 ist die sog. **Datenschutzgrundverordnung (DS-GVO)** in Kraft getreten, Art. 99 DS-GVO. Es handelt sich dabei um einen Rechtsakt der Europäischen Union, der in sämtlichen Mitgliedsstaaten – und damit auch in Deutschland – unmittelbar Anwendung findet, ohne dass es eines weiteren Umsetzungsaktes oder gar der Umwandlung in nationales Recht bedürfte, Art. 288 Abs. 2 AEUV. Die DS-GVO ist damit in der Bundesrepublik Deutschland direkt geltendes Datenschutzrecht und tritt gleichsam an die Stelle des bisherigen Bundesdatenschutzgesetzes (BDSG) in Form der Bekanntmachung vom 14.01.2003.

Der Bundesgesetzgeber hat am 30.07.2017 die **Neufassung des BDSG** beschlossen, die am 25. Mai 2018 – also zeitgleich mit der DS-GVO – in Kraft getreten ist. Darin finden sich nunmehr Bestimmungen, welche die DS-GVO ergänzen, präzisieren oder auch von dieser abweichen. Die DS-GVO bewirkt insofern keine „Vollharmonisierung“ im Sinne starrer Standards, sondern schafft in gewissem Rahmen Spielräume für nationale Modifikationen, die der Bundesgesetzgeber mit dem BDSG geschaffen hat.

Merke: Begnügen Sie sich also bei datenschutzrechtlichen Fragestellungen nicht mit dem Blick allein in die DS-GVO. Diese ist zwar zunächst Ihr Ausgangspunkt. Gehen Sie aber in einem zweiten Schritt stets der Frage nach, ob ggf. das neue BDSG Abweichungen der Modifikationen beinhaltet.

Die Regelungen zum **Sozialdatenschutz nach SGB X** gelten auch seit Inkrafttreten der DS-GVO fort. Diese wurden allerdings mit Gesetz vom 17.07.2018 – in Kraft getreten am 25. Mai 2018 – neu gefasst und an den relevanten Stellen in Einklang mit der DS-GVO gebracht.

II. Wesentliche Grundsätze

Das **bisherige nationale Datenschutzrecht** war verfassungsrechtlich insbesondere durch das vom Bundesverfassungsgericht geprägte **Recht des Einzelnen auf informationelle Selbstbestimmung** bestimmt. Dieser aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG) entwickelter Aspekt betonte die Datenhoheit der Person und den Schutz vor widerrechtlicher Preisgabe und Verwendung sensibler Daten. Erhebung und Verarbeitung unterlagen danach einer strengen, vorab bestimmten Zweckbindung. Aus dem Bestimmtheitsgrundsatz folgte die Transparenz der Erhebung. Allgemeine Verhältnismäßigkeitserwägung und das generelle **Einwilligungserfordernis** in Folge der Datenhoheit sind ebenfalls relevante Faktoren.

Die **DS-GVO** als supranationaler Rechtsakt dagegen muss sich an internationalen Vorgaben – speziell dem Recht auf **Privatheit des Einzelnen aus Art. 8 GRCH** und **Art. 8 Abs. 1 EMRK** messen lassen. Aus diesen werden gemeinhin ähnliche Vorgaben wie aus dem Recht informationeller Selbstbestimmung gelesen (Zweckbindung; Verhältnismäßigkeit;

Transparenz; Einwilligung). Allerdings hat der europäische Gesetzgeber teils ein anderes Verständnis von diesen Begriffen – wenn auch oftmals nur nuanciert, im Ergebnis aber doch erheblich.

Die Datenschutzgrundverordnung ist als europäischer Rechtsakt **autonom auszulegen**. Insofern kann sie nicht nach deutschrechtlichen Standards gelesen und angewandt werden. Vielmehr sind die Begrifflichkeiten unionsrechtlich geprägt und insofern entsprechend zu interpretieren und anzuwenden.

Die DS-GVO kennt – wie das bisherige nationale Datenschutzrecht – die Grundsätze des Verbotes mit Erlaubnisvorbehalt, des Einwilligungsvorbehalts, der Zweckbindung sowie der Transparenz – wenn auch mit teils anderen Abstufungen.

Wesentliche Änderungen haben sich aber insbesondere im Bereich folgender Grundsätze ergeben:

1. Grundsatz der Datenminimierung

Art. 5 Abs. 1 lit. c. DS-GVO normiert den Grundsatz der Datenminimierung. Dieser geht wesentlich über den Grundsatz der Datensparsamkeit, der dem bisherigen Bundesdatenschutzgesetz zu Grunde lag (§ 3a BDSG a.F.), hinaus. Generellen Verhältnismäßigkeitserwägungen werden nunmehr bei der Datenverarbeitung besonderes Gewicht beigemessen, dies insbesondere auf Ebene der Erforderlichkeit und Angemessenheit.

Zwei Aspekte stechen dabei besonders heraus:

- Art, Umfang und Dauer der Verarbeitung durch Technikgestaltung zu begrenzen (**privacy by design**, Art. 25 Abs. 1 DS-GVO).
- Datenschutzkonforme Voreinstellungen sind zwingend (**privacy by default**, Art. 25 Abs. 2 DS-GVO).

Ausfluss bzw. unmittelbare Folge des Grundsatzes der Datenminimierung sind auch der **Grundsatz der Datenrichtigkeit** aus Art. 5 Abs. 1 lit. d. DS-GVO, der die unverzügliche Löschung oder Berichtigung unrichtiger Daten gebietet.

Weiterhin in unmittelbarem Zusammenhang zum Grundsatz der Datenminimierung steht der **Grundsatz der Speicherbegrenzung**, Art 5 Abs. 1 lit. e DS-GVO. Dies erfordert die regelmäßige Überprüfung, ob in zeitlicher Hinsicht ein weiterer Vorhalt personenbezogener Daten noch erforderlich ist.

2. Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit der Datenverarbeitung, Art. 5 Abs. 1 lit. f. DS-GVO erfordert eine Reihe von **Maßnahmen zur Gewährleistung der Datensicherheit** nach Art. 32 DS-GVO, insbesondere Verschlüsselungsstandards. Die Anforderungen sind wesentlich detaillierter als die in § 9 BDSG a.F. geregelten Vorgaben und gehen mutmaßlich deutlich über diese hinaus.

3. Betroffenenrechte

Die DS-GVO stärkt in ihren Art. 12 ff. die Rechte Betroffener in Gestalt umfassender **Informations-, Auskunfts-, Berichtigungs- und Löschungsrechten**. Beachtlich sind insbesondere die umfassenden Informationspflichten, wo zuvor nur Auskunftsrechte auf Verlangen bestanden (§§ 6, 19, 34 BDSG). Weiterhin geht das nunmehrige Recht auf Löschung (Art. 17 DS-GVO) mit Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofes zum **Recht auf Vergessenwerden** deutlich über die bisherige Regelung hinaus.

III. Relevante Neuerungen

Nachfolgend werden schlaglichtartig die für Sie als Berufsbetreuer/in besonders relevanten Neuerungen behandelt. Dabei wird die Auftragsdatenverarbeitung – die Sie regelmäßig **nicht betrifft** – ausgeklammert.

1. Einwilligungserfordernisse

Grundsätzlich besteht für die Verarbeitung personenbezogener Daten ein **Verbot mit Erlaubnisvorbehalt**. Dies bedeutet, dass die Verarbeitung von Daten solange und soweit illegitim ist, als kein gesetzlicher Rechtfertigungsgrund oder eine Einwilligung der betroffenen Person als Erlaubnis eingreifen.

Die Anforderungen an die Einwilligung werden in Art. 7 DS-GVO sowie in „Erwägungsgrund 32 zur DS-GVO“¹ dargestellt. Danach handelt es sich bei der Einwilligung um eine formfreie, freiwillige, jederzeit widerrufbare, auf einen konkreten Verarbeitungsfall bezogene, unmissverständliche, das Einverständnis mit der in Rede stehenden Verarbeitung bekundende Handlung, welche die betroffene Person ausreichend informiert abgegeben haben muss.

¹ Die Erwägungsgründe der Datenschutzgrundverordnung sind Ziele, die mit der Formulierung der Artikel dieser EU-Verordnung verfolgt wurden. Sie sind nicht die eigentlichen Rechtsnormen, aber sie sind hilfreich für die Interpretation der Rechtsnormen.

Insofern muss der Betroffene vor Einwilligungserteilung entsprechend der Art. 13 f. DS-GVO informiert worden sein.

Zunächst stellt sich für Sie als Berufsbetreuer/in die Frage, ob Sie von Ihrem Betreuten eine Einwilligung in die Verarbeitung (Erhebung, Speicherung, Weiterleitung, etc.) seiner personenbezogenen Daten benötigen. Dies ist nicht der Fall, soweit die **Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich** ist, der Sie unterliegen, Art. 6 Abs. 1 lit. c. DS-GVO.

Der Bundesverband der Berufsbetreuer (BdB e.V.) sieht – auf Nachfrage beim Landesbeauftragten für Datenschutz Bremen – diejenigen Verarbeitungstätigkeiten, die **im Rahmen der Ihnen zugewiesenen Aufgabenkreise** erforderlich sind, als Erfüllung Ihrer Pflichten als rechtlicher Betreuer an. Insofern ist eine **Einwilligung nicht erforderlich**. Beachten Sie aber – dem Grundsatz der Datenminimierung entsprechend – keine Daten zu erheben oder zu verarbeiten, die zu Ihrem **Aufgabenkreis keinen Bezug** haben oder für die Erfüllung Ihrer Tätigkeiten im zugewiesenen Aufgabenkreis schlechthin unnötig sind. Insofern wird man aber einen **großzügigen Maßstab** anlegen müssen, um Sie bei der Erfüllung Ihrer Aufgaben nicht vollends zu blockieren. Eine nicht von Art. 6 Abs. 1 lit. c. DS-GVO gedeckte Verarbeitung läge etwa vor, wenn Sie allein mit dem Aufgabenkreis Vermögenssorge betraut sind und ohne Anlass ärztliche Atteste Ihres Betreuten einholen.

Hier käme noch erschwerend hinzu, dass Gesundheitsdaten – wie auch Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person – **besondere Kategorien personenbezogener Daten** i.S.v. Art. 9 Abs. 1 DS-GVO darstellen. Deren Verarbeitung muss den Anforderungen des Art. 9 Abs. 2 DS-GVO genügen. Hier sieht der BdB e.V. ebenfalls eine **Einwilligung** im Lichte des Art. 9 Abs. 2 lit. b DS-GVO **nicht für erforderlich** an, wenn und soweit Sie die Daten in Erfüllung des durch Ihre Aufgabenkreise übertragenen Aufgaben wahrnehmen. Zwar ist die Anwendung dieser Norm – die von der Ausübung von Rechten im Rahmen des Sozialschutzes spricht – insgesamt dem Wortlaut nach eher zweifelhaft, aber pragmatisch sicherlich richtig.

Dennoch sollten Sie mit Blick auf die bestehenden **Unsicherheiten** die genannten besonderen Kategorien von Daten **sehr restriktiv** erheben und **im Zweifel** die **Einwilligung Ihres Betreuten schriftlich einholen**.

Fazit:

Erhebliche Veränderungen zur bisherigen Rechtslage sind insofern – vorbehaltlich anderweitiger Rechtsprechung – vorläufig nicht zu ersehen. Eine **Einwilligung** ist grundsätzlich – im Rahmen der Tätigkeit in Ihren Aufgabenkreisen – **nicht erforderlich**.

2. Verarbeitungsverzeichnis

Art. 30 DS-GVO verpflichtet Sie zur **Führung eines Verarbeitungsverzeichnisses**. In diesem müssen Sie Ihre Datenverarbeitungsvorgänge umfassend darstellen; die in Art. 30 DS-GVO genannten Pflichtangaben sind aufzunehmen. Dies sind:

- Name und Kontaktdaten des Verantwortlichen,
- Name und Kontaktdaten des Datenschutzbeauftragten, sofern vorhanden,
- Verarbeitungszwecke, insbesondere 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,
- Beschreibung der Kategorien betroffener Personen (in der Regel Klienten, ggf. Beschäftigte u.a.),
- Beschreibung der betroffenen Datenkategorien (Adressdaten, Bankdaten, Steuerdaten, Gesundheitsdaten, etc.),
- Kategorien von Datenempfängern (Behörden, Gerichte, Arbeitgeber, etc.),
- Lösungsfristen.

Ein rechtssicheres **Muster-Verarbeitungsverzeichnis** finden Sie auf Seite 23 in diesem Rechtsratgeber.

Entsprechende inhaltsgleiche Pflichten bestanden bisher weithin schon nach §§ 4e, 4f BDSG a.F. (Verfahrensverzeichnis). Das zu erstellende Verarbeitungsverzeichnis ist **nicht öffentlich**. Sie sind aber nach Art. 30 Abs. 4 DS-GVO gehalten, das Verzeichnis der Aufsichtsbehörde – sollte diese das Verzeichnis bei Ihnen anfordern – zur Verfügung zu stellen. Anlassunabhängige Stichproben sind mit Blick auf die derzeitige Arbeitsüberlastung der Aufsichtsbehörden eher nicht zu erwarten. Eine Herausgabe an Klienten und Dritte ist nicht vorgesehen.

3. Informationspflichten, Art. 13, 14 DS-GVO

Kaum praktisch handhabbar sind die Vorgaben zur **Information betroffener Personen über die Verarbeitung personenbezogener Daten**. Art. 13 DS-GVO regelt dabei Fälle, in denen die Daten beim Betroffenen erhoben werden. Art. 14 DS-GVO regelt dagegen Fälle, in denen Daten des Betroffenen bei Dritten erhoben werden. Eine solche Informationspflicht im Sinne einer umfassenden Belehrung ohne Aufforderung kannte das bisherige Recht nicht.

Zunächst ist ohnehin **fraglich, ob die Art. 13 f. DS-GVO auf den rechtlichen Betreuer überhaupt angewendet werden können**. Denn ein Berufsbetreuer fungiert als gesetzlicher Vertreter der betreuten Person. Insofern scheint Art. 13 DS-GVO schon nicht einschlägig, da ansonsten von einem „Erheben“ von Daten der betreuten Person gegenüber sich selbst durch den rechtlichen Betreuer auszugehen wäre, was widersinnig erscheint. Aus denselben Erwägungen ist auch Art. 14 DS-GVO unanwendbar, da ein Berufsbetreuer in seinem Aufgabenkreis als gesetzlicher Vertreter Informations- und Auskunftsrechte der betreuten Person gegenüber Dritten geltend machen kann und insofern ebenfalls nicht von einem „Erheben“ im Rechtssinne auszugehen ist.

Meines Erachtens sprechen überdies gute Gründe dafür, **von der Information** des Betreuten mit der Begründung **abzusehen**, dass er bereits über die relevanten Informationen verfügt, selbst wenn man von einer Anwendbarkeit der Art. 13 Abs. 1 bzw. Art. 14 Abs. 1 DS-GVO ausgeht. Schließlich weiß Ihr Betreuer über die Betreuerbestellung, den Aufgabenbereich und damit auch die wesentlichen Tätigkeiten von Ihnen Bescheid. Er weiß damit von Ihnen als verantwortliche Person und verfügt über Ihre Kontaktdaten, weiß um die Zwecke der Verarbeitung, die betroffenen Datenkategorien und auch die potentiellen Empfänger (zumindest in laienhafter Wertung).

Eine Anwendung von Art. 13 Abs. 4 DS-GVO bzw. Art. 14 Abs. 5 lit. a DS-GVO, wonach eine Informationspflicht nicht besteht, wenn der Betroffene bereits über die Information verfügt, ließe sich also argumentieren.

Dies mag zwar pragmatisch sein, ist so rechtlich allerdings bislang nicht abgesichert. Hier wäre sinnvoll – etwa seitens des BdB e.V. – Auskunft bei den Datenschutzbehörden einzuholen. Auch §§ 32, 33 BDSG enthalten keine Regelungen, welche die **Informationspflicht gegenüber Ihrem Betreuten entfallen ließen**. Insofern wäre auch der nationale Gesetzgeber gefordert, hier Klarheit zu schaffen.

Ungeklärt ist auch die Frage, ob nicht ggf. das Gericht, das Sie als rechtlichen Betreuer bestellt, in der Pflicht ist, die betroffene Person umfassend nach Art. 13 f. DS-GVO zu informieren, was für Sie aber nicht weiter relevant ist.

Bis hierzu **Rechtsklarheit** besteht ist es am sichersten, wenn Sie sich – ggf. auch für Ihre einzelnen Aufgabenbereiche – **eigene Formblätter fertigen**. Diese sollten Angaben zu den Pflichtinformationen nach Art. 13 Abs. 1, 14 Abs. 1 DS-GVO enthalten, die Sie auch Ihrem Betreuten zukommen lassen könnten.

Nutzen Sie hierfür unser **rechtssicheres Muster-Formblatt** auf Seite 30 dieses Rechtsratgebers, das Sie auf Ihre verschiedenen Betreuten anpassen können.

In Ihrem **Formblatt** muss enthalten sein:

- Ihr Name und Ihre Kontaktdaten als verantwortliche Stelle

- Zweck, zu dem die Daten verarbeitet werden sollen und Rechtsgrundlagen (rechtliche Betreuung nach §§ 1896 ff. BGB)
- Betroffene Datenkategorien (Kontaktdaten, Gesundheitsdaten, etc.)
- Empfänger der Daten, wenn Weitergabe avisiert (Behörden, Gerichte, Arbeitgeber, etc.)
- Hinweis auf Dauer der Speicherung und Kriterien für die Löschung
- Hinweis auf Auskunfts-, Berichtigungs- und Löschungsrecht (Art. 15 ff. DS-GVO)
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde

4. IT-Sicherheit, Art. 32 DS-GVO

Weiterhin ist zur Sicherung datenschutzrechtlicher Standards die Einhaltung der sog. technisch-organisatorischer Maßnahmen (TOM) erforderlich, die sich am Stand der Technik zu orientieren haben.

Die konkret anzuwendenden Maßnahmen müssen immer in einer **vernünftigen Kostenrelation** stehen und haben auch den **Zweck und die Hintergründe der Verarbeitung gebührend zu berücksichtigen**.

Als Berufsbetreuer verarbeiten Sie Daten fremdnützig im Interesse Ihres Betreuten im Rahmen eines Ihnen staatlicherseits übertragenen Amtes. Sofern Sie als „Einzelkämpfer“ (oder zusammen mit wenigen Mitarbeitern) tätig sind versteht es sich von selbst, dass an Sie nicht dieselben Maßstäbe wie etwa an ein mittelständisches Unternehmen mit einigen Dutzend Mitarbeitern, das die Daten zudem eigennützig für wirtschaftliche Zwecke verwendet, gestellt werden können.

Zu den TOM zählt zunächst die **Zugangskontrolle** zu Daten. Hierunter fallen insbesondere folgende Maßnahmen:

- **Passwortgeschützter Zugang zu IT-Systemen** (PC, Laptop, etc.). Hier genügt regelmäßig ein Passwort mit mindestens acht Zeichen, wobei mindestens ein Sonderzeichen, ein Groß- und Kleinbuchstabe sowie eine Zahl enthalten sein sollen.
- Gegebenenfalls **Alarmanlagen** und **Sicherheitsschlösser** ; für Sie als Berufsbetreuer sind hier keine überzogenen Anforderungen zu stellen. Es genügt regelmäßig, wenn Sie sämtliche Dokumente, die personenbezogene Daten enthalten, in den herkömmlichen, abschließbaren **Aktenschränken** – die idealerweise feuerfest sein sollten – lagern. Ihr Büro sollte abschließbar sein und auch abgeschlossen werden, wenn Sie sich nicht darin aufhalten, egal, ob es sich um ein Zimmer Ihrer Wohnung/Ihres Hauses oder eine selbstständige Einheit handelt. Besondere Anforderun-

gen an die Schließanlage sind nicht zu stellen; ein handelsübliches Schloss ist ausreichend.

Zentral ist weiter etwa die **Verschlüsselung von Daten**. Die Anforderungen sind insgesamt vielfältig:

- Für Ihren **Email-Account** sollten Sie die Einstellung STARTTLS oder Perfect Forward Secrecy verwenden, um eine durchgängige Verschlüsselung zu gewährleisten.
- Nutzen Sie etwa ein **WLAN-Netzwerk** in Ihrem Betreuungsbüro, ist eine Verschlüsselung desselben mit WPA 2 und einem 20-stelligen Passwort sicherlich hinreichend.
- Wenn Sie **mobile Geräte** (Handy, Tablet, Laptop) nutzen, auf denen sich personenbezogene Daten Ihrer Klienten befinden, sind diese ebenfalls zu sichern. Das Bundesamt für Informationstechnik (BSI) empfiehlt hier das Produkt VeraCrypt. Ob eine bloße Pincode-Sperre ausreichend ist, ist ungeklärt.
- Betreiben Sie eine **eigene Website**, bei der personenbezogene Daten verarbeitet werden (etwa durch Kontaktformulare), so sollten Sie eine HTTPS-Verschlüsselung anwenden.

Weiterhin müssen Sie – im zumutbaren Umfange – die Integrität Ihres IT-Systems sicherstellen. Hierzu gehört etwa die Anwendung von **Virenscannern** oder anderen Intrusion-Detection-Systemen. Weiterhin empfiehlt sich die regelmäßige Fertigung von **back-ups** (etwa auf Datenträgern), um Datenverlust vorzubeugen. Um die **Löschung von Daten** effektiv durchzusetzen, empfiehlt sich der Einsatz spezieller Software. Diese überschreibt den durch die „Löschung“ freigewordenen Speicherplatz mehrfach und beugt einer Wiederherstellung der Daten vor.

Zu nennen ist letztlich noch die **Zugangskontrolle zu Daten** – insbesondere, wenn Sie Mitarbeiter beschäftigen. Hier sind die Vergabe individueller Passwörter, die regelmäßige Prüfung von Berechtigungen sowie die Sperrung ausgeschiedener Mitarbeiter extrem wichtig.

Beachten Sie, dass die konkreten TOM grob im Verarbeitungsverzeichnis nach Art. 30 DSGVO darzustellen und zu umreißen sind. Ein (ausführliches) **Muster** – welches auf Ihre konkrete Situation anzupassen ist – finden Sie auf Seite 23 dieses Rechtsratgebers.

5. **Datenschutzbeauftragter, Art. 37 DS-GVO**

Ein **Datenschutzbeauftragter ist im Betreuungsbüro regelmäßig nicht erforderlich**, sofern nicht regelmäßig mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten befasst sind, § 38 Abs. 1 Satz 1 BDSG. Davon ist mit Blick auf die durchschnittliche Mitarbeiterzahl im Betreuungsbüro nicht auszugehen.

Ein **Bestellungserfordernis nach Art. 37 Abs. 1 lit. c. DS-GVO ergibt sich regelmäßig nicht**. Nach dieser Norm ist ein Datenschutzbeauftragter etwa zu bestellen, wenn umfas-

send besondere Datenkategorien nach Art. 9 DS-GVO verarbeitet werden. Hiervon ist bei nach hier vertretener Ansicht einem Betreuungsbüro – selbst wenn im Rahmen der Gesundheitsvorsorge weithin Gesundheitsdaten verarbeitet werden – regelmäßig nicht auszugehen, da hierin nicht die Kerntätigkeit liegt. Dementsprechend geht auch die Mehrzahl der Mitglieder der Arbeitsgruppe zum Datenschutz des Bundesverbandes freier Berufsbetreuer e.V. (BVfB) nicht von einem Bestellungserfordernis aus.

6. Zwischenfazit

Die DS-GVO schafft erhebliche Rechtsunsicherheiten. Eine Klärung durch die Rechtsprechung bzw. den europäischen oder nationalen Gesetzgeber ist dringend geboten.

Im Moment kann vielfach nur gemutmaßt werden, welche konkreten Maßnahmen die DS-GVO nun vom Rechtsanwender erfordert. Dementsprechende Unsicherheit herrscht durchgängig bei sämtlichen Verpflichteten – insbesondere auch öffentlichen Stellen wie den Finanzämtern.

Prognostisch steht zunächst nicht zu erwarten, dass die deutschen Datenschutzbehörden – die zudem wesentlich durch die jahrelange Anwendung des BDSG a.F. vorgeprägt sind – Berufsbetreuer ins Visier nehmen und diesen in Art und Umfang völlig unangemessene Pflichten auferlegen. Dies würde faktisch den Tod eines Berufsstandes zur Folge haben. Im Übrigen sind die Datenschutzbehörden auch personell nicht annähernd so aufgestellt, als dass nunmehr im großen Stil Jagd auf Datenschutz-Delinquenten gemacht werden könnte. Auch die im Gesetz vorgesehenen drakonischen Strafen wurden bislang dem Hörensagen nach nicht verhängt; es steht auch nicht zu erwarten, dass Verstöße mit existenzbedrohlichen Maßnahmen geahndet werden.

Erheben und Verarbeiten Sie nur so viele Daten, wie es für Ihre Tätigkeit individuell erforderlich ist. Man lässt Ihnen hier sicher einigen Spielraum. Sollten Sie sich aber aus diesem erheblich entfernen, kann durchaus im Einzelfall einmal Ungemach drohen.

IV. Sozialdatenschutz

Der Sozialdatenschutz wurde in den §§ 67 ff. SGB X neu gefasst.

Dabei wurde zunächst der Begriff der Sozialdaten in § 67 Abs. 2 Satz 1 SGB X verändert. Hierunter versteht man nunmehr personenbezogene Daten i.S.v. Art. 4 Nr.1 DS-GVO, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Eine wesentliche Änderung des Begriffs dürfte damit nicht verbunden sein. Denn der Begriff der „persönlichen und sachlichen Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person“ (§ 67 Abs. 1 SGB X a.F.) dürfte mit dem Begriff der personenbezogenen Daten i.S.v. Art. 4 Nr.1 DS-GVO weithin deckungsgleich sein, wenn auch vereinzelt Abweichungen bestehen können.

Die Rechte der betroffenen Person wurden in §§ 81 ff. SGB X weithin an europäische Standards angepasst, wobei § 83 SGB X weiterhin einen Auskunftsanspruch enthält.

Inhaltlich ergeben sich mit Blick insbesondere auf Einwilligungserfordernisse keine gravierenden Änderungen zum bisherigen Recht. Auch im Sozialrecht verhält es sich grundsätzlich so, dass die Verarbeitung von Daten einem **Verbot mit Erlaubnisvorbehalt** untersteht. Die Verarbeitung ist demnach – vorbehaltlich einer gesetzlichen Erlaubnis, wie Sie hier auf Basis des Art. 6 I lit. c. DS-GVO weithin bestehen wird (vgl. oben) – grundsätzlich von der Einwilligung des Betroffenen abhängig. Ist dieser (krankheitsbedingt) nicht mehr einwilligungsfähig, so sind die Kriterien der mutmaßlichen Einwilligung (vgl. § 1901 Abs. 2 BGB) heranzuziehen.

Da die §§ 60, 66 SGB I Mitwirkungspflichten des Betreuten (bzw. hier des rechtlichen Betreuers) vorsehen, deren Erfüllung für die Prüfung des Antrages auf Sozialleistungen (hier Leistungen der gesetzlichen Pflegeversicherung SGB X) erforderlich sind, haben Sie die Angaben/Auskünfte zu übermitteln.

Anders sieht dies ggf. bei einem einsichtsfähigen Betreuten aus, der Ihnen eine Weitergabe ausdrücklich untersagt. Hier sollte der Betreute, von Ihnen gleichwohl schriftlich dokumentiert, auf die Rechtsfolgen der Verweigerung (Versagung der Leistungen durch die Pflegekasse) hingewiesen werden.

Sollte es durch Sozialdatenmissbrauch seitens der Sozialleistungsträger oder in den Schutzbereich des Gesetzes nach § 78 Abs. 1 Satz 1 SGB X mit einbezogenen privaten Stellen (z.B. Arbeitgeber) zu einem Schaden für Ihren Betreuten kommen, so steht Ihrem Betreuten gem. § 82 SGB X Schadensersatz zu. Unabhängig hiervon haben Betroffene gem. § 83 SGB X Auskunftsansprüche gegen jede Stelle i.S.d. § 35 SGB I, welche Daten gespeichert und an wen diese weitergegeben worden sind.

Rechtssicheres Muster-Verarbeitungsverzeichnis (Art. 30 DS-GVO)

Vorbemerkung

Das nachfolgende Verarbeitungsverzeichnis setzt sich aus drei Komponenten zusammen:

1. einem Vorblatt, in welches die Angaben zum Verantwortlichen – also Ihre Daten – sowie Angaben zur Person des Datenschutzbeauftragten (soweit vorhanden) einzugeben sind;
2. ein Musterblatt, welches für jede Verfahrenstätigkeit gesondert auszufüllen ist; alternativ kommt auch die Führung einer Tabelle in Betracht, in welcher die einzelnen Tätigkeiten zu listen und zu spezifizieren sind;
3. eine knappe Darstellung der konkreten TOM (Beispiel, muss auf Ihren konkreten Fall spezifiziert werden).

Beachten Sie, dass das Verzeichnis nicht in Papierform geführt werden muss. Ein Vorhalt in nicht verkörperter Form ist insofern ausreichend.

Eine Herausgabe des Verzeichnisses an Ihre Betreuten und Dritte ist nicht vorgesehen. Das Verzeichnis ist allein der zuständigen Datenschutzbehörde auf Verlangen vorzulegen.

Verzeichnis von Verarbeitungen nach Art. 30 DS-GVO

Angaben zum Verantwortlichen

Name

Straße / Hausnummer

Postleitzahl / Ort

Telefon

Telefax

E-Mail

Angaben zum Datenschutzbeauftragten

Name

Straße / Hausnummer

Postleitzahl / Ort

Telefon

Telefax

E-Mail



Verarbeitungstätigkeit (Art. 30 Abs. 1 Satz 2 lit. a DS-GVO):		Vorgang-Nr.
Einführungsdatum:		Letzte Änderung:
Zwecke der Verarbeitung (Art. 30 Abs. 1 Satz 2 lit b DS-GVO)		
Kategorien betroffener Personen (Art. 30 Abs. 1 Satz 2 lit. c DS-GVO)	<input type="checkbox"/> Betreute / Klienten <input type="checkbox"/> Mitarbeiter <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input type="checkbox"/>	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 Satz 2 lit. c DS-GVO)	<input type="checkbox"/> Kontaktdaten (Name, Anschrift, etc.) <input type="checkbox"/> Bankdaten und Steuerdaten <input type="checkbox"/> Kommunikationsdaten (Email / Telefon) <input type="checkbox"/> Auskunftsdaten <input type="checkbox"/> IP-Adressen <input type="checkbox"/> Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO): <input type="checkbox"/> Gesundheitsdaten <input type="checkbox"/> Daten zur rassischen und ethnischen Herkunft <input type="checkbox"/> Biometrische Daten <input type="checkbox"/>	

<p>Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 Satz 2 lit. d DS-GVO)</p>	<p><input type="checkbox"/> intern</p> <hr/> <p><input type="checkbox"/> extern Empfängerkategorien:</p> <p><input type="checkbox"/> Behörden</p> <p><input type="checkbox"/> Gerichte</p> <p><input type="checkbox"/> Lieferanten</p> <p><input type="checkbox"/></p> <hr/> <p><input type="checkbox"/> Drittland Empfängerkategorien:</p>
<p>ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 Satz 2 lit. e DS-GVO)</p> <p>Nennung der konkreten Datenempfänger</p> <p>Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.</p>	<p><input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant</p> <p><input type="checkbox"/> Datenübermittlung findet wie folgt statt:</p> <p><input type="checkbox"/> Drittland (Name)</p> <p>Dokumentation geeigneter Garantien</p>

Fristen für die Löschung
der verschiedenen Daten-
kategorien
(Art. 30 Abs. 1 Satz 2 lit. f
DS-GVO)

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DS-GVO (Art. 30 Abs. 1 Satz DS-GVO 2 lit. g)

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
 1. *Alarmanlage*

Der Zutritt zu Datenverarbeitungsanlagen ist per Alarmanlage abgesichert. Bei Abwesenheit aller Mitarbeiter im Gebäude wird die Alarmanlage aktiviert.
 2. *Automatisches Zugangskontrollsystem*

Ein Schließsystem mit Transpondern und Codesperre ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Prüfung des Transponders und dem zugeordneten Code.
 3. *Schlüsselregelung*

Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.
 4. *Protokollierung der Besucher*

Besucher, die Zutritt zu Datenverarbeitungsanlagen erhalten (z.B. im Falle von Hardware-Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.
 5. *Videoüberwachung*

Datenverarbeitungsanlagen werden per Videoüberwachung überwacht.

- Zugangskontrolle
 1. *Passwortvergabe*

Ein Zugang zu Datenverarbeitungssystem ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich.
 2. *Einsatz von VPN-Technologie*

Sämtliche Datenverarbeitungssysteme sind für Mitarbeiter des Betreuungsbüros ausschließlich per VPN erreichbar. So wird gewährleistet, dass einerseits ein Zugriff nur für befugte Personen möglich ist und andererseits der Zugriff auf Daten über eine verschlüsselte Verbindung erfolgt.
 3. *Einsatz von Anti-Viren-Software*

Systeme, die von Personen zum Zugriff auf Datenverarbeitungssystem genutzt werden, sind mit einer Anti-Viren-Software ausgestattet. Diese Software wird regelmäßig auf die neusten Virus-Definitionen aktualisiert.
 4. *Verschlüsselung von mobilen Datenträgern*

Sofern mobile Datenträger oder mobile Geräte zum Einsatz kommen, werden die Inhalte verschlüsselt.
 5. *Zuordnung von Benutzerrechten*

Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.
- Zugriffskontrolle
 1. *Sichere Aufbewahrung von Datenträgern*

Datenträger, die personenbezogene Daten enthalten, werden verschlossen gelagert.
 2. *Verwaltung der Rechte durch einen eingeschränkten Personenkreis*

Ausschließlich berechtigte Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert.
 3. *Protokollierung von Zugriff auf Anwendungen*

Zugriffe auf Anwendungen werden protokolliert. Insbesondere die Änderung und Löschung personenbezogener Daten werden protokolliert.
 4. *Ordnungsgemäße Vernichtung von Datenträgern*

Datenträger, die personenbezogene Daten enthalten werden gemäß DIN 66399 vernichtet.
 5. *Passwortrichtlinie*

Passwörter werden regelmäßig geändert und die Anforderungen an Passwörter werden in

einer unternehmensweiten Richtlinie vorgegeben.

- Trennungskontrolle

1. *Festlegung von Datenbankrechten*

Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt.

2. *Trennung von Produktiv- und Testsystemen*

Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.

3. *Logische Mandantentrennung*

Durch den Einsatz unterschiedlicher softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.

B. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle

E-Mail-Verschlüsselung

Bei der Übermittlung von personenbezogenen Daten per E-Mail erfolgt der Versand verschlüsselt

- Eingabekontrolle

1. *Zuordnung von Benutzerrechten*

Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.

2. *Protokollierung von Dateneingaben*

Dateneingaben von personenbezogenen Daten werden protokolliert. Insbesondere die Änderung und Löschung dieser Daten werden protokolliert.

3. *Nachvollziehbarkeit der Eingabe*

Bei der Eingabe, Änderung und Löschung personenbezogener Daten wird der individuelle Benutzername, der die Änderung veranlasst hat, protokolliert.

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

1. *Unterbrechungsfreie Stromversorgung in Serverräumen*

Serverräume sind durch unterbrechungsfreie Stromversorgungen geschützt. Der Schutz ist zweistufig aufgebaut. Bei einem Stromausfall gewährleisten Backup-Batterien die Stromversorgung übergangsweise. Gleichzeitig wird ein Notstrom-Aggregat hochgefahren, das die Stromversorgung der Serverräume übernimmt

2. *Klimaanlagen in Serverräumen*

Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlagen gewährleistet.

3. *Feuer- und Rauchmeldeanlagen in Serverräumen*

Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.

4. *Aufbewahrung von Datensicherungen*

Datensicherungen von personenbezogenen Daten werden auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle

1. *Auswahl von geeigneten Auftragnehmern*

Bei der Auswahl von Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten

2. *Überwachung der Auftragnehmer*

Der Auftragnehmer wird regelmäßig auf die Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.

[Verantwortlicher]

[Datum]

[Unterschrift]



Informationen zur Erhebung personenbezogener Daten

1. Name und Kontaktdaten des Verantwortlichen

Name:	Martina Musterfrau
Straße / Hausnummer:	Musterstraße 1
Postleitzahl / Ort:	12345 Musterstatt
Telefon:	089 1234 5678 9
Telefax:	089 1234 5678 90
Email:	musterfrau@betreuungsbüro-musterfrau.de

2. Erhebung und Speicherung personenbezogener Daten und deren Verwendung

Aufgrund der bestehenden Betreuung erheben wir die im Rahmen der Erfüllung unserer Aufgaben im übertragenen Aufgabenkreis erforderlichen persönlichen Daten. Die Erhebung dieser Daten erfolgt, um die Betreuung ordnungsgemäß durchführen zu können. Die Datenverarbeitung erfolgt zur Erfüllung unserer rechtlichen Verpflichtung als Betreuer, Art. 6 Abs. 1 lit. c DS-GVO. Die von uns erhobenen personenbezogenen Daten werden bis zum Ende der Bearbeitungszeit bzw. bis zum Ablauf der gesetzlichen Aufbewahrungspflicht gespeichert und danach gelöscht. Es sei denn, dass wir nach Art. 6 Abs. 1 Satz 1 lit. c DS-GVO aufgrund von steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten (etwa aus HGB, StGB oder AO) zu einer längeren Speicherung verpflichtet sind oder Sie in eine darüber hinausgehende Speicherung nach Art. 6 Abs. 1 Satz 1 lit. a DS-GVO eingewilligt haben. Weitere als die oben genannten Daten werden nicht gespeichert.

3. Weitergabe von Daten an Dritte

Ihre personenbezogenen Daten werden an Dritte (Gerichte, Behörden, Arbeitgeber, Versicherungen, Vertragspartner, etc.) weitergegeben, sofern dies zur Erfüllung der uns übertragenen Betreueraufgaben erforderlich ist.

4. Betroffenenrechte

Sie haben das Recht:

- gemäß Art. 7 Abs. 3 DS-GVO Ihre einmal erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen;
- gemäß Art. 15 DS-GVO Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten zu verlangen. Insbesondere können Sie Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegen-

über denen Ihre Daten offengelegt wurden oder werden, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft Ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen;

- gemäß Art. 16 DS-GVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen;
- gemäß Art. 17 DS-GVO die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- gemäß Art. 18 DS-GVO die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von Ihnen bestritten wird, die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen und wir die Daten nicht mehr benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder Sie gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben;
- gemäß Art. 20 DS-GVO Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen und
- gemäß Art. 77 DS-GVO sich bei dem Landesbeauftragten für den Datenschutz (Aufsichtsbehörde) zu beschweren.

5. Widerspruchs- und Widerrufsrecht

Sofern Ihre personenbezogenen Daten auf Grundlage von berechtigten Interessen gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO verarbeitet werden, haben Sie das Recht, gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten einzulegen, soweit dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben.

Wenn Sie in die Verarbeitung Ihrer personenbezogenen Daten durch eine entsprechende Erklärung eingewilligt haben (Art. 6 Abs. 1 Satz 1 lit. a DS-GVO), können Sie die Einwilligung jederzeit für die Zukunft gemäß Art. 7 DS-GVO widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt. Ihren Widerruf oder Widerspruch richten Sie einfach per E-Mail an musterfrau@betreuungsbuero-musterfrau.de

(Datum, Unterschrift)



Suchwortregister

A

Aktenschrank	19
Aufsichtsbehörde	18
Auftragskontrolle	27
Auskunfts-, Berichtigungs-, Lösungsrecht	18
Auskunftsrecht	14, 18

B

back-up	20
Berichtigungsrecht	18
Beschwerderecht	18
Bestellungserfordernis	20
Betroffenenrechte	14, 32

D

Datenberichtigung	13
Datenempfänger	16
Datenerhebung	32
Musterformblatt	32
Datenhoheit	12
Datenkategorie	16, 17, 20
Datenlöschung	13, 14, 20
Datenminimierung	13, 15
Datenrichtigkeit	13
Datenschutz	
Grundsätze	12
Datenschutzbeauftragter	16, 20, 24
Datenschutzbehörde	17, 21, 23
Datenschutzfreundliche Voreinstellung	27
Datenschutzgrundverordnung (DS-GVO)	12
Datenschutz-Management	27
Datensparsamkeit	13
Datenverschlüsselung	19
Email-Account	19
Mobiles Gerät	19
Website	20
WLAN-Netzwerk	19

Datenweitergabe

Untersagung	22
Daten-Zugangskontrolle	20

E

Eingabekontrolle	27
Einwilligungserfordernis	14, 21
Einwilligungsvorbehalt	13
Erlaubnisvorbehalt	
Verbot	13
Europäischer Gerichtshof	14

G

Grundsatz der Datenminimierung	13
Grundsätze Datenschutz	12

I

Incident-Response-Management	27
Information zur Erhebung personenbezogener Daten	32
Informationspflicht	14, 17
Integrität	14, 27
IT-Sicherheit	18
Einhaltung technisch-organisatorischer Maßnahmen (TOM)	18, 27

K

Kategorie	25, 26, 32
Betroffene Person	25
Datenempfänger	26
Personenbezogene Daten	15, 25

L

Lösungsrecht	18
--------------------	----

M

Muster-Formblatt	18
Musterformblatt Datenerhebung	32
Muster-Verarbeitungsverzeichnis	16, 17, 20

P		Verarbeitungsverzeichnis	16, 17, 20
Personenbezogene Daten	14, 15, 17, 19, 32	Muster	20, 23
Einwilligung in die Verarbeitung	15, 16	Verpflichtung zur Führung	16
Verarbeitung	14, 15	Verbot mit Erlaubnisvorbehalt	14, 21
R		Verfahren zur Überprüfung, Bewertung und	
Recht auf Vergessenwerden	14	Evaluierung	27
S		Verfahrensverzeichnis	17
Sozialdaten	21	Verfügbarkeitskontrolle	27
Auskunftsanspruch	22	Vergessenwerden	14
Datenverarbeitung	21	Verschlüsselung von Daten	14
Schadensersatz	22	Vertraulichkeit	14, 27
Sozialdatenmissbrauch	22	Verzeichnis von Verarbeitungen	
Sozialdatenschutz	21	Muster	23
Sozialdatenmissbrauch	22	Virens Scanner	20
Sozialdatenschutz	21	W	
Speicherbegrenzung	13	Weitergabekontrolle	27
T		Widerspruchs-, Widerrufsrecht	32
Technische und organisatorische Maßnahmen (TOM)		Z	
.....	27	Zugangskontrolle	19, 27
Transparenz	13	Alarm-, Sicherheitsschloss	19
V		IT-System	19
Verarbeitungstätigkeit	25	Zugriffskontrolle	27
		Zutrittskontrolle	27
		Zweckbindung	13