Diakonie Deutschland

RECHTLICHE RAHMENBEDINGUNGEN DER DIGITALISIERUNG

im Bereich typischer diakonischer Anwendungsfelder

Langfassung/Vertiefungsdokument

Gefördert vom:

Bundesministerium für Familie, Senioren, Frauen und Jugend

INHALTSVERZEICHNIS

TEIL A

A.1. VORWORT

Das Thema Digitalisierung[1] ist bereits seit einiger Zeit in aller Munde. Und es ist zwischenzeitlich derart vielfältig geworden, dass seine Bezüge und Fragestellungen in einem einzelnen Werk schon lange nicht mehr erschöpfend dargestellt werden können. Das betrifft auch die rechtlichen Aspekte der Digitalisierung. Auch dieses Kompendium versucht eine abschließende Darstellung erst gar nicht. Es wird sich vielmehr auf einen bestimmten Ausschnitt des Themas beschränken, darauf nämlich, denjenigen rechtliche Informationen an die Hand zu geben, die sich im Rahmen diakonischer Zielsetzungen mit der Digitalisierung ihrer Angebote befassen. Und da auch das noch zu weit gefasst wäre, nimmt sich das Kompendium zwei typische Situationen vor, die es näher beleuchtet: Die Einführung einer digitalen Lösung als App einerseits und die Vermittlung von Dienstleistungen über eine Online-Plattform (insbesondere die Online-Beratung) andererseits.

Daraus ergibt sich auch die Struktur des Kompendiums. Beschränkt sich juristische Literatur häufig auf die abstrakte Darstellung der rechtlichen Bezüge, wird hier eine an der praktischen Verwendung orientierte Vermittlung versucht. Die beiden Ansätze werden in einem besonderen Teil (Teil B) für sich genommen dargestellt und die ihnen jeweils impliziten Rechtsfragen dabei spezifisch beantwortet. Wenn und soweit die Ausführungen auch für die jeweils andere Anwendung von Relevanz sind, werden sie grundsätzlich nicht wiederholt, sondern durch entsprechenden Verweis eingebettet. Darüber hinaus lockern themenspezifische Exkurse und Vertiefungen die Darstellung auf. Dabei werden mitunter auch solche Rechtsgebiete dargestellt, die für die gerade untersuchte Anwendung zwar keine zwingende Bedeutung haben, thematisch aber in Einzelfällen dennoch so wichtig sein können, dass sie einer Darstellung bedürfen. Ein allgemeiner Teil (Teil C) ist dem besonderen Teil nachgelagert. Darin werden solche Inhalte dargestellt, die grundsätzliche Relevanz für beide Anwendungsformen haben und insbesondere organisatorische Vorfragen betreffen. Dabei geht es beispielsweise um die gemeinnützigkeitsrechtlich relevante Frage der Organisationsform.

Für dieses Kompendium ist umfangreiche Rücksprache mit Praktikern insbesondere aus dem diakonischen Bereich gehalten worden. Ihre Erfahrungen fließen hier ein. Ihnen gilt der Dank des Verfassers.

Dennoch kann das Werk – das muss vorab ausdrücklich betont werden – nur die Grundlage zu einer kritischen Auseinandersetzung mit den angesprochenen Themenkreisen sein. Es soll das Problembewusstsein schaffen und Lösungsmöglichkeiten umschreiben, ohne die Universallösung oder die für jeden einzelnen Fall ideale Lösung darstellen zu können. **Das Kompendium kann natürlich keine Rechtsberatung im Einzelfall leisten oder einer solchen auch nur vorgreifen.** Im einschlägigen Bereich gibt es keine Lösung „von der Stange“. **Jedes einzelne Digitalisierungsvorhaben muss nach seinen Spezifitäten juristisch geprüft und begleitet werden.** Das vorliegende Kompendium kann insoweit nur Anhaltspunkte geben und einen ersten Überblick verschaffen.

Um es also seinem Umfang nach nicht ausufern zu lassen und es seinem Inhalt nach überschaubar und handhabbar zu halten, beschränkt sich das Kompendium an geeigneten Stellen auf eine Einführung in die Thematik, die die Leser*innen für den Problemkreis sensibilisieren soll, und verweist auf externe Materialien, die eine sachgerechte und zielgerichtete Vertiefung in den dargestellten Problemkreisen ermöglichen.

Den rechtlichen Ausführungen wird im Allgemeinen das geltende Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) sowie die DS-GVO zugrunde gelegt. Beide Normenapparate gelten gewissermaßen nebeneinander. Aufgrund des den Kirchen gemäß Art. 137 Abs. 3 WRV iVm. Art. 140 GG eingeräumten Selbstverwaltungsprivilegs, ist es ihnen in Deutschland gestattet, eigene Datenschutzgesetze zu schaffen. Dieses Privileg wird durch die Schaffung der Datenschutz-Grundverordnung (DS-GVO) nicht beseitigt, aber doch relativiert. Art. 91 DS-GVO sieht vor, dass kirchliches Datenschutzrecht fortbestehen kann, sofern es sich im Einklang mit der DS-GVO befindet. Mit einer Novellierung ihrer Datenschutzgesetze haben die beiden Kirchen Deutschlands diesen Einklang auch tatsächlich hergestellt.

[1] Der Begriff der Digitalisierung hat keinen festdefinierten Inhalt. Im ursprünglichen Sinne ist damit die Umwandlung analoger Informationen in digitale Informationen gemeint. Heute wird er häufig auch gleichbedeutend mit Automatisierung und sogar Optimierung verwendet.

Anmerkung:
Da die Regelungen des DSG-EKD also im Wesentlichen den Vorgaben der Datenschutzgrundverordnung (DS-GVO) entsprechen, hat die Frage, ob kirchliches oder weltliches Recht gelten soll, oftmals wenig Bedeutung. Da jedoch in einigen Bereichen, etwa bei den Geldbußen und Informations-/Transparenzpflichten Unterschiede bestehen, ist dennoch zum Teil fraglich, welchem Recht im zu entscheidenden Fall zu folgen ist. Die Frage ist unter Aufsichtsbehörden umstritten.[2] Eine Unterscheidung kann dergestalt getroffen werden, dass das **Kirchenprivileg** nur im kirchlichen Bereich gilt. Wird durch die kirchliche Anbieterin dagegen voll am Wirtschaftswettbewerb teilgenommen, dürfte es für die nichtkirchlichen Konkurrenten unter Umständen einen relevanten Nachteil darstellen, nicht ebenfalls dem Kirchenprivileg zu unterfallen. Jedenfalls dann, wenn unterschiedslos am privaten Wettbewerb teilgenommen wird, empfiehlt es sich, das Angebot vorsorglich anhand der Regelungen der DS-GVO auszurichten, sofern die Regelungen des DSG-EKD hinter diesen zurückbleiben sollten.[3] Dies ist insbesondere im medizinischen Bereich von Relevanz. Im Bereich der Seelsorge beispielsweise dagegen eher weniger.

Unionsrechtliche Vorgaben, sich verändernde Sicherheitslagen und technische Entwicklungen führen zu einer ständigen Bewegung im gesetzgeberischen Bereich. Viele der diesem Kompendium zugrundeliegenden Gesetze werden regelmäßig novelliert. Das vorliegende Kompendium ist im Wesentlichen auf dem Stand Oktober 2020. Obwohl viele der im November und insbesondere im Dezember vorbereiteten oder abgeschlossenen Gesetzesänderungen noch angesprochen werden können, können sie inhaltlich nicht mehr abschließend berücksichtigt werden. Zwar ist nur selten mit substantiellen Änderungen im vorliegend interessierenden Zusammenhang zu rechnen. Einer besonderen Prüfung bedarf es gleichwohl.

Verantwortliche sind daher gehalten, ihre Kenntnisse stets auf dem neuesten Stand zu halten, insbesondere die einschlägige Gesetzgebung und Rechtsprechung zu beobachten und ihre Anwendung auf den Einzelfall zu prüfen. Das Kompendium kann daher lediglich einen **bereichsspezifischen und temporären** Überblick über die zu beachtenden Anforderungen darstellen.

Die hier gegebenen Informationen wurden nach bestem Wissen zusammengestellt.

Besonderer Dank gilt dabei Herrn Prof. Dr. Michael Veddern, der sich um viele wesentliche Ergänzungen und Verbesserungen des Kompendiums verdient gemacht hat. Dennoch kann aber Vollständigkeit und Richtigkeit nicht garantiert werden. **Eine gute Rechtsbegleitung im einzelnen Fall kann durch kein abstraktes Werk ersetzt werden.**

Dank gilt ferner Frau Julia Zillinger, die die Ausführungen zur Finanzierung (C.5) im Wesentlichen beigesteuert hat, sowie Frau Meko Talla, die durch ihre geduldige und präzise Mitarbeit die erfolgreiche Veröffentlichung des Werkes sicherstellte.

Wir wünschen Ihnen viel Erfolg bei der Gestaltung der digitalen Transformation!

Für die Diakonie Deutschland im Dezember 2020
Dr. Daniel Burchardt

[1] Siehe Spyra, in: Clausen/Schroeder-Printzen (Hrsg.), Münchner Anwaltshandbuch Medizinrecht, 3. Aufl. 2020, Rz. 12 zu § 23, Fn. 11.
[3] Der Datenschutzbeauftragte für den Datenschutz EKD empfiehlt, alle Angebot vorsorglich anhand des jeweils strengeren Maßstabs auszurichten. Siehe dazu die „Arbeitshilfe zur Umsetzung von Informationspflichten“ (https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-umsetzung-von-informationspflichten/ – zuletzt abgerufen am 26. Juni 2020).

A.2 EINLEITUNG

Zur Sicherstellung einer zukunftsfähigen Versorgung auf gleichbleibend hohem Niveau einerseits und der Wettbewerbsfähigkeit des eigenen Angebots andererseits bedarf es langfristiger Strategien. Sicher haben Sie sich insoweit die drei wesentlichen Fragen der digitalen Transformation bereits gestellt und zufriedenstellend beantwortet, die Fragen danach, (1) was ist (2) wie (3) warum digital zu transformieren. Hierdurch wissen Sie grundlegend, welchen Weg Sie wie einschlagen wollen. Sie haben dafür ein Konzept entwickelt und planen, eine digitale Anwendung einzusetzen.[4] Sind Sie einmal so weit, setzen Sie wahrscheinlich auf eine plattform- (dazu Teil B.2) oder app-basierte (dazu Teil B.1) Umsetzung. Wie eingangs bereits beschrieben, werden die beiden Anwendungen im folgenden Teil getrennt nach ihren jeweiligen Besonderheiten dargestellt.

[4] Die effektive Vorbereitung digitaler Entwicklungen basiert auf einer Denkhaltung, die nicht nur modulhaft vorgeht, sondern einen stimmigen Gesamtplan verfolgt. Die einzelnen Handlungsfelder können dazu untersucht und der „Reifegrad“ ihres jeweiligen Angebots ermittelt werden. Daraus lassen sich Zukunftsvisionen entwickeln, deren organisatorische Voraussetzungen und notwendigen Umsetzungsschritte präzise bestimmbar und „gesamtplanerisch“ – miteinander – abzustimmen sind.

TEIL B

B.1 APPS

B.1.1 DEFINITION VON APPS

Eine App (kurz für Applikation bzw. application) bezeichnet ein Programm, das auf einer (mobilen) Plattform (das Betriebssystem des Endgeräts, zB. Smartphone) ausgeführt wird.[5] Dabei ist die Unterteilung in drei Kategorien denkbar.

- Native Applikation: zugeschnitten auf die Plattform, auf der sie ausgeführt wird;
- Web-Anwendung: unabhängig von der Plattform läuft sie innerhalb des Webbrowsers des Endgerätes;
- Hybride Lösung: alle möglichen Kombinationen aus nativer App und Web-Anwendung.

Die vorliegend insbesondere in Betracht kommenden (nativen) Apps können sowohl autonom auf dem Endgerät der Nutzer*innen (offline) als auch in Kombination mit einem Backend-Service (ein über das Internet angebundenes zentrales System im Hintergrund) angewendet werden. Solche Apps basieren auf den von der Plattform (zB. Android oder iOS) bereitgestellten Programmierwerkzeugen (Software Development Kits [SDK]). Durch diese ist ein direkter Zugriff auf Gerätekomponenten (wie etwa das Mikrofon und die Kamera) möglich. Bedienbarkeit und Performanz sind bei solchen Anwendungen aufgrund der engen Anbindung an das Betriebssystem des Endgerätes grundsätzlich hoch.

Allerdings sind mit dieser Anbindung auch Nachteile gegenüber Web-Anwendungen verbunden. So zum Beispiel ein womöglich erhöhter Pflegeaufwand. Denn ein Update des Betriebssystems kann zur Notwendigkeit der Anpassung der App führen, damit es nicht zu Beeinträchtigungen kommt. Auch muss die App auf mehrere Betriebssysteme angepasst sein, soll sie allen potentiellen Nutzern zur Verfügung stehen. Soll ein Vertrieb über die klassischen App-Stores erfolgen, sind zudem die vorgegebenen technischen und Qualitätsstandards der App-Stores zu erfüllen.

Web-Anwendungen, die dagegen auf klassischen Programmierwerkzeugen der Webentwicklung wie etwa HTML5 und JavaScript basieren, können dagegen als vom Betriebssystem unabhängige Anwendung auf jeder Plattform eingesetzt werden, ohne dass entsprechende Anpassungen am Programmcode vorgenommen werden müssen. Sie haben gegenüber den nativen Apps aber den bedeutenden Nachteil, dass mit ihnen nur ein sehr eingeschränkter Zugriff auf Gerätekomponenten möglich ist. Auch scheidet ein Vertrieb über die klassischen App-Stores aus.

Hybride Ansätze können die Vorteile der beiden Anwendungsformen ein Stück weit kombinieren, sind aber im Zweifel im Hinblick auf Performanz und Stabilität einer nativen Anwendung unterlegen.

Viele Anwendungen beschränken sich bei der Verarbeitung der Daten nicht ausschließlich auf die Ressourcen des Endgerätes des Nutzers, sondern lagern einzelne Aufgaben (beispielsweise die Authentifizierung der Nutzer oder die Speicherung von Daten) auf ein Backend-System aus. Dafür ist eine Internetverbindung zwingend erforderlich.

Exkurs: Usability/User Experience
Unabhängig davon, dass auch eine digitale Anwendung nur erfolgreich sein kann, wenn sie einen tatsächlichen Mehrwert für die Nutzer*innen verspricht, hängt ihr Erfolg maßgeblich von ihrer Nutzbarkeit (Usability) ab, also dem subjektiven Erleben vor, während und nach der Nutzung der Anwendung. Entscheidend ist vor allem das Oberflächendesign der Anwendung. Ein zeitgemäßes Layout ist das Minimum. Auch muss es auf unterschiedliche Gerätetypen angepasst, insbesondere mobile-responsive sein, um immer ansprechend und gut bedienbar zu sein. Die Nutzer*innen müssen in jedem Falle dort abgeholt werden, wo sie sind.

Häufig sind die Anstrengungen, die Usability zu erhöhen, sehr überschaubar. Nicht selten existiert hierfür kein Budget. Damit ist die Akzeptanz der Lösung – und damit die gesamte Investition – stark gefährdet.

[5] Eine allgemein verbindliche Definition einer App fehlt. Allen bekannten Ansätzen ist die Ausrichtung des Begriffs auf smarte mobile Systeme (Smart Devices) gemein. Ohne dass ein Computer zwischengeschaltet ist, kann der Bezug allein durch das Herunterladen der App aus dem Internet stattfinden, insbesondere aus den App-Stores des jeweiligen Plattformanbieters.

B.1.2 ANWENDUNGS-BEREICH

Der Anwendungsbereich von Apps ist in inhaltlicher Hinsicht grundsätzlich unbeschränkt. Allerdings haben (native) Apps im Vergleich zu webbasierenden Lösungen gewisse technische Nachteile, wenn es um die Sicherstellung voller Anonymität der Nutzer*innen geht. Apps sind daher im Bereich der Beratung mitunter nur eingeschränkt oder unter besonderen Bedingungen einsetzbar. Beratungsleistungen, die volle Vertraulichkeit und Anonymität voraussetzen, werden daher eher auf webbasierte Lösungen setzen (siehe dazu unter B.2). Auch ist fraglich, inwieweit potenziellen Nutzer*innen überhaupt auf eine App zurückgreifen. Eine Suchthilfe-App möchten womöglich nicht alle auf ihrem Gerät installieren, da dies in ungünstigen Fällen einer Stigmatisierung gleichkommen kann.

B.1.3 ANWENDBARES RECHT

In der Praxis ist meist kein oder nur eingeschränkt deutsches Recht anwendbar, wenn ein Auslandsbezug gegeben ist. Ein solcher folgt regelmäßig daraus, dass die Betreiberin des App-Stores ihren Geschäftssitz im Ausland unterhält. Das Internationale Privatrecht überlässt den Beteiligten die Wahl des anwendbaren Rechts, Art. 3 Abs. 1 S. 1 ROM I. Im Verhältnis der Anbieterin der App zur Betreiberin des App Stores erfolgt mitunter eine Festlegung auf das Recht am Sitz des Betreibers, nebst entsprechendem Gerichtsstand.[6]

Für Verbraucherverträge besteht diese Möglichkeit aber nach Art. 6 Abs. 2 S. 1 ROM I nur, wenn hierdurch nicht die im Aufenthaltsland des Verbrauchers geltenden Verbraucherschutznormen abgewählt werden und die ansonsten bestehende Geltung ausländischen Rechts in AGB dem Verbraucher gegenüber hinreichend transparent gemacht wird. Sowohl im Verhältnis zwischen der Anbieterin der App zu den Nutzer*innen als auch zwischen der Betreiberin des App-Stores und den Nutzer*innen ergibt sich somit eine andere Ausgangssituation als zwischen Anbieterin der App und Betreiberin des Stores. In der Praxis sollte daher die **Anwendung deutschen Rechts** im Verhältnis zu den Nutzer*innen **vereinbart** werden,[7] soweit der App-Store dies technisch und rechtlich zulässt.

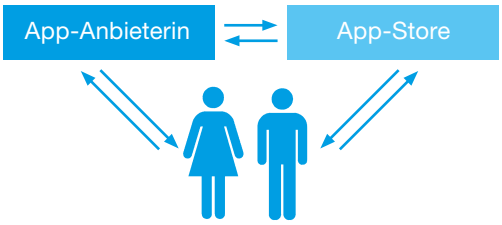


Fig. A. 1: Vertragsverhältnisse bei Angebot einer App

B.1.3.1 Verhältnis zwischen App-Anbieterin und Store-Betreiberin

Aufgrund ihrer Schlüsselstellung zwingen die Betreiberinnen der App-Stores die Anbieterinnen der Apps regelmäßig in US-amerikanisches Recht, wenn es um deren Vertragsbeziehungen geht. Die Bedingungswerke sind so recht einseitig und enthalten regelmäßig

- die Vereinbarung recht umfassender Nutzungsrechte an den Apps (Weitervertrieb);
- technische, inhaltliche und datenschutzrechtliche Vorgaben für die Umsetzung der Apps, die von Shop zu Shop zT. sehr unterschiedlich sind;
- die Möglichkeit der umfassenden Prüfung der App, die allerdings auch bei positivem Ausgang keinen Anspruch auf dauerhaften Verbleib im Store begründet;
- Regelungen zu Laufzeit und Kündigung, die eine umfassende Kündigungsmöglichkeit für die Store-Betreiberinnen begründen;
- umfassende Freistellungansprüche und Haftungsregelungen;
- die Pflicht zur Einhaltung voller Compliance.[8]

Zwar würden viele dieser Regelungen einer ABG-Kontrolle nach deutschem Recht kaum standhalten können. Dieses findet aber – wie erwähnt – regelmäßig in den Beziehungen der App-Anbieterin und der App-Store-Betreiberin keine Anwendung. Etwaige Ansprüche gegen die Store-Betreiberin wären zudem im Regelfall in den USA durchzusetzen.

B.1.3.2 Verhältnis zu den Nutzer*innen

Mit dem Klick auf den „Kaufen“- oder „Laden“-Button kommt zunächst ein Kauf- bzw. Schenkungsvertrag zwischen der Betreiberin des Stores und den Herunterladenden zustande. Aufgrund der Gestaltung des Shops ist für die Nutzer*innen

[6] Selbst wenn keine ausdrückliche Rechtswahl erfolgt, wird regelmäßig das Recht des Geschäftssitzes der App-Store-Betreiberin maßgeblich sein, da sie die relevante Dienstleistung der Bereitstellung der App in ihrem Store erbringt, vgl. Art. 3 Abs. 1b), Abs. 2 ROM I. Das Verbraucherrecht des Aufenthaltsstaates des Verbrauchers bleibt aber dennoch erhalten (Art. 6 ROM I).

[7] Aber auch in diesem Fall bliebe bei einer grenzüberschreitenden Verbreitung den Nutzer*innen das Verbraucherrecht ihres Aufenthaltslandes erhalten (Art. 6 ROM I).

[8] Praxistipp bei Auslandsbezug: Sollte die App auf anderen als dem deutschen Markt Einsatz finden, sind mögliche Regelverstöße auch nach ausländischem Recht umfassend zu prüfen. Bei Einsatz in anderen EU-Staaten befreit allerdings das sog. »Herkunftslandprinzip« in Art. 3 Abs. 1 und 2 E-Commerce-RL 2000/31/EG (§ 3 TMG) gegenüber den Nutzer*innen von dieser Pflicht (Ausnahmen: Verbraucherschutzrecht, Urheber- und sonstiges Recht des geistigen Eigentums, Datenschutzrecht).

regelmäßig nicht klar genug ersichtlich, dass es sich bei den Anbieterinnen von Apps um mehr als die bloßen Entwickler*innen handelt. Nutzer*innen gehen so weitgehend davon aus, dass die Store-Betreiberin auch die Anbieterin ist. Dies trifft insbesondere auf das Vertriebsmodell eines klassischen **»Wholesale/Retail Model«** zu, indem der App-Store eindeutig nach außen als Verkäuferin auftritt.

Soweit der Vertrieb innerhalb des App-Stores einem **»Commission/Agency Model«** folgt, bei dem der App-Store in Form einer Vermittlerin bzw. Handelsvertreterin zwischen App-Anbieterin und Nutzer*innen und auf Provisionsbasis agiert, kann – je nach konkreter Ausgestaltung – auch ein Vertragsschluss zwischen App-Anbieter*in und Nutzer*innen in Betracht kommen. In diesem Fall würde auch die datenschutzrechtliche Verantwortung der App-Anbieterin einschließlich der Erfüllung der datenschutzrechtlichen Informationspflichten bereits mit Anbieten im App-Store greifen (s. B.1.5).[9]

Neben dem Vertragsverhältnis zu der Store-Betreiberin wird beim Herunterladen der App ein Vertragsverhältnis zur Anbieterin der App insbesondere dann entstehen, wenn die Herunterlandenden hierauf **hinreichend hingewiesen** wurden bzw. hiervon zwingend ausgehen mussten. Dies gilt vor allem bei Hinterlegung von AGBs, wobei die Verbraucher mit Blick auf § 305 Abs. 2 BGB die Möglichkeit erhalten müssen, diese in zumutbarer Weise zur Kenntnis zu nehmen, und der Geltung der zusätzlichen Bestimmungen **zuzustimmen** (möglichst per Opt-in). Ob dies im Einzelfall so ist, hängt wesentlich von der Gestaltung des jeweiligen App-Stores ab. Eine schuldrechtliche Beziehung zwischen der App-Anbieterin und den Nutzer*innen ist aber spätestens bei Inbetriebnahme der App anzunehmen.

B.1.4 VERTRIEB VON APPS UND BEGLEITENDE PFLICHTEN UND FOLGEN

B.1.4.1 Pflicht zur Anbieterkennzeichnung und Informationspflichten

Beim Vertrieb von Apps ergeben sich sowohl für die App-Store-Betreiberin des Stores als auch für die Anbieterin der App spezifische Informationspflichten.

Der Store bedarf – wie jeder Online-Shop – einer Anbieterkennzeichnung gem. § 5 Abs. 1 TMG („Impressum"). Hinzukommen können gesellschaftsrechtliche Informationspflichten.

Auch hinsichtlich der App selbst gilt idR. diese Pflicht, da sie zumeist ein Telemedium iSd. § 1 Abs. 1 TMG ist.[10] Aufgrund des strengen Maßstabs, den der BGH im Hinblick auf die Erreichbarkeit eines Impressums aufstellt, sollte dieses möglichst **mit nicht mehr als einem Klick erreichbar** sein,[11] zB. mittels eines Buttons am unteren oder oberen Bildschirmrand.

Sofern auch journalistisch-redaktionell gestaltete Inhalte vermittelt werden, ist gem. § 18 Abs. 2 MStV[12] ergänzend ein hierfür Verantwortlicher unter Angabe von Name und Anschrift zu benennen, wobei bei Angestellten neben der Namensnennung die Angabe der Anschrift der App-Betreiberin ausreicht.[13]

Der Bezug von Apps durch Verbraucher*innen begründet einen Fernabsatzvertrag iSd. § 312c Abs. 1 BGB.[14] Da App-Stores Telemediendienste sind, handelt es sich auch um einen Vertrag im elektronischen Geschäftsverkehr nach § 312i Abs. 1 S. 1 BGB. Damit treffen die Betreiberin – die stets Unternehmerin ist – die Pflichten zur Anbieterkennzeichnung bereits vorvertraglich sowie eine Reihe weiterer allgemeiner und spezifischer Informationspflichten. Den **Informationspflichten**[15] kann formfrei im App-Store oder über eine Website, falls der Download über diese erfolgt, nachgekommen werden. In jedem Fall müssen die Hinweise klar und für die Durchschnittsbetrachterin verständlich sein. Die Verständlichkeit ist an einen besonderen Empfängerhorizont anzupassen, sofern sich die Nutzer*innen vom allgemeinen Durchschnitt absetzen.

Nach Vertragsabschluss sind den Verbraucher*innen per Textform, d. h. per Email, SMS etc., die Vertragsschlüsse möglichst zu bestätigen sowie die weiteren notwendigen Informationen und verwendete AGBs zu übermitteln.[16] Entsprechendes gilt für die Belehrung über das Widerrufsrecht (s. nachfolgend).

B.1.4.2 Einräumung eines Widerrufsrechts

Ein Fernabsatzvertrag über den Bezug einer App („digitaler Inhalt"), begründet gegenüber Verbraucher*innen idR ein zweiwöchiges **Widerrufsrecht** nach § 312g Abs. 1 BGB.

[9] Faktisch muss die App-Anbieterin allerdings mangels Einflusses darauf hoffen, dass die App-Store-Anbieterin datenschutzrechtliche Vorgaben ausreichend erfüllt, obwohl sie hierfür prinzipiell haftbar gemacht werden kann.

[10] Als Telemedium gilt jeder Informations- und Kommunikationsdienst mit Ausnahme reiner Telekommunikationsdienste und des Rundfunks (§ 1 Abs. 1 TMG), sprich jede Internet- oder mobile Anwendung, bei der im Zuge ihrer Nutzung ein Datenaustausch mit Servern stattfindet. Nicht erfasst sind hingegen rein stationär auf dem Endgerät laufende Anwendungen (reines Softwareprodukt).

[11] In seinem Grundsatzurteil zur Erreichbarkeit von Impressen ließ der BGH (Urteil v. 20. Juli 2006, Az. I ZR 228/03) allerdings auch zwei Klicks ausreichen.

[12] Der Medienstaatsvertrag (MStV) soll in Kürze den Staatsvertrag für Rundfunk und Telemedien (RStV) ablösen. Die Vorgängerregelung findet sich in § 55 RStV. Wurde bisher die Information zu der redaktionell verantwortlichen Person im Impressum mit „Inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV" eingeleitet hat, muss diese Formulierung nunmehr dahingehend angepasst werden, dass es zukünftig „Inhaltlich verantwortlich gemäß § 18 Abs. 2 MStV" lauten muss.

[13] Auf keinen Fall sollte statt der Angabe von Anschriften ein Postfach verwendet werden. »Anschrift« meint ladungsfähige Anschrift. Unter einem Postfach kann keine wirksame Ladung zu Gericht erfolgen. Daher wäre die reine Angabe eines Postfachs abmahnfähig.

[14] Sollte es sich um ein B2B-Angebot handeln, ist zu beachten, dass auch für diese – wenn auch etwas begrenztere – Informationspflichten gelten.

[15] Die Informationspflichten sind im Einzelfall gründlich zu ermitteln. In der Regel genügt es, dass die weiteren Informationen vor Vertragsabschluss über einen Link abrufbar sind. Der Prozess des Vertragsabschlusses muss nicht so programmiert sein, dass die Bestellung erst abgesandt werden kann, wenn die Informationen zur Kenntnis genommen sind (BGH, Urteil vom 20.7.2006, I ZR 228/03).

[16] Art. 246b § 2 Abs. 1 S. 2 EGBGB.

Darüber ist geeignet und korrekt zu **belehren**.[17] Das Widerrufsecht kann gemäß § 356 Abs. 5 BGB vorzeitig erlöschen, wenn – mit Download der App – die Ausführung des Vertrags mit ausdrücklicher Zustimmung (Opt-in) der Verbraucher*innen zum Verlust des Widerrufsrechts erfolgt. Dies ist ggf. geeignet zu dokumentieren und in der Vertragsbestätigung zu dokumentieren (§§ 312f Abs. 2 und 3 BGB). Erfolgt keine Zustimmung, besteht das Widerrufsrecht für 14 Tage ab Vertragsschluss. Unterbleibt die Widerrufsbelehrung oder ist sie fehlerhaft, bleibt das Widerrufsrecht nach § 356 Abs. 3 BGB für zwölf Monate und 14 Tage erhalten. Gemäß Art. 246a § 1 Abs. 2 S. 1 Nr. 1 EGBGB ist auch „über das Muster-Widerrufsformular in Anlage 2“[18] zu informieren.

Praxistipp:
Auf der Angebotsseite im App-Store bzw. beim In-App-Purchase[19/20] auf der Bestellseite innerhalb der App sollte ein Hinweis auf das Widerrufsrecht, die Widerrufsbelehrung sowie ein Link zum Widerrufsformular vorhanden sein.

B.1.4.3 Haftung für Mängel

Apps gelten nach der höchstrichterlichen Rechtsprechung als Sachen iSd. § 90 BGB.[21] Daher kommt eine kauf- oder schenkungsrechtliche (Mängel-)Haftung in Betracht.

B.1.4.3.1 Mängelhaftung bei kostenpflichtigen Apps

Bei Vorliegen eines Sach- oder Rechtsmangels iSd. §§ 434 f. BGB greifen Mängelhaftungsansprüche gemäß §§ 437 ff. BGB. Abzustellen ist auf den Zeitpunkt der vollständigen Übertragung der App. Sofern keine besondere Beschaffenheit vereinbart ist, ergeben sich mögliche Sachmängel überwiegend nach § 434 Abs. 1 S. 2 Ziff. 2 BGB, so dass es auf den „gewöhnlicher Gebrauch“ ankommt. Typische Mängel sind Abstürze, Kapazitätsmängel, Inkompatibilitäten oder mangelnde Verfügbarkeit des mit der App bereitgestellten Dienstes.

Auch wenn die App mehr mitbringt als beabsichtigt, kann ein Mangel vorliegen – insbesondere bei Schadsoftware. Denn auch eine **nicht gefahrlose Nutzung** begründet einen Mangel. Gleiches gilt für den Fall, dass bei Nutzung vertrauliche oder personenbezogene Daten ungerechtfertigt übermittelt werden.

Ein möglicher Rechtsmangel kann zudem darin liegen, dass die Betreiberin oder Anbieterin die Nutzungsrechte an der App den Nutzer*innen nicht oder nicht hinreichend einräumen kann, weil sie zB Rechte an urheberrechtlich geschützten Texten, Fotos oder Videos nicht wirksam erworben hat. Die **Rechtsinhaberschaft** bedarf also stets eines besonderen Augenmerks.

B.1.4.3.2 Mängelhaftung bei kostenfreien Apps

Wird eine App kostenfrei angeboten, so beschränkt dies den **Haftungsmaßstab**. Denn der Schenker haftet nach § 524 Abs. 1 BGB bei „Fehlern“ der Sache (Sachmangel im Sinne des § 434 BGB) nur bei Arglist. Eine Haftung kommt z. B. in Betracht, wenn die Anbieterin der App bzw. die Betreiberin des Stores eine App **trotz Kenntnis des Mangels** weiter bereitstellt. Bei bekanntem Fehler ist die App **unverzüglich vom Netz** zu nehmen.

Die **Digitale Inhalte-Richtlinie** (EU) 2019/770 wird die Gewährleistungsrechte für digitale Inhalte und Dienstleistungen in Kürze stark ausweiten. Unabhängig von der Vertragsart werden zugunsten von Verbraucher*innen – ähnlich wie im Kaufrecht – **umfassende Gewährleistungsrechte** eingeführt. Diese sollen auch für entgeltfreie Verträgen gelten, bei denen nur „mit Daten bezahlt“ wird. Zudem werden die Verkäufer zur **kostenfreien Bereitstellung funktionserhaltender Updates und Sicherheitsupdates** verpflichtet. Die EU-Richtlinie ist bis Mitte 2021 umzusetzen.

B.1.4.4 Lauterkeitsrechtliche, marken- und urheberrechtliche Fragen

Die Gestaltung und Anpreisung einer App kann in verschiedenster Hinsicht den Vorwurf einer **Unlauterkeit** begründen, insbesondere sollte jede Form einer irreführenden Angabe oder Anpreisung vermieden werden. So darf beispielweise eine kostenpflichtige App zunächst auf keinen Fall als kostenfrei dargestellt und angeboten werden. Alle zahlungsauslösenden Vorgänge müssen eindeutig als solche gekennzeichnet sein. Auch sonst sollten die Leistungsbeschreibungen und werblichen Darstellungen einer App keine irreführenden Angaben enthalten. Diesbezüglich sind vor

[17] Ein Muster hat der Gesetzgeber gleich mitgeliefert, und zwar als Anlage 1 zu Art. 246a § 1 Abs. 2 S. 2 des Gesetzes zur Umsetzung der Verbraucherrichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung (https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl113s3642.pdf%27%5D__1593509962782)

[18] https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl113s3642.pdf%27%5D__1593509962782

[19] Dabei handelt es sich um aus der App selbst heraus getätigte Rechtsgeschäfte, die Erweiterungen und Ergänzungen der App selbst betreffen. Im Gegensatz dazu ist ein App-Sale der Kauf einer nicht mit der App zusammenhängenden Sache über die App (zB. der Kauf eines über die App angebotenen Buches). Wird eine App zunächst kostenfrei angeboten, ist der spätere Zukauf kostenpflichtiger Elemente für das bestimmungsgemäße Funktionieren der App aber notwendig, darf die App wegen andernfalls möglicher Irreführung nicht als Gratisangebot beworben werden.

[20] Sofern der In-App-Purchase auf Smart Devices mit technisch begrenzter Darstellungsmöglichkeit erfolgt, kommen dem Anbieter hinsichtlich der fernabsatzrechtlichen Bestimmungen die Erleichterungen gem. Art. 246a § 3 EGBGB zugute. Die gesetzeskonforme Darstellung der notwendigen Mindestangaben auf den unterschiedlichen Endgeräten ist aber sicherzustellen.

[21] Grundsätzliches liefert hierzu das Urteil des BGH vom 15. November 2006 – XII ZR 120/04, CR 2007, 75 Rn. 16 – ASP.

allem die Vorgaben des Gesetzes gegen den unlauteren Wettbewerb (UWG) und die hierzu ergangene Rechtsprechung zu beachten.

Besondere Vorsicht ist auch bei an **Kinder und Jugendliche** gerichtete Angebote anzuwenden. Diese dürfen nicht im Hinblick auf finanzielle Entscheidungen intransparent oder mit übermäßigen Anreizen beeinflusst werden. Davon abgesehen ist stets zu beachten, dass Kinder unter sieben Jahren geschäftsunfähig und zwischen sieben bis einschließlich siebzehn Jahren nur beschränkt geschäftsfähig sind (§§ 104 ff. BGB). Sie bedürfen daher für Vertragshandlungen ggf. der Vertretung bzw. der Zustimmung seitens der Eltern bzw. vertretungsberechtigten Personen sowie ggf. zur wirksamen Einwilligung in die Verarbeitung von personenbezogenen Daten (siehe B.1.5.2.2).

Im Zusammenhang mit **medizinischen oder therapeutischen Angeboten** sind zudem die strengen Vorgaben des Heilmittelwerbegesetzes zu beachten. Aus diesem ergeben sich ggf. eine Reihe von Vorgaben und Einschränkungen hinsichtlich der Beschreibung angebotenen medizinischer und therapeutischer Leistungen. Auch bei der werblichen Darstellung sind strenge Vorgaben zu beachten. Soweit ein App als Medizinprodukt iSd. am 26. Mai 2021 in-Geltung-tretenden Medizinprodukte-Verordnung (siehe B.1.6.1) anzusehen ist, sind zudem die Vorgaben in Art. 7 MDR zu berücksichtigen.

Hinsichtlich der Bezeichnung und des grafischen Auftritts hat die Anbieterin einer App **Marken- und Titelrechte** zu beachten. Die Integration von Texten, Fotos, Videos und sonstigem Content hat nach Maßgabe des **Urheberrechts** zu erfolgen. Vorsicht ist auch bei der Übernahme von **Anordnungs- und Zugriffstrukturen** anderer Apps geboten, und zwar unabhängig davon, ob sie Strukturen des User Interfaces oder des Backends betreffen. Denn auch kreative Strukturen können als sog. Datenbankwerk urheberrechtlichen Schutz genießen.

Das Layout bzw. User Interface einer App kann neben einem urheberrechtlichen Schutz, welcher eine gewisse kreative Gestaltungshöhe erfordert, durch einzutragende **Designrechte** (auch Geschmacksmusterrechte) geschützt sein. Unter einem Designschutz können selbst Schriftzeichen bzw. Typografien stehen, wenn diese beim europäischen Amt für geistiges Eigentum oder DPMA eingetragen und nicht älter als 25 Jahre sind.

Da **Programmcodes** idR. urheberrechtlich geschützt sind, darf auch fremder Code grundsätzlich nicht ohne entsprechende Zustimmung bzw. Lizenz seitens der Rechtsinhaber*innen übernommen werden. Wird auf eine freie Open Source-Software zurückgegriffen, sind zudem streng die Bedingungen der Open Source-Lizenz einzuhalten.

Von Beginn an ist im Rahmen eines effektiven **Rechtemanagements** Wert darauf zu legen, dass die App-Betreiberin am Ende alle Rechte bzw. Lizenzen in Bezug auf die App, den Titel, den Code, die Struktur, das Layout und Design sowie den Content erwirbt und in Händen hält sowie berechtigt ist, diese für die Zwecke der Verwertung weiter zu lizenzieren.

Dabei sollte – ebenfalls von Beginn an – auf die **Sicherung und Wahrung eigener geistiger Eigentumsrechte** Wert gelegt werden. Insbesondere soweit **Patente für eine (Software-)Erfindung** in Betracht kommen, ist streng darauf zu achten, dass Erfindungen nicht vor einer möglichen Patentanmeldung Dritten gegenüber – ohne Absicherung durch effektive Geheimhaltungsvereinbarungen – offengelegt werden. Ist eine Erfindung einmal gegenüber der Öffentlichkeit verwendet, präsentiert, publiziert, beschrieben oder sonst mitgeteilt, fehlt ihr die für eine Patentanmeldung nötige Neuheit. Der Erwerb eines Patentes ist damit endgültig gescheitert.

Davon abgesehen können **Ideen für neue Apps, Plattformen, Geschäftsmodelle etc. sowie Entdeckungen, neue Erkenntnisse, Know-how etc. und sonstige geschäftliche Informationen** durch das – in Umsetzung der Richtlinie (EU) 2016/943 erlassene – **Gesetz zum Schutz von Geschäftsgeheimnissen** vor unerlaubter Offenlegung, Nutzung oder unerlaubtem Erwerb geschützt werden. Voraussetzung ist das Bestehen bzw. Ergreifen angemessener Geheimhaltungsmaßnahmen, die jeweils an Art, Verwendung und Bedeutung der konkret zu schützenden Informationen auszurichten sind. Insbesondere bei Einbeziehung Dritter unter Offenlegung von Geschäftsgeheimnissen besteht der gesetzliche Schutz als Geschäftsgeheimnis dabei nur fort, wenn dieser durch zuvor abgeschlossene Vertraulichkeitsvereinbarungen (**Non Disclosure Agreement – NDA**) – möglichst mit Vertragsstrafenversprechen – mit allen einbezogenen Dritten abgesichert ist.

B.1.5 DATENSCHUTZ UND DATENSICHERHEIT (APP-SPEZIFISCH)[22]

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[23]

[22] Siehe allgemein zum Datenschutz unten Teil C.1.1.

[23] BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209/83 (BVerfGE 65, 1 - Volkszählung), Rz. 146 (auf der Website des BVerfG: http://www.bverfg.de/e/rs19831215_1bvr020983.html).

B.1.5.1 Beim Vertrieb der App

Hier wird zunächst davon ausgegangen, dass die App direkt über einen App-Store vertrieben wird. Die Betreiberin des App-Stores ist idR. die Verantwortliche iSd. Datenschutzrechtes. Denn zwischen der Anbieterin der App und den Herunterladenden besteht zu diesem Zeitpunkt noch kein Kontakt. Tritt die App Store-Betreiberin hingegen im Rahmen eines „Commission/Agency"-Models lediglich als Vermittlerin auf, beginnt die datenschutzrechtliche Verantwortung der App-Betreiberin ggf. schon mit dem Anbieten der App im App-Store. In diesem Fall agiert der App-Store ggf. als Auftragsverarbeiterin des App-Anbieters, deren Handeln der App-Betreiberin zuzurechnen ist (siehe auch C.1.1.1.5.1.3).[24]

Die Vorschriften des europäischen **Kundendatenschutzes** sowie des **Datenschutzes im E-Commerce** sind insoweit von der Betreiberin des Stores und auch von der App-Betreiberin umfassend einzuhalten und von Letzterer ggf. gegenüber der App-Store-Betreiberin mittels Auftragsverarbeitungsverträgen inklusive Weisungsrechten sicherzustellen.

Hieran ändert auch nichts, sofern die App-Store-Betreiberin in den USA sitzt. Denn das europäische Datenschutzrecht erhebt einen weltweiten Anspruch, soweit personenbezogene Daten von Europäern oder sich innerhalb der EU aufhaltender Personen oder Daten auf Servern innerhalb der EU verarbeitet werden.[25]

B.1.5.2 Bei der Nutzung der App

Spätestens ab Nutzung der App ist die **Anbieterin** der App **datenschutzrechtlich** verantwortlich und den aus der DS-GVO bzw. dem DSG-EKD (und [noch][26] dem TMG/TKG) folgenden Pflichten unterworfen.

Die Verarbeitung von personenbezogenen Daten ist verboten, soweit sie nicht erlaubt ist. Außerhalb der Einwilligung der Berechtigten kommen für die Anbieterin regelmäßig zwei weitere Erlaubnistatbestände in Betracht:

Zum einen erlaubt Art. 6 Abs. 1 lit. b DS-GVO/§ 6 Ziff. 5 DSG-EKD die Datenverarbeitung dann, wenn diese **zur Erfüllung eines Vertrages** oder zur **Durchführung vorvertraglicher Maßnahmen** auf Anfrage der betroffenen Person erforderlich ist. Dieser Erlaubnistatbestand setzt also voraus, dass bereits ein Schuldverhältnis zwischen der Anbieterin und der betroffenen Person besteht oder dieses zumindest begründet werden soll, und zwar auf Anfrage der betroffenen Person. Wird die Datenverarbeitung auf diesen Erlaubnistatbestand gegründet, so trifft die Verantwortliche die Pflicht, die Daten unverzüglich zu löschen, wenn sich der Verwendungszweck erledigt hat. Eine Ausnahme besteht nur dann, wenn gesetzliche Pflichten (etwa aus dem Bereich des Steuerrechts oder der **GOBD** [dazu C.2]) anderes verlangen.

Darüber hinausgehend kann die Datenverarbeitung aufgrund einer Interessenabwägung gerechtfertigt sein, wenn sie zur Wahrung der berechtigten Interessen der Anbieterin erforderlich ist und **keine überwiegenden Interessen** der schutzwürdigen Person entgegenstehen, Art. 6 Abs. 1 lit. f DS-GVO bzw. § 6 Ziff. 3 und 4 iVm. Ziff. 8 DSG-EKD (sog. „Abwägungsklausel"). Eine umfassende Datenverarbeitung oder die Erstellung von Persönlichkeitsprofilen kann aufgrund dieser Interessenabwägung niemals zugunsten der Anbieterin ausfallen. Bei Kindern oder Menschen mit Einschränkungen/Behinderungen fällt die Abwägung ohnehin besonders restriktiv aus.

In der Praxis der Bundes- und Landesdatenschutzrechtsbeauftragten sowie der Gerichte hat sich mittlerweile eine enge Auslegung abgezeichnet, die im Zweifel einer ausdrücklichen Einwilligung in die Datenverarbeitung den Vorzug gibt. Allerdings hängt die Abwägung im Einzelfall stark von der Art der verarbeiteten Daten ab. So sind berufsbezogene Daten (z. B. wer, wo, in welcher Funktion beruflich tätig ist) weniger schutzwürdig als Daten über persönliche Eigenschaften/Gegebenheiten oder private Handlungen).

Die **Verarbeitung besonderer Kategorien personenbezogener Daten** iSd Art. 9 Abs. 1 DS-GVO/§ 7 Abs. 5 iVm. § 13 DSG-EKD – also etwa die Verarbeitung von Gesundheitsdaten durch sogenannte Health Apps – kann nur nach den strengen Anforderungen des Art. 9 Abs. 2 DS-GVO iVm § 22 BDSG-neu/§ 13 Abs. 2 DSG-EKD als erlaubt angenommen werden, die in der Praxis nur selten vorliegen. Daher kommt in praktischer Hinsicht häufig nur die **Einwilligung** der berechtigten Person als Rechtsgrundlage der Verarbeitung in Betracht.

Im Einzelfall können Verarbeitungsvorgänge aber unter Einhaltung von Informationspflichten und sonstiger strenger datenschutzrechtlicher Vorgaben[27] insbesondere dann zulässig sein (§ 22 Abs. 1 Nr. 1 BDSG-neu/§ 13 Abs. 2 DSG-EKD), wenn diese erforderlich sind,

- um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen;
- zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit eines Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs

[24] Mangels wesentlichen Einflusses auf das Handeln der App Store-Betreiberin bleibt hier faktisch idR nur die Hoffnung, dass diese im Einklang mit den europäischen Datenschutzvorgaben agiert, wobei das Agieren der App Store-Betreiberin der App-Anbieterin durchaus zurechenbar sein kann.

[25] Eine weitere komplexe Frage ist derzeit, ob und unter welchen Voraussetzungen personenbezogene Daten von der EU aus auf Server in die USA übertragen werden dürfen. Der EuGH hatte kürzlich die Rahmenvereinbarungen zwischen den USA und der EU (sog. »Privicy Shield«) wegen eines nicht ausreichenden Datenschutzniveaus innerhalb der USA für europarechtswidrig erklärt (s. EuGH, Urteil v. 16. Juli 2020, Rs. C-311/18 – Facebook Ireland und Schrems). Siehe dazu näher unter C.1.1.1.9.1.1.

[26] Mit Verabschiedung der ePrivacy-Verordnung wird sich das TKG aller Voraussicht nach erledigen.

[27] Zu beachten sind ggf. insbesondere auch die strengen Vorgaben in § 22 Abs. 2 BDSG und § 13 Abs. 3 DSG-EKD. Es sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten.

und wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten;
- die Verarbeitung durch eine verantwortliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der verantwortlichen Stelle oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
- zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

Des Weiteren erlaubt ist die Verarbeitung personenbezogener Daten, die die betroffene Person – z. B. in sozialen Medien – offensichtlich selbst öffentlich gemacht hat. Aber auch in diesen Fällen bleiben die sonstigen datenschutzrechtlichen Vorgaben für die Verarbeitung einschließlich von Informationspflichten (s. Art. 14 DS-GVO iVm § 33 BDSG/§ 18 DSG-EKD) bestehen.

Eine erleichterte Verwendbarkeit von geschützten Daten für zB. Zwecke der Gesundheitsversorgung könnte der geplante Data Governance Act bringen. Der Vorschlag soll die Richtlinie (EU) 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors ergänzen. Der **Data Governance Act**[26] soll über die Richtlinie hinaus – unter bestimmten Voraussetzungen, ua. durch „Datenspenden“ (Datenaltruismus) – auch solche, in der öffentlichen Hand befindliche Daten zugänglich machen, die Rechten Dritter unterliegen. Letztere können sowohl Rechte zum Schutz personenbezogener Daten als auch geistige Eigentumsrechte sein.

Neue Möglichkeiten der digitalen Gesundheitsversorgung eröffnet auch das **Patientendaten-Schutz-Gesetz – PDSG** v. 14. Oktober 2020. Es ermöglicht E-Rezepte per App mit Schnittstellenfunktion, digitale Facharzt-Überweisungen und die **freiwillige elektronische Patientenakte (ePA)** für Befunde, Arztberichte oder Röntgenbilder. Ab 2022 sollen in der ePA zusätzlich auch der Impfausweis, der Mutterpass, das gelbe U-Heft für Kinder sowie das Zahn-Bonusheft gespeichert werden können. Die Patient*innen sollen per elektronischer Steuerung selbst entscheiden können, welche der in der ePA gespeicherten Gesundheitsdaten sie welchen Ärzt*innen und Gesundheitsdienstleistern für welche Zwecke freigeben. Dabei bleiben Ärzt*innen und Gesundheitsdienstleister als Nutzer der ePA für die von ihnen verarbeiteten Gesundheitsdaten voll verantwortlich.

B.1.5.2.1 Einwilligung[29]

Neben den beschriebenen Erlaubnisgründen ist die Einwilligung der wichtigste und im vorliegenden Zusammenhang auch regelmäßig entscheidende Erlaubnistatbestand. Die an die Einwilligung zu stellenden Anforderungen sind an Art. 6 Abs. 1 lit. a iVm. Art. 7 DS-GVO/§ 6 Ziff. 2 iVm. § 13 DSG-EKD (und [noch][30] § 13 Abs. 2 TMG bzw. § 94 TKG) zu messen. Wobei TMG/TKG als Weiterung verlangen, dass die **Einwilligung jederzeit abrufbar**, also für die Berechtigten einsehbar sein muss. Das ergibt sich allerdings auch aus dem Sinnzusammenhang der jederzeitigen Widerrufsmöglichkeit, die voraussetzt, dass einsehbar sein muss, was widerrufen werden darf.

Bei der datenschutzrechtlichen Einwilligung nach Art. 7 DS-GVO/§ 11 DSG-EKD muss es sich um eine **freiwillige**, für den bestimmten Fall **informiert** und **unmissverständlich** abgegebene Willensbekundung handeln. Die Nutzung eines Dienstes darf insbesondere nicht von der Einwilligung in eine Datenverarbeitung abhängig gemacht werden, die für die Nutzung nicht erforderlich ist. So darf das Zustandekommen eines Vertrags nicht von einer Einwilligung zu einer dafür nicht erforderlichen Verarbeitung (zB. Newsletter) abhängig sein. Es läge eine unzulässige Kopplung vor.

Den Erklärenden muss zudem eindeutig offengelegt werden, für welche Zwecke, in welchem Umfang, für welche Dauer und für welche Verarbeitung durch welche Einrichtungen und Unternehmen und für welche Weitergabe an welche Personen sie einwilligen. Auch wie und auf welchem (einfachen) Weg die Einwilligung jederzeit widerrufen werden kann, muss klar kommuniziert sein.

Sofern eine Einwilligungserklärung die zu gebende Einwilligung derart vorbereitet, ist sie zusätzlich noch an der allgemeinen Inhaltskontrolle gemäß §§ 305c Abs. 1, 307ff. BGB zu messen. Dagegen verstoßen beispielsweise Einwilligungserklärungen mit dem Zweck, die Verarbeitung personenbezogener Daten „nach Gutdünken“ zu legitimieren. Die Anbieterin einer App muss sich bei der Einholung der Einwilligung stets auf einen **bestimmten** legitimen Zweck begrenzen, der für die Nutzung der App erforderlich ist. Die Einwilligung ist **optisch hervorzuheben**, wenn ihr Text gemeinsam mit anderem Texten geliefert wird (zB. durch Fettdruck oder Umrandung). Der Versuch, eine Einwilligung versteckt in den Nutzungsbedingungen oÄ. einzuholen, ist von vornherein untauglich.

[29] Sehr hilfreich zum Thema der datenschutzrechtlichen Einwilligung sind auch die „Guidelines 05/2020 on consent under Regulation 2016/679“ des European Data Protection Board: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (zuletzt abgerufen am 06. Dezember 2020).

[30] Mit Verabschiedung der ePrivacy-Verordnung werden sich das TKG und TMG aller Voraussicht nach erledigen.

Bei Apps wird die Einwilligung ausnahmslos elektronisch erklärt. Dabei genügt ein Berühren, Klicken oder Häckchensetzen (Opt-in). Opt-out-Lösungen sind hingegen nicht ausreichend.[31] Die elektronische Form nach §§ 126 Abs. 3, 126a BGB ist aber nicht einzuhalten. Der **Beweislast** gemäß Art. 7 Abs. 1 DS-GVO/§ 11 DSG-EKD/§ 13 Abs. 2 TMG/§ 94 TKG wird die Verantwortliche jedoch ohne eine **Protokollierung** der Einwilligung, die den Wortlaut der Einwilligungserklärung, den Zeitpunkt der Einholung und das zur Authentifizierung der einwilligenden Person genutzte Verfahren festhält, nicht nachkommen können.

Praxis-Hinweis:
Ein Problem bleibt in den Fällen bestehen, in denen das Smart Device von mehreren Nutzer*innen verwendet wird. Dann wird die notwendige Einwilligung im Zweifel nur von einer Nutzer*in eingeholt, aber dennoch die Nutzung der App durch verschiedene Nutzer*innen ermöglicht. Deren Nutzungen erfolgen dann im Zweifelsfall, ohne dass ein Erlaubnistatbestand erfüllt ist. Der sicherste – wenn auch etwas unpraktische – Weg, derartige Probleme zu umgehen, bestünde darin, vor jeder Nutzung eine erneute Einwilligung einzuholen. Eine weitere Möglichkeit bietet eine individuelle Identifizierung per Passwort oder biometrischer Daten (zB. Fingerabdruck).

Vorsorglich sollte **vor dem Download darauf hingewiesen** werden, wenn eine App ohne Einwilligung nicht betreibbar ist.

B.1.5.2.2 Die Einwilligung Minderjähriger[32]

Die Einwilligung Minderjähriger ist ein besonderes Thema. Anbieterinnen müssen sich insbesondere im Bereich der Online-Beratung bewusst sein, dass die die Beratung in Anspruch nehmende Person nicht rechtswirksam in die Verarbeitung ihrer Daten einwilligen kann. Grundsätzlich ist bei Jugendlichen gemäß Art. 8 Abs. 1 S. 1 DS-GVO ab 16 Jahren von der notwendigen Einsichtsfähigkeit auszugehen, so dass diese eine wirksame Einwilligung abgeben können.

Die Regelung begegnet aber im hier interessierenden Bereich zwei Einschränkungen. Immerhin ist für den Bereich der Online-Beratung schon sehr fraglich, ob es sich dabei überhaupt um einen „Dienst der Informationsgesellschaft“ im Sinne der Vorschrift handelt.[33] Zum anderen hat das DSG-EKD von der Öffnungsklausel Gebrauch gemacht und eine eigenständige Regelung gefunden, nämlich § 12 DSG-EKD. Danach sind Minderjährige soweit einwilligungsfähig, wie sie religionsmündig sind. Die Erklärung ist **speziell am Verständnishorizont der Minderjährigen auszurichten.**

Bei Fehlen der Einwilligungsfähigkeit wird die Einwilligung der Sorgeberechtigten bzw. deren Zustimmung in die Einwilligung des Minderjährigen nötig. Keine Einwilligung der Sorgeberechtigten – sogar unabhängig des Alters des Kindes – ist schließlich dann vorauszusetzen, wenn kirchliche Präventions- oder Beratungsdienste einem Kind **unmittelbar** angeboten werden. Wenn also die Leistung direkt gegenüber dem Kind erfolgt, ist das Thema Einwilligung grundsätzlich überhaupt nicht von Relevanz. Umso **fürsorglicher** ist aber mit den Daten des Kindes umzugehen.

Hinsichtlich der beim Erwerb von Apps abzuschließenden Verträge ist – abseits des Datenschutzes – zu beachten, dass Kinder unter sieben Jahren geschäftsunfähig und zwischen sieben bis einschließlich siebzehn Jahren beschränkt geschäftsfähig sind (§§ 104 ff. BGB) und daher ggf. der Vertretung bzw. Zustimmung seitens der Eltern bzw. vertretungsberechtigten Personen bedürfen.[34]

B.1.5.3 Informationspflicht des Anbieters

Die Nutzer*innen sind noch vor der eigentlichen Nutzung in einem gesetzlich vorgeschriebenen Mindestmaß zu informieren. Die Grundsätze einer **fairen und transparenten Verarbeitung** erfordern, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Dies sollte in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache geschehen, was insbesondere für Informationen gilt, die sich speziell an Kinder richten (Art. 12 Abs. 1 DS-GVO, § 16 Abs. 1 DSG-EKG).

Zudem sollte die Verantwortliche den Nutzer*innen alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.[35] Im Falle einer Einwilligung sollte der Einwilligende per Opt-in erklären, dass er die notwendigen Informationen zur Kenntnis genommen hat.

[31] EuGH, Urt. v. 11. November 2020, Rs. C 61/19.

[32] Siehe hierzu auch Ziffer 7.1. der „Guidelines 05/2020 on consent under Regulation 2016/679“ des European Data Protection Board: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (zuletzt abgerufen am 06. Dezember 2020).

[33] Der Begriff „Dienst der Informationsgesellschaft“ (information society service) bezieht sich auf eine Dienstleistung iSd. Art. 1 Nr. 1 lit. b RL 2015/1636/EU. Solche Dienste sind demnach „in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte“ Dienstleistungen. Die Einstufung als entgeltlich im entscheidenden Sinne wäre aber jedenfalls auch dann möglich, wenn zwar keine unmittelbar finanzielle Gegenleistung erfolgte, die den Dienst nutzende Person aber mit ihren Daten „zu bezahlen“ hätte oder Einnahmen über Werbebanner erzielt würden.

[34] Der neue § 14a TMG sieht zudem vor, dass personenbezogene Daten, die eine Diensteanbieterin von Minderjährigen etwa durch Mittel zur Altersverifikation oder andere technische Maßnahmen, oder anderweitig gewonnen hat, nicht für kommerzielle Zwecke verarbeitet werden dürfen.

[35] Vgl. Erwägungsgrund 60; sowie zusätzlich 61-62 im Hinblick auf die Informationspflichten insgesamt.

.

Gemäß Art. 13 Abs. 1 DS-GVO/§ 17 DSG-EKD ist vor[36] Beginn des Nutzungsvorgangs mindestens über

- die Person des Verantwortlichen und ggf. seines Vertreters oder des Datenschutzbeauftragten,
- den Zweck und die Rechtsgrundlage der Verarbeitung,
- über das ggf. verfolgte berechtigte Interesse sowie ggf. über (Kategorien von) mögliche/n Empfänger(n) und
- ggf. die Absicht der Übermittlung in ein Drittland,[37] einschließlich Informationen zum (Nicht-)Vorhandensein eines Angemessenheitsbeschlusses der EU-Kommission oder ggf. bestehender Verhaltensregeln (siehe C.1.1.1.9.1)

zu informieren.

Weitere Informationspflichten ergeben sich aus Art 13. Abs. 2 DS-GVO/§ 17 Abs. 2 DSG-EKD, und zwar insbesondere im Hinblick auf die

- Dauer der Datenspeicherung oder, falls nicht möglich, Kriterien für die Bestimmung der Dauer,
- Rechte der Nutzer*innen wie Auskunfts-, Löschungs- und Berichtigungsansprüche sowie das Beschwerderecht bei der Aufsichtsbehörde,
- ggf. bestehende Widerrufsmöglichkeit (bei Datenverarbeitung aufgrund von Einwilligungen immer),
- ggf. gesetzlich oder vertraglich vorgeschriebene oder für einen Vertragsschluss erforderliche Bereitstellung der personenbezogenen Daten, und welche mögliche Folgen die Nichtbereitstellung hätte.

Zudem sollten die Nutzer*innen in einschlägigen Fällen über das Bestehen einer **automatisierten Entscheidungsfindung** sowie eines möglichen **Profilings** unterrichtet werden und ihnen aussagekräftige Informationen über die insoweit zugrundeliegende Logik, Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung gegeben werden. Im Rahmen automatisierter Entscheidungen sind zudem stets Beschränkungen und Voraussetzungen von Art. 22 DS-GVO zu beachten.

Sind Daten nicht beim Betroffenen selbst erhoben worden, sondern – gedeckt durch einen Erlaubnistatbestand – aus anderen Quellen, sind die notwendigen Informationen nachträglich zur Verfügung zu stellen (Art. 14 DS-GVO, § 18 EKD-DSG). Zusätzlich ist in diesen Fällen über die zur Person gespeicherten Daten, deren Herkunft oder die evtl. empfangenden Stellen zu informieren.

Die nachgelagerte Informationspflicht entfällt, wenn

- die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert,
- die Erlangung oder Offenlegung durch Rechtsvorschriften, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist,
- die personenbezogenen Daten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Im Übrigen ist die nachgelagerte Informationspflicht auszuüben:

- innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
- falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
- falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

Beabsichtigt die Verantwortliche Stelle, personenbezogenen Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt sie der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck zur Verfügung, Art. 13 Abs. 3 DS-GVO/§ 17 Abs. 3 DSG-EKD. Allerdings sind nachträgliche Zweckänderungen ohne Einwilligung des Betroffenen nur in engen Grenzen möglich (Art. 6 Abs. 4 DS-GVO, § 7 DSG-EKD, §§ 23, 24 BDSG).

Die gesetzlich vorgesehene Ausnahme zu den Informationspflichten nach Art. 13 Abs. 4 DS-GVO/§ 17 Abs. 4 DSG-EKD (die betroffene Person verfügt bereits über die Information) kann bei der erstmaligen Installation einer App nicht zur Anwendung kommen. Zu beachten ist, dass die Kenntnisnahme **nicht unnötig erschwert** werden darf; dies verstieße gegen das Transparenzgebot, Art. 12 Abs. 1 DS-GVO/§ 16 DSG-EKD.

Da es sich bei den Informationen auch um **Allgemeine Geschäftsbedingungen** (AGB) handelt, müssen sie sich auch an den Vorgaben der §§ 305ff. BGB messen lassen.

Praxis-Hinweis:
Hält sich die Verantwortliche an die obenstehenden Vorgaben, ist ein Verstoß gegen AGB-rechtliche Regelungen kaum denkbar, sofern keine zusätzlichen Klauseln aufgenommen werden.

Eine Arbeitshilfe zur Umsetzung von Informationspflichten findet sich auf der Seite des Datenschutzbeauftragten der EKD.[38]

[36] Bestenfalls vor dem Download, wenn es durch die Installation bereits zur Datenverarbeitung kommt. Anderenfalls vor der ersten Nutzung/Aktivierung der App.

[37] Eine Übertragung von personenbezogenen Daten in Staaten, die nicht der EWG angehören, ist eine datenschutzrechtlich komplexe Frage. Insbesondere in die USA ist dies derzeit nur im Rahmen sog. „Standard-Datenschutzklauseln" möglich, wobei auch diesbezüglich weiterhin Fragen ungeklärt sind (siehe EuGH, Urteil v. 16. Juli 2020, Rs. C-311/18 – Facebook Ireland und Schrems).

[38] https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-umsetzung-von-informationspflichten/ (zuletzt abgerufen am 07. Dezember 2020).

B.1.5.4 Pflichten nach TKG[39]

Das gegenüber der DS-GVO speziellere Datenschutzrecht des TKG kann für Apps Anwendung finden, die Voice-over-IP-Telefonfunktionen (VoIP) einschließlich der Vermittlung oder Entgegennahme von Anrufen in bzw. aus Festnetz- oder Mobilfunknetzen bieten.[40] Dies kann insbesondere bei Beratungs-Apps der Fall sein, die den Nutzer*innen eine persönliche Telekommunikation mit Beratenden ermöglichen.

Um die Darstellung nicht zu überfrachten, wird im Folgenden nur auf einige wichtige bereichsspezifische Besonderheiten des TKG eingegangen.[41] Im Übrigen ist bei Einrichtung von Telekommunikationsdiensten wie VoIP eine intensive Auseinandersetzung mit dem TKG und insbesondere den spezifischen Vorschriften zum Fernmeldegeheimnis sowie zum Datenschutzschutz unerlässlich (insb. §§ 88 ff. TKG, §§ 109, 109a TKG). Die zur DS-GVO gemachten Ausführungen sind auch bei Anwendung des TKG weitestgehend zu beachten.[42]

Sofern die App die Möglichkeit zu einer persönlichen Kommunikation einräumt, berührt sie das verfassungsrechtlich (in Art. 10 GG) geschützte Fernmeldegeheimnis. War dies ursprünglich insbesondere gegenüber dem Staat zu schützen, gebietet die Möglichkeit des privaten Angebots von Kommunikationsdiensten die Notwendigkeit, den Schutz im Hinblick auf diese Dienste auszuweiten. In Anlehnung an die verfassungsrechtliche Rechtsprechung zu Art. 10 Abs. 1 GG erfasst daher auch § 88 Abs. 1 TKG die nähen Umstände der Telekommunikation, sofern diese eine Gefährdung der Vertraulichkeit des Kommunikationsvorgangs begründen. Hierunter fallen alle Informationen über Zeit und Ort und sowie Art und Weise des unkörperlichen Kommunikationsvorgangs, einschließlich erfolgloser Verbindungsversuche oder der Tatsache, ob jemand am Vorgang beteiligt war oder nicht.

Im Hinblick auf die Einhaltung von Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses soll auf Folgendes hingewiesen werden:[43]

- Zur Wahrung des Fernmeldegeheimnisses ist jede Diensteanbieterin verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort; sie trifft alle mit den Daten in Kontakt kommenden Mitarbeiter*innen persönlich, auch nach Beendigung der Tätigkeit.
- Jeder Diensteanbieter hat erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen.
- Es ist zu verhindern, dass Diensteanbieter sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Gleichermaßen ist zu verhindern, dass sich unbefugte Dritte Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation erlangen. Dies gilt für alle technischen Einrichtungen zur mittelbaren und unmittelbaren Übertragung von Nachrichteninhalten sowie Einrichtungen zur Erhebung, Verarbeitung und Nutzung von Verkehrsdaten.
- Im Bereich der Verwaltung und Verwahrung von Akten, welche dem Fernmeldegeheimnis unterliegen, sind für den Datenschutz hinreichende Aufbewahrungsbehältnisse zu verwenden sowie entsprechende Räume und Anlagen mit effektiver Zugangskontrolle sinnvoll einzusetzen. Es dürfen nur Personen Zugriff und Zugang haben, welche eine ausreichende Belehrung über die Sensibilität dieser Daten erhalten haben, Geheimhaltungspflichten unterliegen und für die ein Datenzugriff notwendig ist.
- Es muss sichergestellt werden, dass bei Nachrichtenübermittlungssystemen mit Zwischenspeicherung ausschließlich die Teilnehmenden durch ihre Einwilligung Inhalt, Umfang und Art der Verarbeitung bestimmen. Schutzmaßnahmen, die lediglich den Teilnehmenden selbst gestatten zu entscheiden, wer Nachrichteninhalte eingeben und darauf zugreifen darf, können durch entsprechende Zugangscodes und Kennwörter erfüllt werden. Diese werden nur den Teilnehmenden vertraulich übermittelt und sollen von diesen selbständig nach Erhalt verändert werden. Es liegt in der Einwilligungsfreiheit der Teilnehmenden, an welche Personen sie die Zugangskennungen weitergeben.
- Schutzmaßnahme gegen eine ungerechtfertigte, entgegen des Vertragsverhältnisses vereinbarte Löschung von

[39] Mit einer umfassenden Novelle des TKG ist alsbald zu rechnen. Ein Referentenentwurf für eine umfassende TKG-Novelle wurde jüngst veröffentlicht (siehe auch https://www.bundesregierung.de/breg-de/aktuelles/faq-tkg-novelle-1827846 [zuletzt abgerufen am 16. Dezember 2020). Im weiteren Gesetzgebungsverfahren sind allerdings noch erhebliche Änderungen möglich. Die wichtigen Bereiche Fernmeldegeheimnis und Datenschutz sind zudem aus dem Entwurf der TKG-Novelle herausgelöst. Beides soll – nach derzeitigem Stand – in einem separaten Gesetz für die Bereiche Telekommunikation und Telemedien zusammenfassend geregelt werden („Telekommunikations-Telemedien-Datenschutz-Gesetz – TTDSG"). Die Konzentrierung der Vorschriften in diesem neuen Gesetz hätte den Vorteil, dass der Gesetzgeber bei Erlass der europäischen ePrivacy-VO das TKG (und ggf. TMG) nicht erneut ändern, sondern nur das TTDSG entsprechend aufheben müsste.

[40] Bei Nutzung einer eigenen Infrastruktur außerhalb des öffentlichen Internets ist ein Telekommunikationsdienst iSd. § 3 Nr. 24 TKG anzunehmen.

[41] Allgemein zum TKG kann einordnend gesagt werden, dass es Regelungen zum Schutz des Fernmeldegeheimnisses bereichsspezifisch in §§ 88 ff. TKG trifft. Den Schutz personenbezogener Daten verfolgen die §§ 91 ff. TKG. Gegenstand der §§ 100, 109 Abs. 5 TKG ist der Schutz der Telekommunikationsinfrastruktur vor Störungen und die Verfügbarkeit der Telekommunikationsdienste.

[42] Entsprechend Art. 95 DS-GVO kommen Vorschriften der DS-GVO vorrangig zur Anwendung, es sei denn eine entgegenstehende Regelung des TKG erfolgt in Umsetzung der ePrivacy-Richtlinie. § 95 TKG wird daher beispielsweise weitestgehend von der DSGVO verdrängt, wogegen § 109 TKG eine Umsetzung von Art. 4 Abs. 1 ePrivacy-Richtlinie sowie der Richtlinie 2002/21/EG (Rahmenrichtlinie) darstellt und insofern vorrangig anwendbar ist. Es ist damit zu rechnen, dass die anstehende TKG-Novelle auch Vorschriften der Verordnung (EU) 2016/679 vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO) umsetzt. Insofern steht der 2. Abschnitt des 7. Teils des TKG wohl vor einer Neuordnung.

[43] Ausführlich zu den Anforderung nach TKG: Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 01. Juli 2020).

Nachrichteninhalten durch die Diensteanbieterin kann beispielsweise das Anlegen von Backup-Systemen sein.
- Die Nutzer*innen sind über die ggf. besonderen Risiken der Verletzung der Netzsicherheit aufzuklären und ggf. auch über mögliche Abhilfen zu informieren.
- Im Fall einer Verletzung des Schutzes personenbezogener Daten ist unverzüglich die Bundesnetzagentur und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen.

B.1.5.4.1 Verkehrsdaten[44]

Während Bestandsdaten im Rahmen von Vertragsverhältnissen unter den Voraussetzungen des § 95 TKG erhoben und verarbeitet werden dürfen,[45] ist dies für Verkehrsdaten ausschließlich für die in § 96 Abs. 1 TKG aufgelisteten Zwecke möglich. Dabei handelt es sich ausschließlich um technische Zwecke, die etwa Aufbau, Aufrechterhaltung und Abrechnung der Verbindungen dienen.

Unter bestimmten weiteren Bedingungen kann die Ermittlung von Kommunikationsprofilen einzelner Teilnehmer und die Analyse von Verkehrsströmen mittels Einwilligung und umgehender Anonymisierung zulässig sein, § 96 Abs. 3 S. 1 TKG. Die Verkehrsdaten sind von der Diensteanbieterin idR. nach Beendigung der Verbindung unverzüglich zu löschen, § 96 Abs. 1 S. 3 TKG.[46] Die Pflichten zur Vorratsdatenspeicherung in § 113b TKG sind bis auf Weiteres ausgesetzt.[47]

Für Verbindungen zu bei der Bundesnetzagentur registrierten Anschlüssen von Organisationen aus dem sozialen oder kirchlichen Bereich, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, ist zu beachten, dass die Verkehrsdaten solcher Verbindungen durch die Diensteanbieterin **auch nicht auf Anordnung** der Strafverfolgungsbehörden nach § 100g Abs. 2 StPO iVm. § 113b TKG auf Vorrat gespeichert und übermittelt werden dürfen (§ 113b Abs. 6 TKG). Der Betreiber des Telekommunikationsdienstes wie VoIP hat die Liste der registrierten Einrichtungen hierzu quartalsweise abzufragen und Änderungen unverzüglich anzuwenden.

B.1.5.4.2 Abrechnung

Sind die aufgebauten Verbindungen entgeltpflichtig, so sind die gespeicherten Daten der entsprechenden Verbindungen nur dann mitzuteilen, wenn die Nutzerin/der Nutzer vor dem maßgeblichen Abrechnungszeitraum in Textform (zB. Brief, Email, SMS) einen Einzelverbindungsnachweis verlangt hat. Nur auf Wunsch dürfen auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. Zu den weiteren Einzelheiten der Bereitstellung von Einzelverbindungsnachweisen insbesondere auch bei Anschlüssen mit mehreren Nutzern oder an Betriebsstätten siehe § 99 Abs. 1 TKG. Auf Anfrage der Nutzenden ist der Einzelverbindungsnachweis (geschützt) zur Verfügung zu stellen.

In diesem Zusammenhang sei betont, dass § 99 Abs. 2 S. 1 TKG den Einzelverbindungsnachweis immer dann ausschließt, wenn es sich um Verbindungen von Personen, Behörden und Organisationen in sozialen und kirchlichen Bereichen handelt, die Beratungsleistungen gegenüber einem grundsätzlich anonymen Personenkreis durch zur Verschwiegenheit verspflichteten Mitarbeitern erbringen (zB. im Rahmen der Telefonseelsorge), soweit deren Anschlüsse bei der Bundesnetzagentur **registriert** sind.

Sind bei der Erstellung von Telekommunikationsrechnungen oder der Erbringung von Telekommunikationsdienstleistungen Dritte eingebunden (z. B. durch Diensteanbieter ohne eigene Netzinfrastruktur), dann sind technische und organisatorische Schnittstellen-Beziehungen zwischen Auftraggeberin (Diensteanbieterin) und Auftragnehmerin (Erfüllungsgehilfin) eindeutig zu regeln. Nicht benötigte Daten nach § 97 Abs. 3 TKG sind unverzüglich zu löschen.

B.1.5.4.3 Standortdaten

Standortdaten dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden und selbst dann auch nur, wenn sie **anonymisiert** wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine – elektronische[48] – **Einwilligung** erteilt hat (§ 98 TKG). In diesen Fällen hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Nutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurde, zu informieren. Von dieser Verpflichtung ist der Anbieter befreit, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden.

Es ist ein **Prozess** zu gestalten, vermittels dessen die Verarbeitung von Standortdaten für jede Verbindung zum Netz oder für **jede** Übertragung auf einfache Weise und unentgeltlich zeitweise von den Nutzer*innen untersagt werden kann.[49]

[44] Vgl. zu diesen und dem Umgang mit ihnen ausführlich Schramm/Shvets, Verkehrsdaten zwischen ePrivacy-RL und ePrivacy-VO, MMR. 09/2019, S. 568 ff. Zu Bestandsdaten allgemein: Schramm/Shvets, MMR 2019, S. 228 ff.

[45] Ergänzend sollten hierzu die Vorgaben der DS-GVO für die Verarbeitung von personenbezogenen Daten im Rahmen von Vertragsverhältnissen berücksichtigt werden.

[46] Auf den Leitfaden des/der BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten (Stand 19.12.2012) wird verwiesen (abrufbar unter www.bundesnetzagentur.de).

[47] EuGH, Urteil v. 6.10.2020 – Rs. C-511/18, C-512/18, C-520/18 hat zwar unter bestimmten Bedingungen erstmals eine Vorratsdatenspeicherung zugelassen. Die dt. Vorschriften müssen dem neuen Urteil aber noch angepasst werden.

[48] Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen.

[49] Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Anbieter allerdings sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

B.1.5.4.4 Datenerhebung zur Beseitigung von Störungen

Die Diensteanbieterin darf zum Erkennen und zur Abwehr von Störungen im erforderlichen Umfang Bestands-, Verkehrs- und Steuerdaten erheben und verwenden. Dies wird durch § 100 Abs. 1 TKG mit einem datenschutzrechtlichen Erlaubnistatbestand unterlegt.

Allerdings ist dieses in bestimmten Fällen mit einer Berichtspflicht verknüpft.[50] Es ist aber abzusehen, dass § 100 Abs. 1 TKG und die mit dieser Vorschrift verbundene Berichtspflicht mit den datenschutzrechtlichen Anpassungen in einer geplanten umfassenden Novelle des TKG obsolet werden.[51]

B.1.5.4.5 Informationspflichten im Falle einer Datenschutzpanne (Data Breach)

§ 109a TKG regelt bestimmte Informationspflichten im Falle einer Verletzung des Schutzes personenbezogener Daten („Datenschutzpanne“ oder „Security Breach“). Der Diensteanbieterin obliegen in diesem Zusammenhang bestimmte Benachrichtigungspflichten gegenüber dem Betroffenen, aber auch gegenüber der Bundesnetzagentur und dem/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[52] Insbesondere hingewiesen wird auf die die DS-GVO übersteigende Verpflichtung, Datenpannen binnen 24 Stunden online zu melden (Art. 2 i. V. m. Anhang I der „Datenpannen-VO“).[53]

Zur Abwendung von Störung und Missbrauch darf die Diensteanbieterin den Datenverkehr einschränken, umleiten oder unterbinden, § 109a Abs. 5 und 6 TKG.

B.1.5.5 Schulung und Sensibilisierung der Mitarbeitenden

Die Mitarbeitenden müssen durch geeignete Schulungsmaßnahmen für die Belange des Datenschutzes und Verschwiegenheitspflichten sensibilisiert werden. Sie trifft eine persönliche Verpflichtung zur Wahrung des Datengeheimnisses (§ 26 DSG-EKD, § 53 BDSG), welche über das Arbeitsverhältnis hinauswirkt.

Daneben sollte eine vertragliche Verpflichtungserklärung zur Wahrung des Datenschutzes von allen tangierten Mitarbeitern abgegeben werden. Dies ist zugleich eine wichtige Maßnahme zur Umsetzung der datenschutzrechtlichen Verantwortung und damit einhergehender Rechenschaftspflichten.[54]

Diese kann sich an dem angefügten Muster orientieren.[55]

B.1.5.6 Profiling

Unter Profiling ist im Allgemeinen die nutzbare Erstellung des Gesamtbildes einer Persönlichkeit für bestimmte Zwecke zu verstehen. Im Sinne des Datenschutzrechtes meint es nach Art. 4 Ziff. 4 DS-GVO bzw. § 5 Ziff. 5 DSG-EKD

„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.

Auch und gerade für das Profiling bedarf es eines Rechtsgrundes. Im vorliegenden Zusammenhang kommt im Wesentlichen nur die Einwilligung in Betracht, die eine umfassende Information bezüglich Zweck und Risiko des Profilings voraussetzt.[56]

In engem Rahmen, soweit dies zur funktionellen Erfüllung eines Vertrages oder eines Dienstes technisch zwingend notwendig ist, können Aspekte eines Profilings auch ohne Einwilligung möglich sein, wobei eine Anonymisierung oder mindestens eine Pseudonymisierung angezeigt sind. Die Informationspflichten sind dabei weiterhin in vollem Umfang zu erfüllen. Zudem sollte eine Opt-out-Möglichkeit bestehen.

Aufgrund des besonderen Risikos, das sich aufgrund des Profilings für die Betroffenen ergeben kann, ist davon im diakonischen Bereich grundsätzlich abzusehen. Ein Einsatz setzt jedenfalls eine eingehende rechtliche Prüfung voraus.

B.1.5.7 Apps und die Nutzung von Cloud-Services

Stellt die App Funktionen zur Verfügung, die die Verarbeitung personenbezogener Daten durch Cloud-Services[57]

[50] Allgemeine Hinweise zur Berichtspflicht nach § 100 Abs. 1 TKG und deren Geltung sind unter www.bundesnetzagentur.de abrufbar.

[51] Zudem haben Diensteanbieter sowohl tatsächlich eingetretene als auch mögliche beträchtliche Sicherheitsverletzungen unverzüglich der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik mitzuteilen. Auf das aktuell gültige Umsetzungskonzept zur Meldung von Vorfällen wird verwiesen (Stand: 10.11.2017, Version: 4.0, ABl. BNetzA Nr. 22 v. 22.11.2017).

[52] Auf die Hinweise der Bundesnetzagentur, abrufbar auf www.bundesnetzagentur.de („Benachrichtigungspflichten im Fall einer Verletzung des Schutzes personenbezogener Daten“ – zuletzt abgerufen am 20. Oktober 2020) wird verwiesen.

[53] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF (zuletzt abgerufen am 20. Oktober 2020).

[54] Siehe Art. 5 Abs. 2, 24 Abs. 1, 28 Abs. 3 Satz 2 b) DS-GVO

[55] Siehe D.2.3: Verpflichtungserklärung (Muster) für Mitarbeitende von Beratungsstellen und D.2.4: Merkblatt zur Wahrung der Vertraulichkeit in der sozialen Arbeit.

[56] Vgl. EuGH, Urteil v. 1.10.2019, Rs. C-673/17 – Planet24 zu einer ähnlichen Problematik beim Einsatz von Cookies, wobei die mit Cookies einhergehende Speicherung auf dem Endgerät des Nutzers noch weitergehende Rechtsfragen aufwirft.

[57] Cloud-Services sind über das Internet verfügbar gemachte IT-Infrastrukturen. Sie ermöglichen Dienste, ohne dass diese auf dem lokalen Rechner installiert sein müssen.

erfordern bzw. auslösen, sind besondere Anforderungen zu erfüllen.

Werden beispielsweise im Rahmen eines eingebundenen Dienstes Daten einem anderem als dem Verantwortlichen offengelegt, wird es sich häufig um eine Auftragsverarbeitung nach Art. 28 DS-GVO/§ 30 DSG-EKD handeln. Dabei ist zu beachten, dass die App-Betreiberin Verantwortliche für die Einhaltung datenschutzrechtlicher Vorgaben bleibt und diese in einem Auftragsverarbeitungsvertrag (AV-Vertrag) inklusive Weisungsrechten gegenüber dem Anbieter der Cloud- oder sonstigen Dienste umfassend sicherzustellen hat. Dabei sind zwingend die Vorgaben aus Art. 28 DS-GVO/§ 30 DSG-EKD zu beachten, insbesondere die Festlegung der organisatorischen und technischen Maßnahmen (TOM) nach Art. 28 Abs. 3 lit. c iVm. Art. 32 DS-GVO/§ 28 Abs. 3 Ziff. 3 iVm. § 27 DSG-EKD.

Liegt dagegen eine eigene Verarbeitung durch einen Empfänger personenbezogener Daten vor, sind die Nutzer*innen gem. Art. 13 Abs. 1 lit. e/f DS-GVO/§ 17 Abs. 1 Ziff. 4 DSG-EKD hiervon zu unterrichten. Dies gilt insbesondere dann, wenn die Übermittlung außerhalb des EWR beabsichtigt ist. Wobei zu beachten ist, dass Letztere – je nach Empfangsstaat – Verboten oder erheblichen Beschränkungen unterliegen kann (siehe C.1.1.1.9.1).[58]

Die Unterrichtung ist nur entbehrlich, wenn und soweit die Nutzer*innen über die Information bereits verfügen oder über entsprechende Optionen in der App dort erzeugte Inhalte wissentlich und selbständig in einem Cloud-Service ablegen, wobei sich diese nicht als integraler Bestandteil des eigenen Dienstes darstellen dürfen.

B.1.6 HEALTH-APPS

Weist die App Bezüge zur Gesundheit der Nutzer*innen auf, so handelt es sich um eine sogenannte Health-App. Bereits 2015 (!) kamen mehr als 100.000 Health-Apps neu auf den Markt und haben 22% der Deutschen Vitalwerte mittels solcher Apps kontrolliert.[59] Sofern Informationen über den körperlichen, geistigen oder seelischen Zustand der Nutzer*innen verarbeitet werden, handelt es sich um die Verarbeitung besonderer Datenkategorien, an die hohe Anforderungen zu stellen sind. Da eine Interessenabwägung als Rechtsgrund per se ausscheidet, ist eine Verarbeitung in aller Regel nur aufgrund einer expliziten, gut informierten und aktiven Einwilligung möglich. Ausnahmen können sich allenfalls für Angehörige eines Gesundheitsberufs ergeben bzw. dann, wenn die Verarbeitung aus Gründen der öffentlichen Gesundheit erforderlich ist (s. B.1.5.2).

Sofern es sich bei der App gar um ein Medizinprodukt iSd. § 3 MPG handelt, zB einer App, die der Erkennung, Überwachung oder Behandlung von Krankheiten dient oder letztere maßgeblich beeinflusst, ist zudem auch das Medizinproduktrecht anwendbar.

B.1.6.1 Vertiefung: Medizinprodukterecht

Der Einsatz von Apps für den Gesundheitssektor (Medical Apps) ist vielfältig. So geben einige nur Gesundheitstipps, andere messen den Herzschlag oder erheben gar Anamnesen und berechnen die Medikation. In Abhängigkeit vom Umfang der Nutzungsmöglichkeiten und deren Auswirkung kann eine Medical App als genehmigungspflichtiges Medizinprodukt einzustufen sein. Das ist insbesondere dann problematisch, wenn die Entwicklerin dies zunächst nicht bemerkt. Dafür ist insbesondere entscheidend, ob die App algorithmusgesteuert in diagnostische oder therapeutische Entscheidungen oder Aussagen eingreift oder diese in sonstiger Weise maßgeblich beeinflusst.

So vielfältig die Einsatzmöglichkeiten sind, so umfassend die Rechtsfragen, die dadurch aufgeworfen werden. Deren Lösung wird zu einem beträchtlichen Teil durch das Medizinproduktrecht geregelt. Zentral ist insoweit das **Medizinproduktegesetz (MPG)**[60], das im Wesentlichen das In-Verkehr-Bringen von Medizinprodukten regelt. Es wird ab 26. Mai 2021 schrittweise durch das Medizinprodukterecht-Durchführungsgesetz abgelöst.[61] Mit sechs Strafvorschriften enthält das Medizinproduktegesetz auch Nebenstrafrecht.

Zur Ausführung des MPG sind mehrere Verordnungen erlassen worden. Zu den wichtigsten zählen die Folgenden: Die **Medizinprodukte-Verordnung (MPV)**[62] regelt die Bewertung und Übereinstimmungsfeststellung bezüglich der Anforderungen des MPG. Hinzu tritt die **Verordnung über klinische Prüfungen von Medizinprodukten (MPKPV)**[63], welche die Rahmenbedingungen von klinischen Prüfungen und genehmigungspflichtigen Leistungsbewertungsprüfungen im Sinne des MPG regelt. Die **Verordnung über die Erfassung, Bewertung und Abwehr von Risiken bei Medizinprodukten (MPSV)**[64] hat zudem zum Ziel, Verfahren für die Erfassung und Bewertung und Abwehr von nach In-Verkehr-Bringung auftretenden Risiken zu normieren. Wichtig ist ferner die **Verordnung über**

[58] Eine Übertragung von personenbezogenen Daten in Staaten, die nicht der EWG angehören, ist eine datenschutzrechtlich komplexe Frage. Insbesondere in die USA ist dies derzeit nur im Rahmen sog. „Standard-Datenschutzklauseln" möglich, wobei auch diesbezüglich weiterhin Fragen ungeklärt sind (siehe EuGH, Urteil v. 16. Juli 2020, Rs. C-311/18 – Facebook Ireland und Schrems). Siehe dazu näher C.1.1.1.9.1.1

[59] Nachweise bei Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rz. 67 zu § 28.

[60] Neugefasst durch Beschluss vom 07. August 2002 BGBl. I S. 3146; zuletzt geändert durch Artikel 223 der Verordnung vom 19. Juni 2020 BGBl. I S. 1328.

[61] Auch an diesem plant die Bundesregierung noch Veränderungen in der laufenden Legislatur.

[62] Verordnung vom 20. Dezember 2001 BGBl. I S. 3854; zuletzt geändert durch Artikel 3 der Verordnung vom 27. September 2016 BGBl. I S. 2203.

[63] Artikel 1 der Verordnung vom 10. Mai 2010 BGBl. I S. 555; zuletzt geändert durch Artikel 11b Gesetzes vom 28. April 2020 BGBl. I S. 960.

[64] Artikel 1 der Verordnung vom 24. Juni 2002 BGBl. I S. 2131; zuletzt geändert durch Artikel 11a Gesetzes vom 28. April 2020 BGBl. I S. 960, 1018.

das Errichten, Betreiben und Anwenden von Medizinprodukten (MPBetreibV)[65], welche Betrieb und Anwendung und Instandhaltung von Medizinprodukten und damit zusammenhängende Tätigkeiten regelt. So finden sich darin Anforderungen an die Hygiene bei der Aufbereitung von Medizinprodukten sowie zur Qualitätssicherung laboratoriumsmedizinischer Untersuchungen. Die Verschreibungspflicht von Medizinprodukten regelt schließlich die **Verordnung zur Regelung der Abgabe von Medizinprodukten (MPAV)**[66,67].

Gemäß der Legaldefinition des § 3 Ziff. 1 MPG sind Medizinprodukte

„alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke

a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
c) der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
d) der Empfängnisregelung

zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann."

Dient also eine Medical App als **Zubehör oder Erweiterung eines bestehenden Medizinproduktes**, zB. indem es dieses **ansteuert oder dessen gemessene Werte anzeigt**, so ist ihre Einstufung als Medizinprodukt im Sinne des MPG wahrscheinlich. Neben der objektiven Komponente ist aber nach der Vorschrift auch die Zweckbestimmung durch die Herstellerin von Belang.[68] Dabei sind auch auf die Gebrauchsinformationen und Werbematerialen (zB. die Bewerbung im App-Store) abzustellen. Insoweit stellt das prüfende Bundesinstitut für Arzneimittelprodukte (BfArM) auch auf „Anhaltsbegriffe" ab. Wird also der Zweck der App mit „Alarmieren", „Analysieren", „Berechnen", „Diagnostizieren", „Feststellen", „Interpretieren", „Messen", „Steuern", „Überwachen", „Verstärken" oder Ähnlichem umschrieben, so spricht die Beschreibung bereits für das Vorliegen eines Medizinproduktes.

Kriterien für die Einstufung als Medizinprodukt	**Kriterien gegen die Einstufung als Medizinprodukt**
Die App dient der Entscheidungsfindung oder entscheidet selbst über therapeutische Maßnahmen	Die App speichert nur Daten
Die App berechnet die Dosierung einer Medikation oder gibt zur Ausführung der selbständigen Berechnung Hinweise	Die App archiviert und verdeutlicht Daten
Die App überwacht den Patienten, etwa indem sie Messwerte sammelt, die Auswirkungen auf die Therapie haben	Die App dient lediglich der Kommunikation
Die App steuert ein Medizinprodukt	Die App dient lediglich der Recherche

Wenn eine App hingegen ausschließlich der Dokumentation dient oder nur Trainings-, Wohlfühl- oder Ausbildungszwecke verfolgt oder nur ein Kommunikationsmittel ist, dürfte sie nicht als Medizinprodukt zu klassifizieren sein. Greift eine App jedoch in Therapien, Medikationen oder Medizinprodukte steuernd ein oder beeinflusst diese maßgeblich, wird die App voraussichtlich als Medizinprodukt einzustufen sein.

Soweit eine App als Medizinprodukt zu klassifizieren ist, gelten besondere rechtliche Bedingungen nach den oben genannten Vorschriften. So bedarf ein Medizinprodukt bei In-Verkehr-Bringung zwingend des CE-Zeichens, § 6 Abs. 1 MPG. Dies setzt voraus, dass es die grundlegenden Anforderungen nach § 7 MPG erfüllt und – gemäß § 6 Abs. 2 MPG – das jeweilige Konformitätsbewertungsverfahren erfolgreich durchlaufen hat. Dieses gewährleistet, dass das Produkt den einschlägigen Sicherheitsanforderungen genügt. Letztere können sich im bloßen Erstellen einer Dokumentation erschöpfen, aber auch erfordern, dass ein vollständiger Qualitäts-

[65] Neugefasst durch Beschluss vom 21. August 2002 BGBl. I S. 3396; zuletzt geändert durch Artikel 9 Verordnung vom 29. November 2018 BGBl. I S. 2034.
[66] Artikel 1 der Verordnung vom 25. Juli 2014 BGBl. I S. 1227; zuletzt geändert durch Artikel 3a Gesetzes vom 10. Februar 2020 BGBl. I S. 148.
[67] Im Rahmen der Tätigkeiten nach MPG ggf. anfallende Gebühren (insbesondere des Genehmigungsverfahrens) werden durch dir Gebührenordnung zum Medizinproduktegesetz und den zu seiner Ausführung ergangenen Rechtsvorschriften (B-KOstV-MPG) geregelt (MP-GEBV vom 27. März 2002, idF. vom 03. November 2014, BGBL, I, S. 1676.
[68] Näher definiert in § 3 Ziff. 10 MPG.

managementprozess etabliert und umgesetzt wird. Dies ist abhängig von der Risikoklasse des Produkts (I, IIa, IIb, III – aufsteigendes Risiko).[69]

Zu Risikoklasse I mit „geringem“ Risiko gehören etwa Mullbinden und Lesebrillen, wogegen etwa Implantate und Herzkatheter dem „sehr hohen“ Risiko der Risikoklasse III angehören. Bei „mittlerem“ Risiko ist Risikoklasse IIa einschlägig; das gilt etwa für Zahnfüllungen und Hörgeräte. Ein „hohes“ Risiko besitzen beispielsweise Röntgengeräte, Infusionspumpen und Intraokularlinsen. Zusammenfassend lässt sich sagen, dass die Konformitätsprüfung umso umfangreicher und anspruchsvoller ausfällt, je größer das gesetzte Risiko ist. Und das Risiko ist umso höher, je mehr die Entscheidung eines Arztes ersetzt wird oder die Gefahr schwerer Gesundheitsschäden besteht. Software, die ein Produkt steuert oder dessen Anwendung beeinflusst, wird automatisch derselben Klasse zugerechnet wie das Produkt.[70]

Mit Geltungsbeginn der **Medical Device Regulation**[71] (MDR) ab 26. Mai 2021 werden die Anforderung an Medical Apps erheblich komplexer. Als europäische Verordnung gilt sie (wie etwa auch die DS-GVO) ohne weiteren Umsetzungsakt in den Mitgliedstaaten der Europäischen Union unmittelbar, wird aber durch nationale Regelungen ergänzt. Medical Apps gelten unter ihrer Ägide im Regelfall als Medizinprodukt (der Risikoklasse 2 oder höher). Eine Amortisierung des durch die erhöhten Anforderungen entstehenden Kostenaufwuchses ist aber über § 33a bzw. § 68a SGB V möglich.

Medical Apps werden durch die MDR ausdrücklich geregelt und grundsätzlich in eine höhere Risikostufe eingeordnet. Ganz ähnlich dem § 3 Ziff. 1 MPG bestimmt Art. 2 Ziff. 1 MDR:

„Medizinprodukt“ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

- Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
- Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
- Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben

und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Erwartbar erweitert wird der Anwendungsbereich des MDR durch Art. 2 Ziff. 2, nach dem konsequenter Weise auch Zubehör eines Medizinprodukts als Medizinprodukt gilt, selbst wenn es an sich kein Medizinprodukt ist, aber von Seiten eines Herstellers als Zubehör eines oder mehrerer Medizinprodukte bestimmt ist. Im Übrigen genügt es, wenn eine App einem der aufgezählten medizinischen Zwecke dient.[72]

In Fortschreibung der bisherigen Praxis stellt die MDR grundlegende Anforderungen an das In-Verkehr-Bringen einer Medical App auf. Kapitel 1 zu Anhang I des MDR bestimmt in seiner Ziff. 1, dass die Apps so ausgelegt sind, dass sie sich unter den erwartbaren Anwendungsbedingungen für ihre Zweckbestimmung eignen. Risiken im Zusammenhang mit möglichen negativen Wechselwirkung zwischen App und IT-Umgebung, in der sie eingesetzt wird, müssen dabei so weit wie möglich, reduziert werden.[73] Ein Laie muss die App in allen Phasen ihrer Anwendung sicher und fehlerfrei bedienen können.[74] Sie müssen sicher und wirksam hergestellt sein und dürfen Sicherheit und Gesundheit der Nutzer*innen und Dritter nicht gefährden. Bei ihrer Herstellung muss dem Stand der Technik entsprochen werden, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind.[75]

Nach Ziff. 3 des Kapitels 1 zu Anhang I des MDR haben die Herstellerinnen ferner ein geeignetes Risikomanagementsystem zu etablieren, umzusetzen, zu dokumentieren und es fortzuschreiben. Nach Ziff. 4 sind Rest- und Gesamtrisiko zu moderieren und müssen unter allen Umständen als akzeptabel anzusehen sein; die Nutzer*innen sind darüber zu informieren. Es ist auch sicherzustellen, dass die Herstellerangaben für die Nutzer*innen gut verständlich sind.[76]

Die App muss nach alledem so konstruiert sein, dass sie trotz eines relativen Unvermögens der Nutzer*innen korrekt und sicher funktioniert oder eine Rückfallebene aufweist, die die Sicherheit unvermögender

[69] Die Einordnung erfolgt aktuell anhand des Anhangs IX der Richtlinie 93/42/EWG, auf die in § 2 Abs. 4a MPG Bezug genommen wird und die das MPG umsetzt.
[70] Anwendungsregel 2.3 des Anhangs IX der Richtlinie 93/42/EWG.
[71] Ursprünglich für Mai 2020 geplant, aufgrund der Corona-Pandemie aber verschoben.
[72] Erwägungsgrund 19 zur MDR.
[73] Ergänzung durch Anhang I, Kapitel 14, Ziff. 14.2d) MDR.
[74] Ergänzung durch Anhang I, Kapitel 2, Ziff. 22.1ff. MDR.
[75] Ergänzung durch Ziff. 17.2 zu Kapitel 2 des Anhangs I des MDR.
[76] Anhang I, Kapitel 2, Ziff. 22.1ff. MDR.

Nutzer*innen gewährleistet. Dass durch eine falsche Handhabung oder Ergebnisinterpretation begründbare Risiko muss so gering wie möglich ausfallen und darf die Grenze des Akzeptablen nicht überschreiten.

Es wurde schon angesprochen, dass die MDR eine veränderte Risikoeinordnung vornimmt. Zwar gehören nach ihr alle nicht-invasiven Produkte grundsätzlich in die Klasse I. Für Software[77] gilt aber nach Regel 11 (6.3) des Kapitel III zu Anhang XIII des MPG unter Umständen eine erhebliche Ausnahme:

„Software, die dazu bestimmt ist, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:

- den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder
- eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse IIb zugeordnet.

Software, die für die Kontrolle von physiologischen Prozessen bestimmt ist, gehört zur Klasse IIa, es sei denn, sie ist für die Kontrolle von vitalen physiologischen Parametern bestimmt, wobei die Art der Änderung dieser Parameter zu einer unmittelbaren Gefahr für den Patienten führen könnte; in diesem Fall wird sie der Klasse IIb zugeordnet.

Sämtliche andere Software wird der Klasse I zugeordnet."

Medical Apps dürften daher ab 26. Mai 2021 häufig der Risikoklasse IIa oder höher angehören.

Neu ist auch, dass alle Medizinprodukte einschließlich Software und Apps zum Zwecke der eindeutigen Identifizierung und Rückverfolgung mit einer zu registrierenden internationalen UDI-Produktkennung („Unique Device Identification") zu versehen sind. Diese ist auf Systemebene zuzuteilen und den Nutzer*innen in einem leicht zugänglichen Fenster und lesbaren reinen Textformat anzuzeigen.[78]

B.1.6.2 Checkliste Medical App

- Im Vorfeld der Entwicklung einer jeden Medical App sollte geprüft werden, welche medizinprodukterechtlichen Vorgaben einzuhalten sind. Dabei sollte auf die zum 26. Mai 2021 durch In-Geltung-Treten der MDR anstehenden Veränderungen geachtet werden.
- Sofern durch die App personenbezogene Daten verarbeitet werden, ist zwingend eine Einwilligung der Nutzer*innen einzuholen und zu dokumentieren. Die Verarbeitung muss in einem Verarbeitungsverzeichnis beschrieben werden. Ebenso muss ggf. darin beschrieben werden, dass eine Übermittlung der Daten stattfindet. In diesen Fällen ist ggf. auf den Abschluss eines Auftragsverarbeitungsvertrages zu achten, der die Einhaltung der datenschutzrechtlichen Vorschriften hinreichend gewährleistet. Auch im Übrigen gelten die Grundsätze und Vorgaben des DS-GVO bzw. DSG-EKG.
- Eine nicht als Medical App geplante Anwendung sollte so beschrieben und dokumentiert werden, dass ihre Klassifikation als Medizinprodukt ausgeschlossen ist
- Soweit eine Medical App Therapieempfehlungen treffen soll, muss vor deren Umsetzung nach aktuellem Stand zwingend eine ärztliche Entscheidung darüber erfolgen.
- Bei gefahrbegründendem Einsatz an Patienten sind versicherungsrechtliche Fragen vorab zu klären.

[77] Gemäß Art. 2 Ziff. 4 MDR hat Software immer als „aktives Produkt" zu gelten.

[78] Anhang VI Teil C Ziffer 6.5.1 MDR.

B.1.7 GESUNDHEITS-DATEN ALS SOZIAL-DATEN IM SINNE DER §§ 67FF. SGB X

Sofern Gesundheitsdaten durch eine qualifizierte, in § 35 SGB I enumerativ aufgelistete Stelle verarbeitet werden, handelt es sich zusätzlich um Sozialdaten iSd § 67 Abs. 1 SGB X. In diesem Fall sind – innerhalb des von der DS-GVO vorgegebenen Rahmens – die besonderen Bestimmungen des Sozialdatenschutzrechts gem. §§ 67ff. SGB X zu beachten.

Die von anderen Stellen – etwa die von privaten Leistungserbringern erhobenen Daten (BSG 10.12.2008 – B 6 KA 37/07 R, BSGE 102, 134) – sind per definitionem **keine Sozialdaten in diesem Sinne.** Sie werden es erst dann zu Sozialdaten, wenn sie in den Herrschaftsbereich des Leistungsträgers gelangt sind.

B.1.8 VERTIEFUNG: DIGITALE-VERSORGUNG-GESETZ (DVG)

Mit dem Digitale-Versorgung Gesetz soll das deutsche Gesundheitssystem an die Bedingungen der Digitalisierung angepasst und so verbesserte Voraussetzungen für digitale Innovationen schaffen. Mit Einführung des Gesetzes haben rund 73 Mio. gesetzlich Versicherte einen Anspruch auf eine Versorgung mit Digitalen Gesundheitsanwendungen (z.B. medizinische Apps), die von Ärzten und Psychotherapeuten verordnet werden können und durch die Krankenkasse erstattet werden. Digitale Gesundheitsanwendungen sollen so in die Regelversorgung überführt werden können. Zugleich setzt das DVG einen Schwerpunkt auf die finanzielle Förderung von Start-ups (Innovationsfonds), die Digitale Gesundheitsanwendungen (DiGA) entwickeln. Des Weiteren sollen die Telematik-Infrastruktur erweitert sowie die Telemedizin gestärkt werden.

Als sogenanntes Artikelgesetz passt das DVG verschiedene Gesetze an, darunter etwa die Bundespflegesatzverordnung und das SGB XI. Vornehmlich aber nimmt das DVG Änderungen am SGB V vor. Dabei sind die folgenden Normen von zentraler Bedeutung:

- § 33a SGB V (Digitale Gesundheitsanwendungen)
- § 68a SGB V (Förderung der Entwicklung digitaler Innovationen durch Krankenkassen)
- § 68b SGB V (Förderung von Versorgungsinnovationen)
- § 134 SGB V (Vergütung digitaler Gesundheitsanwendungen)
- § 139e SGB V (Verzeichnis für digitale Gesundheitsanwendungen)

Der im Rahmen des Innovationsfonds (siehe §§ 92a und b SGB V) entstehende Erfüllungsaufwand wird vollständig durch jährlich von der GKV zur Verfügung zu stellende Mittel in Höhe von € 200 Millionen gedeckt.[79] Auch die PKV ist – mit einem vergleichsweise geringen Beitrag – beteiligt.

B.1.8.1 Digitale Gesundheitsanwendungen, Aufnahme in das Verzeichnis

In § 33s SGB V werden Digitale Gesundheitsanwendungen (DiGA) legaldefiniert. Davon umfasst ist reine Software wie auch auf anderen Technologien basierende Medizinprodukte mit gesundheitsspezifischer Zweckbestimmung. Der Gesetzgeber erhofft sich durch Etablierung der DiGA eine deutliche Verbesserung der Versorgung und die Sensibilisierung für eine gesundheitsförderliche Lebensführung, und zwar insbesondere durch Gesundheits-Apps (Medical Apps). Dies ist für Start-ups interessant, da der Rechtsanspruch auf Versorgung und die Klärung der Vergütungsfragen viele typische Gründer-Schwierigkeiten gelöst hat.

Von den bislang auf dem Markt befindlichen herkömmlichen Untersuchungs- und Behandlungsmethoden unterscheiden sich die DiGA durch

- ihren digitalen Charakter,
- hohe Individualisierung,
- modulare Erweiterbarkeit und
- einen schnellen Innovations- und Entwicklungszyklus bei
- geringem Risikopotenzial.[80]

Die beiden letztgenannten Punkte sind quasi als Junktim zu lesen. Denn Digitale Gesundheitsanwendungen sind aufgrund ihres hohen Innovationsrhythmus der klassischen Methodenbewertung nicht zugänglich, was nur im Falle untergeordneter Risiken unbeachtlich bleiben kann. Mit Anwendung der Medical Device Regulation (MDR) zum 26. Mai 2021[82] ändert sich aber die Risikoklassifizierung, da Medical Apps unter die Risikoklassen IIa, IIb oder gar III fallen. Erfolgt eine

[79] Dies entspricht einer Reduktion um ein Drittel, da seit 2016 ursprünglich eine Förderungsmöglichkeit von bis zu € 300 Millionen vorgesehen war.
[80] Siehe BT-Drucksache 19/13438, S. 43.
[81] Veränderung des Datums aufgrund der Corona-Pandemie durch den Vorschlag der Kommission „zur Änderung der Verordnung (EU) 2017/745 über Medizinprodukte hinsichtlich des Geltungsbeginns einiger ihrer Bestimmungen".
[82] Medical Device Directive [Medizinprodukte-Richtlinie] 93/42/EWG.

Höherstufung der Risikoklasse von MDD -Klasse I zu MDR-Klasse IIa ist die Anwendung weiter als DiGA zulässig, sofern unter Einbezug der Übergangsvorschriften eine gültige CE-Zertifizierung vorliegt. Erfolgt jedoch eine Höherstufung in Risikoklasse IIb oder höher, erfüllt die Anwendung nicht mehr die Grundanforderungen und wäre damit keine DiGA gemäß DVG mehr.

Das Bundesinstitut für Arzneimittel (BfArM) ist die Aufgabe übertragen, ein amtliches Verzeichnis erstattungsfähiger DiGA zu führen, in das die Anwendung nach erfolgreicher Durchführung eines entsprechenden Verwaltungsverfahrens, dh. insbesondere bei Vorliegen „positiver Versorgungseffekte“,[83] aufzunehmen ist. Falls für die DiGA noch keine ausreichenden Nachweise für positive Versorgungseffekte vorliegen, aber die weiteren Anforderungen erfüllt sind, kann der Hersteller auch einen Antrag auf vorläufige Aufnahme in das Verzeichnis stellen und die notwendige vergleichende Studie innerhalb einer Erprobungsphase von bis zu einem Jahr – in Ausnahmefällen bis zu zwei Jahren – durchführen. Gemäß § 139e Abs. 3 SGB V hat das BfArM binnen drei Monate nach (elektronischem) Eingang des vollständigen Antrags über die Aufnahme zu entscheiden („Fast Track“).

Für Anwendungen ist womöglich wichtig, ob der Genehmigungsbescheid eine ärztliche Hilfeleistung zur Nutzung der Anwendung festlegt **(Arztvorbehalt)**. Das kann für das Ausrollen der Anwendung kritisch sein und das Nachschießen von Gründungskapital erforderlich machen. Mit der Aufnahme in das Verzeichnis sind alle Kostenträger zur Kostenerstattung verpflichtet, so dass Einzelverhandlungen nicht notwendig sind.

Voraussetzungen für die Aufnahme sind im Wesentlichen die folgenden drei Punkte:

1. Die DiGA muss bestimmte Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität und
2. spezifische Anforderungen des Datenschutzes und der Datensicherheit erfüllen sowie
3. einen positiven Versorgungseffekt84 aufweisen.

Allgemein lässt sich sagen, dass der Verzicht auf hohe Evidenzanforderungen und damit die Aufnahme in das Verzeichnis umso wahrscheinlicher wird, je geringer potenzielles Risiko und Kosten der Anwendung ausfallen. Auch mittelbare Faktoren wie etwa die Sicherstellung der Sachrichtigkeit der Inanspruchnahme einer bestimmten Behandlungsmethode oder die Sicherstellung

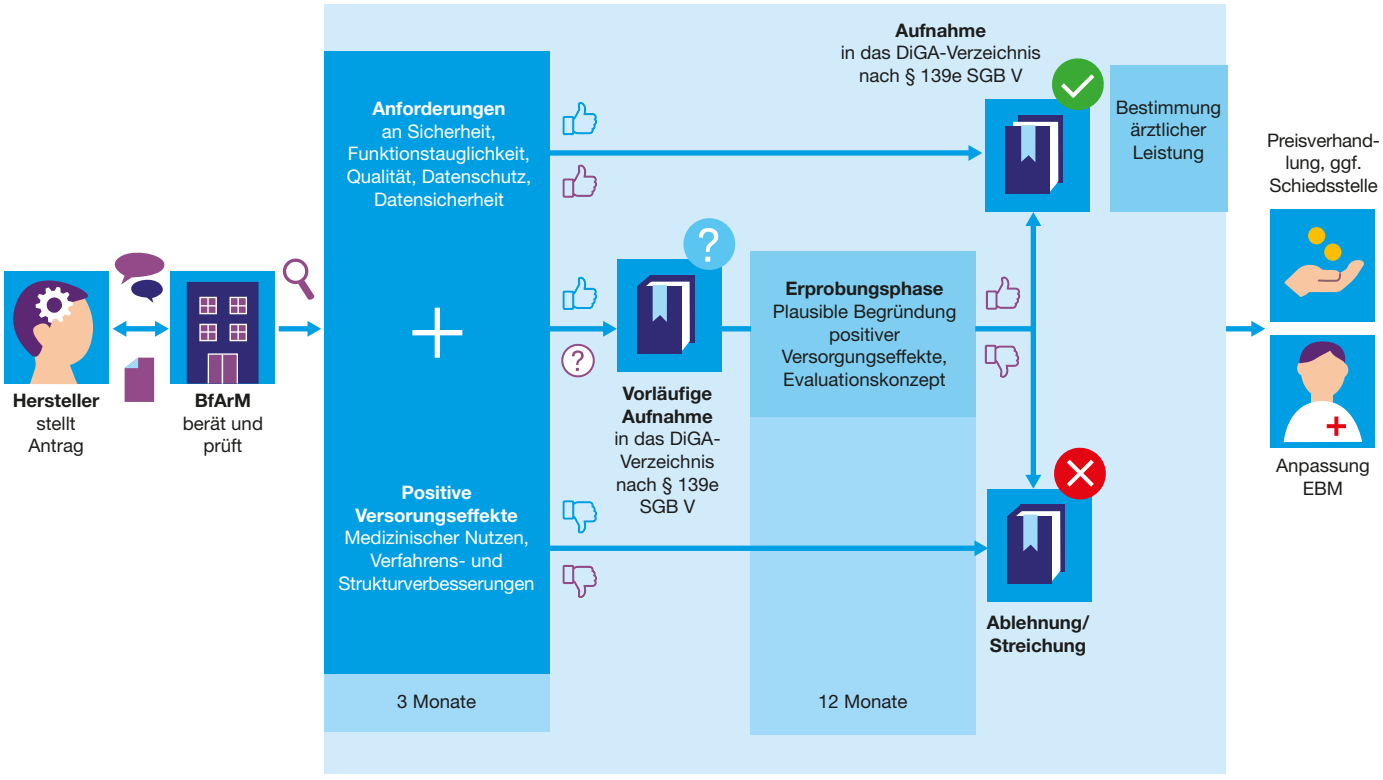


Fig B.2: Fast-Track-Verfahren; Quelle: BfArM

[83] Die Details zum Antragsverfahren, zu den Anforderungen an die DiGA und zur Ausgestaltung des DiGA-Verzeichnisses hat das Bundesministerium für Gesundheit (BMG) mit der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) umfassend geregelt. Ein Leitfaden des BfArM gemäß § 139e Absatz 8 Satz 1 Fünftes Buch Sozialgesetzbuch (SGB V) zum Antrags- und Anzeigeverfahren interpretiert diese Rechtsverordnung und ergänzt die Details zu den konkret zu durchlaufenden Verfahren beim BfArM: https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Beratungsverfahren/DiGA-Leitfaden.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 25. Juni 2020).gelten.

[84] Einzelheiten zur Definition des positiven Versorgungseffekts wie auch zu den weiteren vorgenannten Punkten finden sich in dem in der vorherigen Fußnote angegebenen Leitfaden des BfArM.

einer zweckgerichteten Koordinierung des Versorgungsablaufs, die Förderung der Patienteninformation und -souveränität uÄ. können die Annahme eines positiven Versorgungseffekts und damit die Erstattungsfähigkeit der DiGA begründen. Wesentliche Veränderungen einer DiGA sind anzeigepflichtig.

B.1.8.2 Vergütung

DiGA werden von den Krankenkassen im ersten Jahr grundsätzlich nach dem vom Hersteller festgelegten Abgabepreis vergütet. Die Vergütung für die Folgezeit wird zwischen dem Spitzenverband Bund der Krankenkassen mit den Herstellerinnen vereinbart, § 134 Abs. 1 SGB V. Der Herstellerin bleibt es aber unbenommen, über die vereinbarte Vergütung hinausgehende Preisanteile zu verlangen, die dann von den Versicherten selbst zu tragen sind.

B.1.8.3 Innovationsförderung

Auszug aus § 68a SGB V – Förderung der Entwicklung digitaler Innovationen durch Krankenkassen:

(1) Zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung können Krankenkassen die Entwicklung digitaler Innovationen fördern. Die Förderung muss möglichst bedarfsgerecht und zielgerichtet sein und soll insbesondere zur Verbesserung der Versorgungsqualität und Versorgungseffizienz, zur Behebung von Versorgungsdefiziten sowie zur verbesserten Patientenorientierung in der Versorgung beitragen.

(2) Digitale Innovationen im Sinne des Absatzes 1 sind insbesondere
1. digitale Medizinprodukte,
2. telemedizinische Verfahren oder
3. IT-gestützte Verfahren in der Versorgung.

Die durch § 68a SGB V neu geschaffene Möglichkeit der gezielten Innovationsförderung im digitalen Sektor zielt darauf ab, die Krankenkassen als Kostenträger aktiv in die versorgungsnahe und bedarfsgerechte Entwicklung innovativer DiGA einzubeziehen. Bei einer Förderung sind jedenfalls das Wettbewerbsrecht, Beihilferecht und das Haushaltsrecht zu beachten. Voraussetzung ist ferner, dass zwischen der Krankenkasse und der Förderpartnerin ein Kooperationsvertrag geschlossen wird, der eine Kapitalbindungsdauer von maximal zehn Jahren vorsieht und so ausgestaltet sein muss, dass eine Rückzahlung des Investments realistisch erscheint und ein angemessener Ertrag zugunsten der fördernden Krankenkasse zu erwarten ist.[85]

Neben der Förderung nach § 68a SGB V ist auch eine Förderung nach § 68b SGB V denkbar.

Auszug aus § 68b – Förderung von Versorgungsinnovationen

(1) Die Krankenkassen können Versorgungsinnovationen fördern. Diese sollen insbesondere ermöglichen,
1. die Versorgung der Versicherten anhand des Bedarfs, der aufgrund der Datenauswertung ermittelt worden ist, weiterzuentwickeln und
2. Verträge mit Leistungserbringern unter Berücksichtigung der Erkenntnisse nach Nummer 1 abzuschließen.

Ein Eingreifen in die ärztliche Therapiefreiheit oder eine Beschränkung der Wahlfreiheit der Versicherten im Rahmen von Maßnahmen nach Satz 1 ist unzulässig. Für die Vorbereitung von Versorgungsinnovationen nach Satz 1 und für die Gewinnung von Versicherten für diese Versorgungsinnovationen können Krankenkassen die versichertenbezogenen Daten, die sie nach § 284 Absatz 1 rechtmäßig erhoben und gespeichert haben, im erforderlichen Umfang auswerten. […]

Die Förderung nach § 68b SGB V zielt anders als nach § 68a SGB V nicht auf eine finanzielle Förderung von DiGA ab. Ergänzend will der Gesetzgeber vielmehr Krankenkassen unabhängig von den Befugnissen nach § 68a „als Treiber für digitale Versorgungsinnovationen bzw. als Gestalter digital gestützter Versorgungsprozesse stärken“ und eröffnet ihnen „erweiterte Freiräume für die Ableitung von Versorgungsbedarfen, für die individuelle Kommunikation von Angeboten an die Versicherten und für Datenanalysemöglichkeiten“. Derart ergänzende Angebote an Versicherte, die besonderen Unterstützungsbedarf haben, könnten wichtige zusätzliche Impulse für die Fortentwicklung der Versorgung bringen.[86] Die Vorschrift will – bei nach § 68b SGB V vorausgesetzter Einwilligung der Versicherten – Big Data-Analysen mit Einwilligung der Versicherten zur Ermittlung deren Unterstützungsbedarfs ermöglichen, um ihnen sodann basierend auf umfassender Beratung zielgerichtet individuell angepasste und mit Leistungserbringerinnen selektivvertraglich vereinbarte innovative Versorgungsmaßnahmen anzubieten. Damit schafft die Norm zugleich die Möglichkeit für die einzelne Kasse, sich im Wettbewerb mit den weiteren Kassen zu profilieren.[87]

Hinweis:
Mit dem Digitale-Versorgung und Pflege-Modernisierungs-Gesetz (DPVMG) wird der Gesetzesrahmen

[85] Jorzig, Sarangi, Digitalisierung im Gesundheitswesen, 2020, S. 48f.
[86] BT-Drs. 19/13438, S. 47.
[87] Scholz, in Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), BeckOK Sozialrecht, 56. Ed., 2020, Rz. 1 zu § 68 b.

alsbald weiter geschärft. Neben dem Ziel der Weiterentwicklung von E-Rezept und elektronischer Patientenakte sowie dem Ausbau der Telemedizin tritt es insbesondere auch dazu an, die Versorgung mit digitalen Gesundheitsanwendungen weiter auszubauen. Aller Voraussicht nach wird es die Anforderungen an Datenschutz und Datensicherheit weiter konkretisieren und eine mit dem Bundesamt für Sicherheit in der Informationstechnik abgestimmte Sicherheitsprüfung sowie eine Schweigepflicht für Hersteller digitaler Gesundheitsanwendungen einführen.

B.1.9 EXKURS E-HEALTH-GESETZ

Das als E-Health[88]-Gesetz bekannt gewordene Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze[89] ändert als Artikelgesetz im Wesentlichen Vorschriften des SGB V und regelt so einen wesentlichen Teilbereich möglicher Gesundheitsanwendungen im Bereich der gesetzlichen Gesundheitsversorgung. Es gibt insoweit einen konkreten Fahrplan für den Aufbau der sicheren Telematikinfrastruktur, die Akteure des öffentlichen Gesundheitswesens miteinander informationstechnisch verbindet, sowie die Einführung medizinischer Anwendungen vor. Die Organisationen der Selbstverwaltung erhalten darin klare Vorgaben und Fristen, die bei Nichteinhaltung teilweise auch zu Sanktionen führen.

Die Schwerpunkte der Regelungen sind:

- Anreize schaffen für die zügige Einführung und Nutzung medizinischer Anwendungen (modernes Versichertenstammdatenmanagement, Notfalldaten, elektronischer Arztbrief und einheitlicher Medikationsplan),
- die Telematikinfrastruktur öffnen und perspektivisch als die maßgebliche und sichere Infrastruktur für das deutsche Gesundheitswesen entwickeln,
- die Erstellung eines Interoperabilitätsverzeichnisses zur Verbesserung der Kommunikation verschiedener IT-Systeme im Gesundheitswesen,
- die Förderung telemedizinischer Leistungen (Online-Videosprechstunde, telekonsiliarische Befundbeurteilung von Röntgenaufnahmen).

Gerade der letzte Punkt macht deutlich, dass damit die Voraussetzungen dafür geschaffen werden, dass die Bürger*innen einen erleichterten und zeitgemäßen Zugang zur gesundheitlichen Versorgung erlangen. Dies soll ihnen dabei helfen, sich mehr und mehr „compliant“ mit gesundheitlichen Notwendigkeiten zu verhalten, insbesondere einem ggf. gegebenen Therapieplan folgen zu können, um eine schnelle Genesung zu erreichen. Hiermit ist der weite Bereich des **„Patienten-Empowerment“** angesprochen.

Eine wesentliche Rolle für die Vernetzung des öffentlichen Gesundheitsbereichs spielt die gesetzlich bestimmte (§§ 291a ff. SGB V) Gesellschaft für Telematik (gematik GmbH)[90], die die weiteren Regelungen zur Telematikinfrastruktur trifft und deren Aufbau und Betrieb übernimmt.

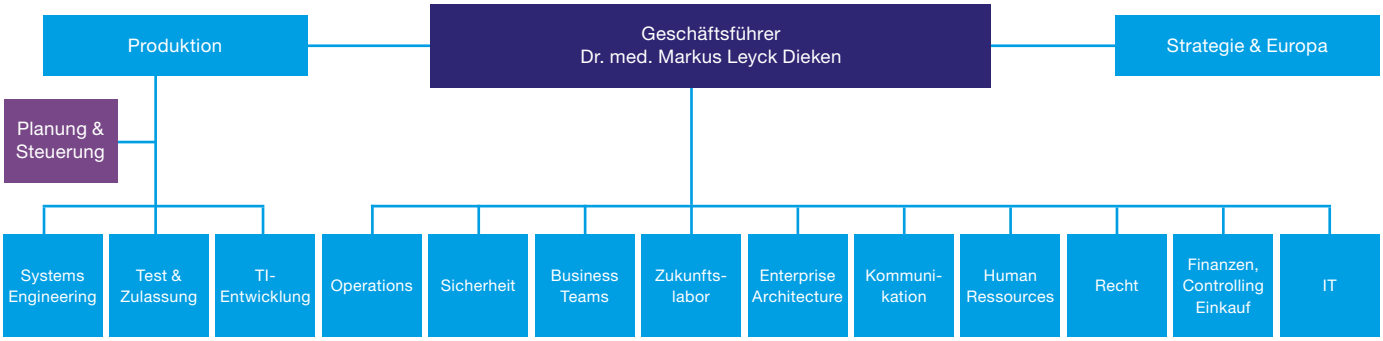


Fig. B.3: Übersicht über die Organisation der gematik GmbH; Quelle: gematik GmbH

[88] Eine allgemeine Definition von E-Health ist nicht existent. Einen guten Anhaltspunkt liefert das Verständnis des Bundesministeriums für Gesundheit (BMG): „Unter E-Health fasst man Anwendungen zusammen, die für die Behandlung und Betreuung von Patientinnen und Patienten die Möglichkeiten nutzen, die moderne Informations- und Kommunikationstechnologien (IKT) bieten. E-Health ist ein Oberbegriff für ein breites Spektrum von IKT-gestützten Anwendungen, in denen Informationen elektronisch verarbeitet, über sichere Datenverbindungen ausgetauscht und Behandlungs- und Betreuungsprozesse von Patientinnen und Patienten unterstützt werden können […]“, https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health.html (zuletzt abgerufen am 03. Juli 2020).

[89] Gesetz vom 21. Dezember 2015, BGBl. I S. 2408 (Nr. 54).

[90] Die Gesellschafter der Gematik sind das Bundesministerium für Gesundheit (BMG), die Bundesärztekammer (BÄK), die Bundeszahnärztekammer (BZÄK), der Deutsche Apothekerverband (DAV), die Deutsche Krankenhausgesellschaft (DKG), der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV-SV), die Kassenärztliche Bundesvereinigung (KBV) und die Kassenzahnärztliche Bundesvereinigung (KZBV). Der Bund hält (derzeit) 51% der Geschäftsanteile, der GKV-Spitzenverband 24,5%.

Bei der Telematikinfrastruktur handelt es sich um eine als „geschlossenes Netz“ konzipierte Infrastruktur, der nur registrierte und fachlich qualifizierte Akteure des Gesundheitswesens beitreten können. Es begründet die Vernetzung verschiedener informationstechnischer Systeme und die technische Möglichkeit, Informationen aus verschiedenen Quellen zu verknüpfen. Die Akteure des Gesundheitswesens sollen dadurch effektiv und sicher miteinander kommunizieren können.

Die für die Vernetzung notwendigen technischen Komponenten umfassen den **Konnektor**, der den Zugang zur Infrastruktur überhaupt ermöglicht; das **Kartenterminal**, über das die Authentifizierung der Anwender*innen mittels des **Praxisausweises** erfolgt; den VPN-Zugangsdienst sowie die **Anpassung des Praxisverwaltungssystems**, dass die Einbindung des Zugangs in die Praxisverwaltung begründet.

Komponenten und Dienste der Telematikinfrastruktur müssen von der gematik GmbH zugelassen werden, was dieser eine umfassende Steuerungsmöglichkeit einräumt. Dabei ist einem transparenten Kriterienkatalog zu entsprechen, nach dem die Funktionsfähigkeit, Interoperabilität und Sicherheit der Dienste und Komponenten überprüft wird.[91]

Hinweis:
Auch im Hinblick auf die Telematik-Infrastruktur wird das Digitale-Versorgung und Pflege-Modernisierungs-Gesetz (DPVMG) aller Voraussicht nach Veränderungen mit sich bringen. So sollen namentlich deren Nutzungsmöglichkeiten erweitert und ihre Nutzung anwendungsfreundlicher gestaltet werden. So soll zum Zweck der Entlastung der Leistungserbringer von der in der Datenschutz-Grundverordnung vorgesehenen Möglichkeit Gebrauch gemacht werden, eine Datenschutz-Folgenabschätzung bereits im Rahmen des Gesetzgebungsverfahrens durchzuführen.

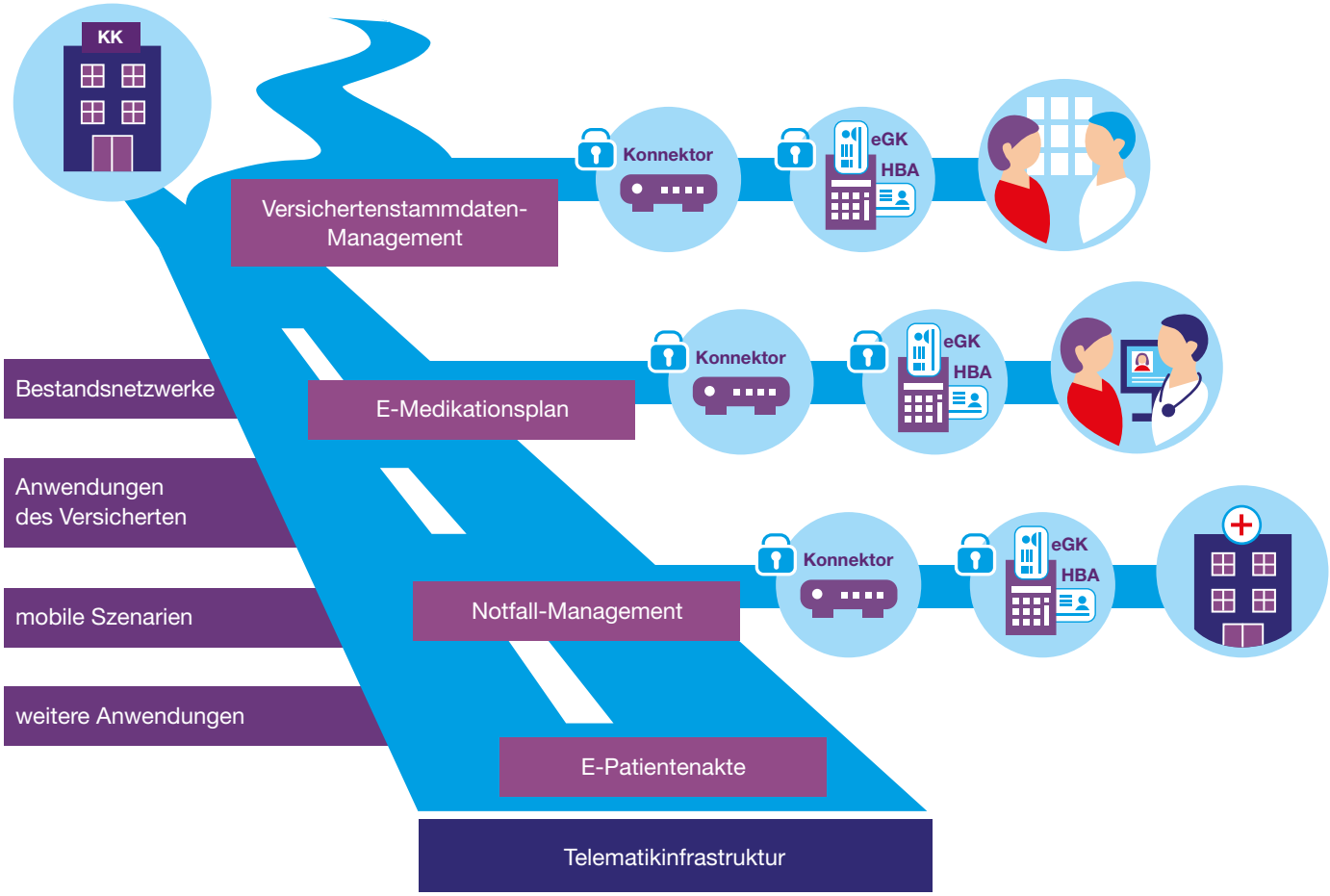


Fig. B.4: Schaubild zur Telematikinfrastruktur; Quelle: gematik GmbH

[91] Siehe dazu die Hinweise unter https://fachportal.gematik.de/spezifikationen/ (zuletzt abgerufen am 03. Juli 2020).

B 1.10 CHECKLISTE APPS

- Ist geprüft, ob sich die Umsetzung als App für die Dienstleistung überhaupt hinreichend eignet (beispielsweise sind volle Vertraulichkeit und Anonymität eher webbasiert herstellbar)?
- Ist geprüft, welches Recht für die Beziehungen zur App-Store-Betreiberin und User*innen zur Anwendung gelangt und sind die daraus resultierenden Vorkehrungen getroffen bzw. Konsequenzen gezogen worden?
- Wird den geltenden Informationspflichten (zB. Anbieterkennzeichnung/Impressum) nachgekommen?
- Werden User*innen über das ihnen zustehende Widerrufsrecht aufgeklärt (Hinweis auf das Widerrufsrecht, die Widerrufsbelehrung sowie Link zum Widerrufsformular) und alle sonstigen vor und nach Vertragsabschluss bestehenden Informationspflichten erfüllt?
- Sind alle Vorkehrungen getroffen, um einer möglichen Mängelhaftung vorzubeugen?
- Sind alle Fragen der Rechtsinhaberschaft geklärt? Können den Nutzer*innen alle Nutzungsrechte an der App vorbehaltslos eingeräumt werden?
- Sind alle im Einzelfall möglichen lauterkeitsrechtlichen Probleme ausgeräumt, vor allem Irreführungen über Kosten, Funktionen und Leistungen der App ausgeschlossen?
- Ist jede Verarbeitung personenbezogener Daten durch einen Rechtsgrund und nötigenfalls durch eine Einwilligung hinreichend abgesichert?
- Sind besondere Rechtsgründe für eine ggf. erfolgende Verarbeitung personenbezogener Daten besonderer Kategorien iSd. Art. 9 DS-GVO/§ 13 DSG-EKD sichergestellt?
- Ist eine ggf. notwendige Einwilligung in die Verarbeitung personenbezogener Daten besonderer Kategorien und ihre ausreichende Dokumentation sichergestellt?
- Sind die Voraussetzungen für die Wirksamkeit einer solchen Einwilligung (inkl. der Besonderheiten bei Minderjährigen) gewahrt?
- Werden die datenschutzrechtlichen Informationspflichten eingehalten? Werden dabei die Besonderheiten der Datenverarbeitung in allen in Betracht kommenden Einzelfällen berücksichtigt?
- Halten die Informationen auch der AGB-rechtlichen Überprüfung stand?
- Werden die umfassenden Pflichten nach TKG für evtl. Telekommunikationsdienste eingehalten?
- Sind die betreffenden Mitarbeitenden ausreichend geschult und sensibilisiert und zur Geheimhaltung verpflichtet?
- Ist ein Profiling ausgeschlossen bzw. erfolgt es nur unter seinen sehr engen, besonderen Voraussetzungen?
- Sind die besonderen Voraussetzungen bei Nutzung eines Cloud-Services eingehalten, insb. Auftragsverarbeitungsverträge inkl. Weisungsrechten und TOM abgeschlossen?
- Sind ggf. die Vorgaben des Medizinprodukterechts eingehalten?
- Sind ggf. die an eine DiGA zu stellenden Anforderungen erfüllt?

B.2 ONLINE-PLATTFORMEN

Die für digitale Märkte prägenden Unternehmen sind überwiegend Plattformen. Im hier interessierenden Zuschnitt handelt es sich bei einer Online-Vermittlungsplattform um eine internet- (und algorithmen-)basierte technische Infrastruktureinrichtung, auf der Anbieterinnen von Dienstleistungen diese entweder kostenfrei oder gegen ein Entgelt einstellen oder in sonstiger Weise auf ihr Leistungsangebot aufmerksam machen. Interessierten Nutzer*innen werden diese Angebote angezeigt und können über die Plattform in einen direkten Kontakt mit den Dienstleistern treten oder mit ihnen sogar ein Vertragsverhältnis begründen. Der entsprechende Vertrag kommt als zweiseitige Vereinbarung (also ohne weitere Einbindung der Plattformbetreiberin) unmittelbar zwischen diesen Parteien zustande.

B.2.1 VERTRAGSRECHTLICHES

Sofern die Online-Plattform lediglich die Leistungen anderer Diensterbringer hostet, entsteht eine dreiecksartige Leistungsbeziehung.

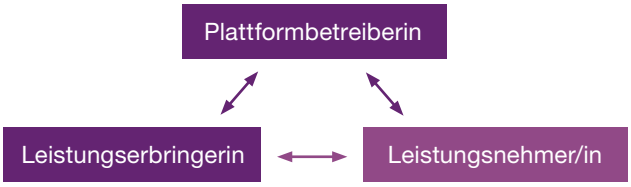


Fig. B.5: Vertragsverhältnisse bei Angebot einer Dienstleistung über eine Online-Plattform

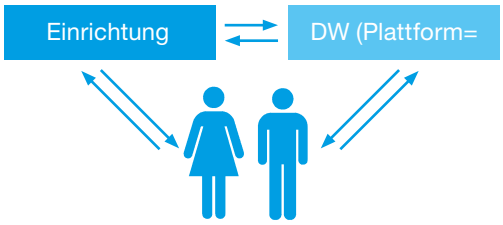


Fig. B.6: Beispiel der Zur-Verfügung-Stellung einer Online Plattform durch ein diakonisches Werk, auf der Einrichtungen ihre Dienste bewerben

Die Diagramme verdeutlichen, welche Vertragsbeziehungen wichtig sind. Für ihre rechtliche Einordnung und die Bestimmung der Vertragsinhalte kommt es auf die konkrete Gestaltung im Einzelfall an. Daher kann hier nicht auf die allgemeine Vertragsgestaltung zwischen Leistungserbringerinnen und Leistungsnehmerinnen eingegangen werden. Allerdings kann ein Überblick gegeben werden, welche Punkte regelmäßig zu bedenken sind.

Zu unterscheiden sind die Vertragsbeziehungen zwischen der Plattformbetreiberin und der Leistungserbringerin (1), der Plattformbetreiberin und der/dem Leistungsnehmer/in (2) sowie der Leistungserbringerin und der/dem Leistungsnehmer (3):

1. Zwischen der Plattformbetreiberin und der Leistungserbringerin

- Zur Erfüllung der eigenen Sorgfaltspflicht ist die Sicherstellung einschlägiger [fachlicher] Standards mit den Anbietern zu vereinbaren, und dass sie sich an alle einschlägigen rechtlichen Vorgaben halten.
- Die Plattform nach der vorgegebenen bzw. vereinbarten Bestimmung und nicht zu nicht vereinbarten Zwecken zu nutzen.
- Sind die Regelungen zur gemeinsamen Verantwortlichkeit, Art. 26 DS-GVO, § 29 DSG-EKD ausreichend berücksichtigt und vertraglich ausgestaltet,[92] oder liegen sogar Konstellationen einer Auftragsverarbeitung vor, die durch AV-Verträge[93] abzusichern sind?
- Allgemeine Geschäftsbedingungen (AGB) und deren Änderungen sowie die bestehenden Informationspflichten sind nachvollziehbar zu gestalten. Ferner dürfen AGBs nicht rückwirkend geändert werden.
- Es sind die Informationen zur Kündigung oder Beendigung der Dienste durch die Plattformbetreiberin klar darzustellen.
- Für den Fall des fortgesetzten und nicht unerheblichen Verstoßes gegen die vorgenannten Pflichten und die allgemeinen vertraglichen Treuepflichten ist die Auslistung vorzubehalten.
- Daneben ist eine Haftungsfreistellung für den Fall zu vereinbaren, dass die Plattformbetreiberin von einem Dritten (einer Nutzerin/einem Nutzer) für einen Umstand in Anspruch genommen wird, der dem Verantwortungskreis der Leistungserbringerin obliegt.
- Ranking-Parameter sind ggf. offenzulegen (Bekanntgabe des Algorithmus ist aber nicht erforderlich); ebenso der Umfang, die Art und Bedingungen des Zugriffs auf bestimmte Datenkategorien und deren Nutzung durch die Plattformbetreiberin.
- Es ist ein leicht zugängliches, transparentes und kostenfreies internes Beschwerdemanagementsystem sowie eine Teilnahmemöglichkeit an externen außergerichtlichen Streitbeilegungsmechanismen (Mediation) einzurichten.

2. Zwischen der Plattformbetreiberin und der/dem Leistungsnehmer/in

- Die Plattformbetreiberin sollte bereits bei der Gestaltung der Plattform sicherstellen, dass für die Nutzer*innen die Vertragspartner klar erkennbar sind. Erbringt die Plattformbetreiberin etwa die auf der Plattform beworbenen Dienstleistungen nicht selbst, ist der jeweilige Vertragspartner klar herauszustellen.
- Werden nur Leistungen vermittelt, so ist eindeutig klarzustellen, dass die Betreiberin der Plattform selbst mit den Nutzer*innen – abgesehen von der Vermittlung – in keine

[92] Siehe hierzu B.2.2.4.3.4.
[93] Siehe hierzu C.1.1.1.5.1.3.

eigene Vertragsbeziehung eintreten wird. Dies nur in den AGB/Nutzungsbedingungen zu tun, dürfte nicht ausreichend sein.
- Auch ist herauszustellen, dass die Plattform ggf. keinen vollständigen Überblick über den Markt gibt, sondern nur einen Auszug daraus – etwa die diakonischen Einrichtungen – vermittelt.
- Deklaratorisch sollte darauf hingewiesen werden, dass die Haftung für Fehlleistungen der Leistungserbringer ausgeschlossen ist, soweit kein eigenes Verschulden die Fehlleistung begründet hat.
- Soweit den Leistungserbringern vorvertragliche Aufklärungs- und Beratungspflichten obliegen, empfiehlt es sich, der Erfüllung dieser Pflichten – soweit möglich – bereits auf der Online-Plattform nachzukommen, um einer ggf. möglichen Sachwalterhaftung schon im Ansatz zu begegnen. Daneben sollten bereits auf der Plattform die notwendigen Datenschutzhinweise gegeben werden. Ggf. sind datenschutzrechtliche Einwilligungen einzubinden, soweit die Leistungsnehmerinnen im Falle eines Vertragsabschlusses mit einer Leistungsanbieterin personenbezogene Daten über die gesetzlichen Erlaubnistatbestände (siehe dazu B.1.5.2) hinaus hergeben.
- Je nach dem Grad der Kooperation zwischen Plattformanbieterin und Leitungserbringern kann die Tätigkeit der Plattformanbieterin als Auftragsverarbeitung[94] iSv. Art. 4 Nr. DS-GVO, § 4 Nr. 10 DSG-EKD einzuordnen sein. In diesem Fall hat die Datenverarbeitung der Plattformbetreiberin unter Aufsicht und ggf. Weisung der Leistungsnehmerin stattzufinden, was durch einen Auftragsverarbeitungsvertrag (AV-Vetrag) iSv. Art. 28, 29 DS-GVO, § 30 DSG-EKD abzusichern ist (siehe C.1.1.1.5.1.3).
- Im Rahmen eines Shopsystems ist der Bestellprozess zudem an den Vorgaben von §§ 312i ff. BGB auszurichten.
- Mit Umsetzung der Modernisierungs-Richtlinie (EU) 2019/2161 sind von Online-Marktplätzen gegenüber Verbraucher*innen neue Hinweispflichten zu erfüllen zB. bzgl. der wesentlichen Kriterien eines Rankings von Suchergebnissen oder Preisen, die aufgrund automatischer Entscheidungen personalisiert wurden.

3. Zwischen der Leistungserbringerin und der/dem Leistungsnehmer/in

- Das Vertragsverhältnis sollte klar ausgestaltet sein. So kann durch die allgemeinen Leistungsbeschreibungen auf der Plattform oder der verlinkten Website eine konkrete Leistungsbeschreibung erfolgen.
- Sofern der Leistungserbringerin hinsichtlich der avisierten Leistung besondere vorvertragliche Aufklärungs- und Beratungspflichten obliegen, ist diesen umfassend vor Abschluss des Vertrages nachzukommen. Hinzukommen die allgemeinen Informationspflichten vor und nach Vertragsschluss, wie sie für Fernabsatzverträge und/oder Verbraucherverträge gelten.[95]
- Diese Beschreibung kann durch **verständliche Nutzungsbedingungen** ergänzt bzw. konkretisiert werden.[96] Daneben ist frühzeitig, sofern personenbezogene Daten verarbeitet werden sollen, insbesondere an die Datenschutzinformation und nötigenfalls datenschutzrechtliche Einwilligungen zu denken.

Vertragsschluss mit dem/der Leistungsnehmer/in/Nutzer*innen

An einen Vertragsschluss selbst sind besondere Anforderungen zu stellen. Den Nutzer*innen muss eindeutig verdeutlicht werden, wenn es dazu kommt (Gebot der Transparenz). Sind die Leistungsnehmer*in Verbraucher*innen, so ist die entgeltpflichtige Bestellsituation und insbesondere der Bestellbutton zwingend so zu gestalten, dass die Verbraucher*innen mit ihrer Bestellung ausdrücklich bestätigen, dass sie sich zu einer Zahlung verpflichten (§ 312j Abs. 3 BGB)

Sämtliche wesentlichen Vertragsinhalte müssen – unter gleichzeitiger Zurverfügungstellung aller Pflichtinformationen, AGBs, Widerrufsbelehrungen gegenüber Verbraucher*innen und Datenschutzhinweise[97] – zudem so dargestellt sein, dass sie für die Nutzer*innen unmittelbar verständlich sind.

Für den Vertragsinhalt und die Vertragsbeziehung zwischen Anbieterin und Nutzer*innen sind Auftritt und Darstellung der Anbieterin von entscheidender Bedeutung, da sich hieraus wesentliche Konsequenzen für den Vertragsinhalt ergeben können. Was auf der Website formuliert wird, prägt den Erwartungshorizont der Interessent*innen.

B.2.2 GESETZLICHE ANFORDERUNGEN

B.2.2.1 Verordnung (EU) 2019/1150 zu Fairness und Transparenz (Platform-to-Business oder P2B-VO)

B.2.2.1.1 Allgemeines

Im Juli 2020 trat die sogenannte P2B-VO in Kraft, die als Verordnung keiner Umsetzung in nationales Recht bedarf und so zwischen den Beteiligten unmittelbar wirkt. Die VO soll für Fairness und Transparenz für gewerbliche Nutzerinnen von Online-Vermittlungsdiensten sorgen. In erster Linie geht es dabei um den Schutz gewerblicher Nutzer, also von Anbieterinnen von Produkten oder Dienstleistungen, die die Leistungen einer Plattformbetreiberin in Anspruch nehmen. Sie sollen vor **intransparenten und unfairen Geschäftspraktiken**

[94] „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSG-VO/§ 4 Nr. 10 DSG-EKG.

[95] So ist immer an die Erfüllung der Informationspflichten nach §§ 312d, 312f, 312j BGB (iVm. §§ 246a-246c EGBGB), insbesondere auch über ein ggf. bestehendes Widerrufsrecht, zu denken. (sa. Informationspflichten oben B.1.4.1)

[96] Eine Orientierungsvorlage für die Erstellung von Nutzungsbedingungen für eine Online-Beratung finden sich im Anhang unter D.2.5

[97] Im Rahmen des Bestellvorgangs sollte die Leistungsempfänger*innen jeweils separat bestätigen, dass sie insbesondere die AGBs und Datenschutzhinweise zur Kenntnis genommen haben.

von Plattformanbieterinnen geschützt werden. Denn die Verhandlungsmacht der Plattformbetreiberinnen nimmt weiter zu und damit auch die Abhängigkeit der Drittanbieterinnen von plattformbasierten Vertriebsmöglichkeiten.

Die EU verfolgt das Ziel, ein „faires, vorhersehbares, tragfähiges und vertrauenswürdiges Online-Geschäftsumfeld im Binnenmarkt“ zu schaffen, wozu die P2B-VO beitragen soll. Per se nicht anwendbar ist die VO für „Peer-to-Peer-Online-Vermittlungsdienste ohne Beteiligung gewerblicher Nutzer, reine Business-to-Business-Online-Vermittlungsdienste, die nicht Verbrauchern angeboten werden, Online-Werbeplatzierungsinstrumente und Online-Werbebörsen“[98].

Zwar sind die Vorschriften der VO auch im vorliegend interessierenden Zusammenhang **mitunter anwendbar**. Eine erhebliche Bedeutung dürften sie in der Praxis aber nicht besitzen. Es ist davon auszugehen, dass der von der VO angestrebte Mindeststandard des Schutzes von Anbieterinnen auf Plattformen durch die Betreiberinnen von Plattformen ohnehin gewahrt sein dürfte.

Überblicksmäßig bringt die P2B-VO zugunsten der gewerblichen Nutzerinnen Verbesserungen gegenüber den Plattformbetreiberinnen durch die Forderung nach

- einer nachvollziehbaren Gestaltung von Allgemeinen Geschäftsbedingungen (AGB) und deren Änderungen sowie von bestimmten Informationspflichten sowie eines Verbots der rückwirkenden Änderungen von AGBs,
- Bereitstellung von Informationen zur Kündigung oder Beendigung der Dienste durch die Plattformbetreiberin,
- Offenlegung von Ranking-Parametern (Bekanntgaben des Algorithmus sind aber nicht erforderlich),
- Offenlegung des Umfangs, der Art und der Bedingungen des Zugriffs auf bestimmte Datenkategorien und deren Nutzung durch die Plattformbetreiberin, und
- Einrichtung eines leicht zugänglichen, transparenten und kostenfreien internen Beschwerdemanagementsystems sowie Teilnahme an externen außergerichtlichen Streitbeilegungsmechanismen (Mediation).

B.2.2.1.2 AGB

Zusätzlich zu den ohnehin immer Geltung beanspruchenden Regelungen zur Gestaltung rechtsgeschäftlicher Schuldverhältnisse durch Allgemeine Geschäftsbedingungen (§§ 305ff. BGB) haben Plattformbetreiberinnen insbesondere Folgendes gemäß Art. 3 P2B-VO **sicherzustellen**:

- AGB müssen sowohl „klar und verständlich formuliert“ als auch für die gewerblichen Nutzerinnen vor und nach dem Vertragsabschluss „leicht verfügbar“ sein.
- Für den Fall, dass gewerbliche Nutzerinnen ganz oder teilweise von einer Plattform ausgeschlossen werden, müssen die Gründe dafür klar und nachvollziehbar benannt sein.
- Sollen AGB Auswirkungen auf geistige Schutzrechte der gewerblichen Nutzer haben, muss dies in den AGB klar und nachvollziehbar dargestellt sein, unter anderem bzgl. der Verwendung von Logos, Marken und geschäftlichen Bezeichnungen.
- Werden durch die Plattformbetreiberin „zusätzliche Vertriebskanäle oder etwaige Partnerprogramme“ für den Vertrieb der Waren und Dienstleistungen der gewerblichen Nutzerinnen genutzt, setzt dies eine entsprechende Vorab-Information der gewerblichen Nutzerinnen voraus.
- Änderungen der AGB müssen grundsätzlich mindestens mit einem Vorlauf von 15 Tagen angekündigt werden, wobei den gewerblichen Nutzerinnen ein Kündigungsrecht zu gewähren ist.

Ferner müssen die AGB nach Maßgabe der Art. 8, 9 und 10 P2B-VO insbesondere

- klare Bestimmungen zur Beendigungsmöglichkeit seitens der Nutzerinnen enthalten;
- darüber informieren, ob und welcher Zugang den gewerblichen Nutzerinnen und/oder Dritten zu den aggregierten Daten eingeräumt wird, die sie bereitgestellt haben oder die durch sie veranlasste Nutzungen der Plattform generiert werden; und
- ggf. die Gründe dafür benennen, sofern die Plattformbetreiberin die gewerblichen Nutzerinnen darin einschränken möchte, ihre Angebote auch unabhängig von der Plattform anzubieten.

B.2.2.1.3 Ranking

Ein zentrales Anliegen der VO ist die Herstellung von Transparenz in Bezug auf das Ranking der gewerblichen Anbieterinnen. So sind gem. Art. 5 P2B-VO die hierfür bestimmenden Hauptparameter und die Gründe für ihre relative Gewichtung gegenüber anderen Parametern verständlich anzugeben. Ist eine Beeinflussung des Rankings gegen Entgelt möglich, ist dies klar, nachvollziehbar und leicht verfügbar zu erläutern.

B.2.2.1.4 Ausschluss und Beschränkung

Der Ausschluss einer Anbieterin oder die Beschränkung ihres Angebots setzt gemäß Art. 4 Abs. 1 und 2 P2B-VO eine entsprechende Information und idR auch eine Begründung voraus. Im Falle der vollständigen Beendigung muss die Benachrichtigung grundsätzlich 30 Tage vor der Beendigung erfolgen, sofern keine Ausschlussgründe für die Fristsetzung nach Art. 4 Abs. 4 P2B-VO gegeben sind (zB. gesetzliche bzw. behördliche Verpflichtungen oder erhebliche Vertragsverletzungen seitens der Nutzerin). Im Falle einer Einschränkung, Aussetzung oder Beendigung bietet der Anbieter von

[98] Erwägungsgrund 11.

Online-Vermittlungsdiensten den gewerblichen Nutzerinnen die Möglichkeit, die Tatsachen und Umstände im Rahmen des internen Beschwerdemanagementverfahrens zu klären.

Im Falle einer Auslistung aufgrund der Mitteilung eines Dritten, ist die Nutzerin darüber zu informieren und ihr die Möglichkeit einzuräumen, den Inhalt der Mitteilung einzusehen.

B.2.2.1.5 Differenzierte Behandlung

Gemäß Art. 7 P2B-VO ist jede etwaige unterschiedliche Behandlung der Angebote unter Einbeziehung der wichtigsten wirtschaftlichen, geschäftlichen oder rechtlichen Erwägungen, die einer solchen differenzierenden Behandlung zugrunde liegen, in den AGB darzulegen.

B.2.2.1.6 Weitere Pflichten

Werden Verbraucherinnen auf der Plattform entweder durch deren Betreiberin oder durch Dritte Nebenwaren oder -dienstleistungen angeboten, ist dies nach Art. 6 P2B-VO in den AGB nach der Art der angebotenen Nebenwaren und -dienstleistungen nachvollziehbar zu beschreiben. Es ist ferner darzulegen, ob und unter welchen Bedingungen die gewerbliche Nutzerin ebenfalls berechtigt ist, eigene Nebenwaren und -dienstleistungen über die Plattform zu vertreiben.

Zudem müssen Plattformbetreiber nach Art. 11 P2B-VO ein internes Beschwerdemanagement einrichten, das für die gewerblichen Nutzerinnen leicht zugänglich und eine kostenfreie, zeitnahe und faire Bearbeitung möglicher Beschwerden gewährleistet. Zugang und Funktionsweise des Systems sind verständlich darzustellen und jährlich zu überprüfen.

Es sind von der Plattformbetreiberin mindestens zwei externe Mediatorinnen zu benennen, die in Streitfällen zwischen der Betreiberin und den gewerblichen Anbieterinnen schlichten, insbesondere wenn eine Beschwerde nicht über das Beschwerdemanagementsystem des Art. 1 P2B-VO lösbar ist.

Die Einhaltung der Verordnung können Interessenvertretungen und bestimmte Verbände gerichtlich durchsetzen. Zudem ist jeder EU-Mitgliedstaat angehalten, für eine angemessene und wirksame Durchsetzung der VO zu sorgen. Plattformbetreiberinnen sind schließlich aufgefordert, sich Verhaltenskodizes zu geben, die die Erreichung der VO-Ziele unterstützen. Bis zum 12. Januar 2022 – und anschließend alle drei Jahre – soll die EU-Kommission die Verordnung evaluieren.

B.2.2.1.7 Checkliste P2B-VO

- Sind die AGB verständlich und nachvollziehbar abgefasst und enthalten sie insbesondere die Angaben zu Art. 3, 8, 9 und 10 P2B-VO?
- Wird ein ggf. vorgenommenes Ranking nachvollziehbar erläutert?
- Werden die Bedingungen eines Ausschlusses oder einer Beschränkung der durch die gewerblichen Nutzerinnen eingestellten Angebote nachvollziehbar beschrieben?
- Wird eine ggf. vorhandene differenzierte Behandlung der Angebote nachvollziehbar und mitsamt der ihnen zugrundeliegenden Erwägungen dargelegt?
- Werden Nebenwaren bzw. –dienstleistungen angeboten und wird dies sowie eine ggf. vorhandene Berechtigung ebenfalls Nebenwaren oder –dienstleistungen anzubieten, nachvollziehbar beschrieben?
- Ist ein internes Beschwerdemanagementsystem nach Maßgabe des Art. 11 P2B-VO eingerichtet und gegenüber den gewerblichen Nutzerinnen nachvollziehbar erläutert?
- Sind mindestens zwei externe Mediatorinnen benannt, die ggf. entstehende Streitfälle zügig schlichten können?

B.2.2.2 Barrierefreiheit von Website und mobilen Anwendungen

Zum 23. September 2020 müssen Websites und mobile Anwendungen öffentlicher Stellen im Sinne des § 12 BGG[99] laut der EU-Richtlinie 2016/2102 (in Deutschland umgesetzt durch das Behindertengleichstellungsgesetz [BGG] und die dieses konkretisierende Barrierefreie Informationstechnik-VO 2.0 [BITVO 2.0] bzw. die jeweiligen landesrechtlichen Vorschriften) barrierefrei sein. So müssen sie Erläuterungen in Deutscher Gebärdensprache und Leichter Sprache wie auch eine Erklärung zur Barrierefreiheit vorhalten und über einen **Feedback-Mechanismus** verfügen.[100] Die Richtlinie begründet zudem ein Durchsetzungsverfahren, wenn Barrieren gemeldet werden und für den Bund und die Länder Überwachungs- und Berichtspflichten.

Weitere Vorgaben zur Ermöglichung der Barrierefreiheit durch private Anbieter von Websites und Apps schafft die Richtlinie (EU) 2019/882, die bis zum 28. Juni 2022 in nationales Recht umsetzen ist[101]. Die Anforderungen der Richtlinie (EU) 2019/882 sollen – zusätzlich zu den Vorgaben der Richtlinie

[99] Öffentliche Stelle idS. sind auch sonstige Einrichtungen des öffentlichen Rechts, die als juristische Personen des öffentlichen oder des privaten Rechts zu dem besonderen Zweck gegründet worden sind, im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen, wenn sie überwiegend vom Bund finanziert werden, hinsichtlich ihrer Leitung oder Aufsicht dem Bund unterstehen oder ein Verwaltungs-, Leitungs- oder Aufsichtsorgan haben, das mehrheitlich aus Mitgliedern besteht, die durch den Bund ernannt worden sind, und Vereinigungen, an denen mindestens eine öffentliche nach obiger Definition oder ein sonstiger Träger öffentlicher Gewalt beteiligt ist, wenn die Vereinigung überwiegend vom Bund finanziert wird, die Vereinigung über den Bereich eines Landes hinaus tätig wird, dem Bund die absolute Mehrheit der Anteile an der Vereinigung gehört oder dem Bund die absolute Mehrheit der Stimmen an der Vereinigung zusteht.

[100] Beispielhaft kann auf die entsprechende Erklärung des BMAS verwiesen werden: https://www.bmas.de/DE/Infos/Erklaerung-Barrierefreiheit/erklaerung-barrierefreiheit.html (zuletzt abgerufen am 07. Juli 2020).

[101] Zwingend sind ihre Regeln voraussichtlich erst ab dem 28. Juni 2025.

(EU) 2016/2102 – auch für Websites und mobile Anwendungen öffentlicher Stellen gelten. Damit soll künftig gewährleistet werden, dass der Online-Verkauf von Produkten und Dienstleistungen unabhängig davon, ob der Verkäufer ein öffentlicher oder privater Akteur ist, für Menschen mit Behinderungen in vergleichbaren Maße barrierefrei ist.[102]

Beide Richtlinien unterliegen den folgenden vier Grundsätzen[103]:

- **Wahrnehmbarkeit:** die Informationen und Komponenten der Nutzerschnittstelle müssen den Nutzer*innen in wahrnehmbarer Weise dargestellt werden.
- **Bedienbarkeit:** die Nutzer*innen müssen die Komponenten der Nutzerschnittstelle und die Navigation handhaben können.
- **Verständlichkeit:** die Informationen und die Handhabung der Nutzerschnittstelle müssen den Nutzer*innen verständlich sein;
- **Robustheit:** die Inhalte müssen robust sein, damit sie zuverlässig von einer Vielfalt von Benutzeragenten, einschließlich assistiver Technologien, interpretiert werden können.

Die Barrierefreiheit von Websites basiert letztlich auf IT-rechtlichen Standards. Grundlegend sind die Web Content Accessibility Guidelines 2.1 (WCAG 2.1). Aus den genannten vier Prinzipien werden 78 Erfolgskriterien abgeleitet, die einzuhalten sind. Die WCAG sind über die europäische Norm EN 301 549 (aktuell V 3.1.1) verbindlich, und zwar über den dynamischen Verweis des § 3 BITVO 2.0. Die begleitende deutsche DIN EN 301549:2020-02 nimmt zwar nicht an der Konformitätsvermutung des § 3 Abs. 2 BITVO 2.0 teil. Sie konkretisiert aber den nach § 3 Abs. 3 BITVO einzuhaltenden Stand der Technik. Über diesen sind ggf. auch die User Agent Accessibility Standards 2.0 und die Authoring Tool Accessibility Standards 2.0 zu beachten.

Auch wenn die Pflicht nicht in jedem Fall für die hier interessierenden Anwendungen greift,[104] sollte auf die Barrierefreiheit der Seite natürlich schon aus Eigeninteresse geachtet werden, um die Website einem möglichst umfassenden Kreis zugänglich zu machen.

B.2.2.3 ePrivacy RL/TMG: Der Einsatz von Cookies

Was sind Cookies?
Ein Cookie ([ˈkʊki]; englisch „Keks“) ist ein technisches Hilfsmittel, das es erlaubt, über die Besucher*innen einer Website eine dauerhafte Textinformation zu speichern. Es wird im Browser der Besucher*innen zu einer besuchten Website gespeichert. Dazu wird es entweder vom Webserver an den Browser gesendet oder im Browser selbst durch ein Skript erzeugt. So kann der Webserver bei späteren Besuchen entweder die Information selbst auslesen oder durch das Skript übertragen bekommen.

Ohne solche Cookies würde das Internet in vielerlei Hinsicht für die meisten Nutzer*innen nicht richtig funktionieren. Das Abspeichern von Logins oder eines Warenkorbs bei einer Online-Händlerin wäre nicht mehr möglich. Aber auch weitergehende Funktionen bis hin zum Tracking durch Cookies sind möglich. Dann können voneinander unabhängige Websites von ihrer Nutzung durch die Nutzer*innen erfahren und aus dieser Information Vorteile ziehen.[105]

Bei dem Einsatz von Cookies wird daher gemeinhin zwischen folgenden Klassen von Cookies unterschieden:

- den erforderlichen, die für den ordnungsgemäßen technischen Ablauf der Website unbedingt erforderlich sind (dazu können Prozess- und Sicherheitscookies gehören);
- den funktionalen, die Komfortfunktionen für die Besucher*innen (zB. Spracheinstellungen) ermöglichen;
- den statistischen Cookies, die zur Verbesserung der Website (grundsätzlich anonym) Daten zum Nutzer*innenverhalten aggregiert;
- den analytischen Cookies, die die Optimierung der Website aber auch die Anpassung der Inhalte an die jeweiligen Nutzer*innen erlaubt und (so etwa bei Google Analytics) nicht im Sinne der DS-GVO anonymisieren und
- Cookies zu Marketingzwecken, die im Sinne des Marketingtrackings Informationen über die Nutzer*innen mit anderen Anbieterinnen teilen.

Zudem wird vielfach zwischen First-Party-Cookies und Third-Party-Cookies unterschieden. Mit dieser Unterscheidung ist aber in vielen Fällen nichts Substanzielles gewonnen, da sie die relevanten Verantwortlichkeiten nicht notwendig abbildet. So können First-Party-Cookies auch als Third-Party-Cookies ausgeliefert werden und vice versa.

B.2.2.3.1 Allgemeines

Die Datenschutzrichtlinie für elektronische Kommunikation (auch: **ePrivacy-Richtlinie**) ist eine 2002 erlassene Richtlinie der Europäischen Gemeinschaft, die verbindliche Mindestvorgaben für den Datenschutz in der Telekommunikation setzt. Sie wurde 2009 novelliert und ist seitdem als sogenannte **Cookie-Richtlinie** bekannt. Denn die Novelle enthielt Regelungen zur Setzung einiger Arten von Cookies auf Webseiten.

[102] Siehe Erwägungsgrund 46 der Richtlinie (EU) 2019/882.
[103] Siehe Erwägungsgrund 47 der Richtlinie (EU) 2019/882.
[104] Die Pflicht zur Umsetzung kann sich auch aus vergaberechtlichen Auflagen ergeben.
[105] Die Enthüllungen durch Edward Snowden machten darüber hinaus bekannt, dass bestimmte Cookies von der NSA genutzt werden, um eine zielgerichtete Überwachung von Rechnern zu erlauben.

Die ePrivacy-Richtlinie gilt auch nach Inkrafttreten der DS-GVO und soll im Zuge einer weiteren Anpassung des Datenschutzrechts durch die ePrivacy-Verordnung (ePrivVO) abgelöst werden. Diese scheiterte jedoch im europäischen Gesetzgebungsverfahren Ende 2019 vorerst, da sich die Mitgliedstaaten nicht auf einen gemeinsamen Text verständigen konnten. Mit einem Inkrafttreten ist realistischer Weise eher erst zum Jahre 2022 zu rechnen. Zu Widerspruch führte insbesondere, dass das Datenschutzregime der VO teilweise strenger ausfallen soll als in der DS-GVO. Der letzte Entwurf scheint deren Niveau dagegen teilweise eher zu unterlaufen. Die Entwicklungen sollten zur Sicherstellung der Compliance ständig beobachtet werden.

In Deutschland wurde die ePrivacy Richtlinie ua. durch das TMG (teilweise) umgesetzt. Dabei hat sich der Gesetzgeber nicht eng genug an der Richtlinie orientiert.[106] So sieht das TMG nur vor, dass Cookies widersprochen werden kann, die Verwendung also keiner expliziten Einwilligung bedarf. Die Richtlinie setzt demgegenüber aber die Einwilligung voraus.[107] Die betreffende Regelung im TMG ist daher weitestgehend nicht anzuwenden.

Anmerkung:
Der maßgebliche Unterschied zwischen einer Widerspruchslösung (Opt-out) und einer Einwilligung (Opt-in) ist, dass im Falle einer Widerspruchslösung eine Datenverarbeitung als unwidersprochen stattfinden darf, sofern der Betroffene der Verarbeitung nicht ausdrücklich widersprochen hat. Hingegen darf eine Verarbeitung bei einer Opt-in-Lösung erst beginnen, nachdem eine wirksame Einwilligung vom Nutzer erteilt ist.

B.2.2.3.2 Cookie-Entscheidungen des EuGH und BGH

Mittlerweile ist durch zwei wesentliche Gerichtsentscheidungen deutliche Bewegung in die Sache gekommen. Zum einen hatte bereits der EuGH im Herbst 2019 entschieden[108], dass die Einholung einer Einwilligung „aufgrund klarer und umfassender Information“ für Cookies zur Verarbeitung personenbezogener Daten Pflicht ist. Eine wirksame Einwilligung liege aber nicht vor, „wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss“.[109] Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können, gehören danach zu den Informationen, die die Anbieterinnen dem Nutzer einer Website zu geben haben.

In seiner Planet49-Entscheidung[110] hat der BGH dies auch im Rahmen des deutschen Rechts noch einmal nachvollzogen. Danach ist § 15 Abs. 3 TMG im Einklang mit der ePrivacy-Richtlinie auszulegen. Nur notwendige Cookies (die etwa sicherstellen, dass sich die Seite im Browser der Nutzer*innen richtig aufbauen kann und sicher läuft) können weiterhin ohne eine wie oben dargestellt qualifizierte Einwilligung gesetzt werden. Das **TMG soll nun entsprechend angepasst** werden.

Relativ sicher ist damit zu rechnen, dass der Einsatz von Cookies durch die ePrivVO so geregelt wird, wie es durch die Rechtsprechung bereits vorausgesetzt wird. Für **alle nicht-essentiellen Cookies ist eine aktive, explizite und informierte Einwilligung notwendig**. Ferner darf die Nutzung der Website **nicht durch eine Cookie-Wall** von der Einwilligung in die Speicherung nichtessentieller Cookies abhängig gemacht werden (Kopplungsverbot). Auch wird es wohl für alle **Nutzungen der Verarbeitungsfunktionen im Endgerät (zB. die Speicherung von Daten) einer Einwilligung** bedürfen. Das macht große Teile des Webtrackings ohne Einwilligung hinfällig.

Da der **Einsatz von – zB. für den Betrieb der Website – technisch notwendigen (Session)-Cookies nicht per se einwilligungsbedürftig** ist,[111] sollten Anbieterinnen einen **Cookie-Banner und -Konfigurationsplattformen (Consent-Tools) immer dann einrichten, wenn der Einsatz von Cookies über das zwingend notwendige Maß hinausgeht**. Letzteres gilt insbesondere für alle Third-Party-Cookies.

Die Cookie-Konfigurationsplattform ist so anzulegen, dass die die Nutzer*innen ihre Cookies einfach und direkt auf der gewünschten Website verwalten können. Über den Bildschirmausschnitt (Fold) hinauslaufende oder mit Text überladene Cookie-Banner sind aber zu vermeiden. Insgesamt sollten Cookie-Banner folgendermaßen ausgestaltet sein:[112]

- Beim erstmaligen Öffnen einer Website erscheint das Banner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses HTML-Element aus einer Übersicht über alle einwilligungsbedürftigen Verarbeitungsvorgän-

[106] Ein formeller Umsetzungsakt der ePrivacy-Richtlinie 2002/58/EG in der Fassung der Änderung durch die Richtlinie 2009/136/EG2 ist im 4. Abschnitt des TMG nicht erfolgt. Insbesondere fehlt es an einem Umsetzungsakt für Art. 5 Abs. 3 der ePrivacy-RL im deutschen Recht insgesamt. Es stellt sich daher die Frage nach der Anwendbarkeit der Vorschriften des 5. Abschnitts des TMG seit der Geltungserlangung der DSGVO.

[107] Siehe insgesamt auch die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien des DSK aus April 2018, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (zuletzt abgerufen am 18. Juni 2020).

[108] Urteil vom 01. Oktober 2019, C - 673/17 – Planet49, auf Vorlage des BGH zwecks Auslegung der EU-Datenschutzvorschriften.

[109] „Der Schutz erstreckt sich auf alle in solchen Endgeräten gespeicherten Informationen, unabhängig davon, ob es sich um personenbezogene Daten handelt, und erfasst insbesondere […] „Hidden Identifiers“ oder ähnliche Instrumente, die ohne das Wissen der Nutzer in deren Endgeräte eindringen.“, EuGH a.a.O.

[110] Urteil v. 28. Mai 2020, I ZR 7/16 – Cookie-Einwilligung II.

[111] Die Pflicht zu Information über den Umfang der Datenverarbeitung in einem Datenschutzhinweis bleibt aber auch in Fällen eines nicht einwilligungsbedürftigen Einsatzes eigener, technisch notwendiger Session-Cookies bestehen.

[112] Die folgende Darstellung ist der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien der DSK, Stand März 2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (zuletzt abgerufen am 18. Juni 2020), S. 9, entnommen.

ge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt wird und über ein Auswahlmenü aktiviert werden können (Opt-in). Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht – als Opt-out – „aktiviert“ voreingestellt sind.
- Während das Banner angezeigt wird, werden zunächst alle weitergehenden Skripte einer Website oder einer WebApp, die potenziell Nutzerdaten erfassen, blockiert. Der Zugriff auf Impressum und Datenschutzerklärung darf durch „Cookie-Banner“ nicht verhindert werden.
- Erst wenn der Nutzer seine Einwilligung(en) durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Banner oder den Klick auf eine Schaltfläche abgegeben hat (Opt-in), darf die einwilligungsbedürftige Datenverarbeitung tatsächlich – durch technische Maßnahmen sichergestellt – stattfinden.
- Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DS-GVO (bzw. § 11 Abs. 1 DSG-EKD) ist es gem. Art. 11 Abs. 1 DS-GVO (bzw. § 15 Abs. 1 DSG-EKD) nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. DS-GVO-Erwägungsgrund 26) ist ausreichend. Damit die Entscheidung des Nutzers für oder gegen eine Einwilligung bei einem weiteren Aufruf der Website berücksichtigt wird und das Banner nicht erneut erscheint, kann deren Ergebnis auf dem Endgerät des Nutzers – mit dessen Zustimmung – ohne Verwendung einer User-ID o. ä. gespeichert werden. Durch ein solches Verfahren kann der Nachweis einer vorliegenden Einwilligung erbracht werden.
- Da eine Einwilligung widerruflich ist, ist eine entsprechende Möglichkeit zum Widerruf zu im-plementiert. Der Widerruf muss so einfach sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 S. 4 DS-GVO (§ 11 Abs. 3 S. 4 DSG-EKD).

Verantwortliche müssen sicherstellen, dass die Einwilligung nicht nur das Setzen von einwilligungsbedürftigen Cookies umfasst, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z.B. auch eventuelle Verfahren zur Verfolgung der Nutzer durch Zählpixel oder diverse Fingerprinting-Methoden, soweit diese nicht aufgrund einer anderen Rechtsgrundlage zulässig sind.

Folgendes Vorgehen kann beispielsweise gewählt werden:

Die Nutzer*innen werden über **eigene Session-Cookies**, die für die korrekte Basisfunktionsweise der Website **technisch notwendig** sind, mittels Cookie-Banner informiert. Nutzen sie die Website weiter, bedeutet dies, dass sie die essentiellen Cookies akzeptieren. Das unmittelbare Schließen der Website bedeutet hingegen ein Opt-out. Ein eigenes Opt-in ist dafür also nicht notwendig. Beim Verlassen der Website sind die Cookies jedoch zwingend zu löschen. Wird die Website nicht geschlossen (vom Opt-out also kein Gebrauch gemacht), werden weitere Cookies, die Analyse- oder Marketingzwecken dienen, nur dann geladen, wenn ein – aktives, explizites und informiertes – Opt-in erfolgt, etwa durch einfaches Klicken auf das markierte Feld des Cookie-Banners. Ohne diesen Klick funktionierte die Website weiterhin. Es dürfen jedoch keine weiteren Cookies installiert sein.

In besonderen Fällen, wenn die Verarbeitung beispielsweise mit einem **erhöhten Risiko** für die Nutzer*innen verbunden ist, sollte ein **weiterer Dialog hinzukommen**, der ein zusätzliches – aktives, explizites, informiertes – Opt-in ermöglicht. Ein solches Double-Opt-in (auch Closed-Loop-Opt-in genannt) wird nach Klicken und Eingabe einer E-Mail-Adresse oder Mobilnummer per E-Mail oder SMS-/Messenger-Nachricht zur Bestätigung abgefragt. Die besonderen Verarbeitungen erfolgen zwingend erst nach Freigabe durch Anklicken eines in der E-Mail, SMS oder Messenger-Nachricht befindlichen Links.

Ein solches Vorgehen sollte auch für alle Vorgänge gewählt werden, bei denen beabsichtigt ist, Daten der Nutzer*innen zu verarbeiten, um ihnen Newsletter[113], Informationen oder sonstige Inhalte an ihre E-Mail-Adresse oder Mobilnummer zu senden. Nur so kann sichergestellt werden, dass die E-Mail-Adresse und Mobilnummer vom tatsächlichen Inhaber stammt.

B.2.2.3.3 Tracking und Profiling[114]

Auf **Cookies zu Marketing-Zwecken** sollte ganz verzichtet werden. Diese genießen auch eine eher fragwürdige Reputation. Falls sie doch genutzt werden sollen,[115] ist in jedem Fall

- eine **aktive, explizite und informierte Einwilligung**[116] sowie
- ggf. der Abschluss eines Auftragsverarbeitungsvertrages mit Drittanbietern[117] sowie die DS-GVO-Konformität einer ggf. stattfindenden Datenübermittlung ins außereuropäische Ausland erforderlich. Zudem ist/sind
- der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO bzw. § 5 Abs. 1 Ziff. 5 DSG-EKD) zu beachten, also ein Löschkonzept (siehe dazu unten C.1.1.1.5.1.2) zu erstellen,
- ggf. eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DS-GVO, § 34 DSG-EKD)[118],
- die Datenschutzerklärung anzupassen und
- die technischen und organisatorischen Maßnahmen (TOM) gemäß dem Stand der Technik angemessen umzusetzen und ständig zu überprüfen.

[113] Siehe dazu auch B.2.2.4.3.3.
[114] Siehe dazu bereits oben B.1.5.6.
[115] Vom Einsatz von SuperCookies/Evercookies/Zombie-Cookies sollte jedenfalls abgesehen werden. Bei diesen handelt es sich um Cookies, die dauerhaft und vor allem versteckt gespeichert, so dass sie von den Nutzer*innen nur schwer oder gar nicht entfernt werden können, zumal sie sie sich nach dem Löschen selbständig neu installieren.
[116] Siehe ergänzend zur Einholung der Einwilligung die Empfehlungen der CNIL (Commission Nationale de l'Informatique et des Libertés [die nationale Datenschutz-Aufsichtsbehörde Frankreichs mit Sitz in Paris]) zum Einsatz von Cookies und anderen Tracking Devices: https://www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf (zuletzt abgerufen am 21. August 2020).
[117] Siehe hierzu C.1.1.1.5.1.3 und das Muster D.2.7 (Teil D).
[118] Siehe hierzu die sog. „Muss“-Liste der gemeinsamen Datenschutzkonferenz der Datenschutzbeauftragten: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf (zuletzt abgerufen am 7. November 2020)

Zu beachten ist, dass umfangreichere Datensammlungen, die Informationen über individuelle Personen offenbaren, auch für Kriminelle von besonderem Interesse sind. Mit technischem Know-how ausgestattet, können Kriminelle mitunter auf Cookies einer Website zugreifen.

Dadurch können sie sich unter Umständen ein Persönlichkeitsprofil der betroffenen Person erstellen, die nachfolgend im Wege des sogenannten Spear-Phishings angegriffen wird. Auch im Rahmen der „Kill-Chain" eines APT-Angriffs[119] werden Cookies zur Auswahl einer geeigneten Zielperson ausgenutzt, deren digitale Identität leichter zu übernehmen ist. Mittels einer so übernommenen Identität kann dann der Zugriff auf das eigentliche Zielsystem (zB. das sensitive Kontoführungssystem einer Bank) erfolgen.

Unabhängig davon, welche Cookies konkret eingesetzt werden,

- es sollten immer nur solche eingesetzt werden, die auch tatsächlich genutzt werden;
- in ihnen abgelegte Daten sollten möglichst anonymisiert – mindestens aber pseudonymisiert – werden;
- der Lebenszyklus von Cookies sollte aktiv verwaltet und
- ihre Speicherdauer sowie die Aufzeichnungsdauer von Logfiles sollten – möglichst auf die Dauer des Aufrufs des Dienstes – oder aber anderweitig begrenzt werden; ferner sollten
- die Schablonen zur Interpretation der in den Cookies gespeicherten Informationen nicht veröffentlicht werden. Anderes kann nur gelten, sofern die Website in ein Open-Source-Umfeld gefasst ist. Dann ist darauf zu achten, nur unbedingt benötigte Informationen in Cookies zu speichern.

Praxis-Tipp:
Ergänzend sei darauf hingewiesen, dass das Nutzen von Kartendiensten nur dann geschehen sollte, wenn die datenschutzsichere Nutzung der Daten durch die Anbieter sichergestellt ist. Das ist bislang regelmäßig nicht der Fall, da sich die kostenfreie Bereitstellung dieser Dienste als Geschäftsmodell nur vor dem Hintergrund der Datennutzung lohnt. So ist es zwar für Anbieterinnen verlockend, den Gratisdienst einzusetzen, ethisch vertretbar ist es aber häufig nicht, da für diesen Vorteil die Nutzer*innen mit ihren Daten zahlen.[120]

Erfolgt dennoch eine Einbindung sollte die Anwendung in der Grundeinstellung möglichst nicht scharfgeschaltet, sondern erst durch ein aktives, informiertes Handeln der Nutzer*innen freischaltbar sein (z. B. durch Betätigung eines Schiebereglers).

Ein besonderes Problem stellt das sogenannte **Profiling** dar. Bei diesem handelt es sich um die nutzbare Erstellung des Gesamtbildes einer Persönlichkeit für bestimmte Zwecke, die durch das Zusammenführen von Daten sowie deren anschließende Analyse und zweckbezogene Auswertung erreicht wird. Im Marketing wird es verwendet, um möglichst präzise Kundenprofile zu erstellen, die die Beeinflussung von Kaufentscheidungen ermöglichen. Vom Einsatz solcher Techniken, die ohnehin **nur bei Einhaltung anspruchsvoller Voraussetzungen rechtlich möglich** sind, ist **grundsätzlich abzuraten**.

B.2.2.3.4 Überprüfung bereits bestehender Websites: Checkliste

Auch wenn Sie keine neue Website planen, ist das Vorstehende auch für bestehende Websites zu beachten. Diese sollten mindestens auf Folgendes überprüft werden:

- Ist die Datenschutzerklärung an die Transparenzpflichten der DS-GVO angepasst?
- Werden Analysetools (zB. Google Analytics, Matomo etc.) eingesetzt?
- Werden Cookies eingesetzt? Sind diese „notwendig" oder dienen sie weiteren Interessen (Marketing/Werbeinteressen)?

Nur für die Funktionalität einer Website zwingend notwendige, eigene Session-Cookies benötigen keine **aktive, informierte und explizite Einwilligung** der Nutzer*innen (aber mindestens eines Datenschutzhinweises auf der Website).

B.2.2.3.5 Checkliste Cookies

- Werden ohne Einwilligung (aber mit einem Datenschutzhinweis) nur eigene, technisch notwendige Session-Cookies eingesetzt?
- Ist die Einrichtung eines Cookie-Banners/Consent-Tools notwendig (kommen also nicht nur essentielle eigene Session-Cookies zum Einsatz)?
- Ist der Einsatz aller weiteren Cookies – insbesondere auch Third-Party-Cookies – durch aktive, explizite und informierte Opt-ins abgesichert?
- Werden generell nur solche Cookies eingesetzt, die auch tatsächlich genutzt werden?
- Wird umfassend und transparent über alle eingesetzten Cookies informiert?
- Wird der Lebenszyklus von Cookies aktiv verwaltet und ist ihre Speicherdauer sowie die Aufzeichnungsdauer von Logfiles auf das notwendige Maß begrenzt und sind Daten, soweit wie möglich, anonymisiert oder – wenn nicht möglich – pseudonymisiert?
- Ist sichergestellt, dass die Schablonen zur Interpretation der in den Cookies gespeicherten Informationen Dritten nicht zugänglich sind (außer bei entsprechender Einbettung in ein Open-Source-Umfeld, dann aber mit entsprechender Einwilligung)?

[119] Advanced Persistent Threat = ausgeklügelte, andauernde Bedrohung.
[120] Die Verwendung der Karten-App sollte nicht einfach durch einen Screenshot ersetzt werden, wenn nicht die Rechte an dessen Verbreitung gesichert sind. Anderenfalls läge ein Verstoß gegen das Urheberrecht vor.

- Ist sichergestellt, dass die Nutzung der Website nicht von der Einwilligung in die Nutzung nicht-essentieller Cookies abhängig ist?
- Ist der Einsatz nicht-essentieller Cookies durch eine aktive, explizite und informierte Einwilligung nicht nur abgesichert, sondern auch gut dokumentiert?
- Ist bei Datenübertragungen an Dritte und Einbindung von Drittdiensten ein Auftragsverarbeitungsvertrag (AV-Vertrag) abgeschlossen?
- Ist die Übermittlung von Daten ins außereuropäische Ausland ggf. DS-GVO-konform bzw. rechtlich überhaupt möglich?
- Wird bei Nutzungen der Verarbeitungsfunktionen im Endgerät (zB. Speicherung von Daten) eine aktive, explizite und informierte Einwilligung eingeholt?
- Ist den Nutzer*innen die einfache Verwaltung der Cookies inklusive eines nachträglichen Widerrufs ihrer Einwilligungen (wie oben beschrieben) ermöglicht?
- Werden neben den Einwilligungen für Cookies auch Einwilligungen für weitere einwilligungsbedürftige Verarbeitungstätigkeiten, wie z.B. auch eventuelle Verfahren zur Verfolgung der Nutzer durch Zählpixel oder diverse Fingerprinting-Methoden, soweit diese nicht aufgrund einer anderen Rechtsgrundlage zulässig sind, eingeholt?
- Ist der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO bzw. § 5 Abs. 1 Ziff. 5 DSG-EKD) hinreichend beachtet, insbesondere ein Löschkonzept erstellt?
- Ist die Datenschutzerklärung im Hinblick auf alle Verarbeitungsvorgänge angepasst worden?
- Ist eine Datenschutz-Folgenabschätzung iSv. Art. 35 DS-GVO, § 34 DSG-EKD durchzuführen?[121]
- Entsprechen die begleitenden technischen und organisatorischen Maßnahmen (TOM) dem Stand der Technik angemessen umsetzen und wird dies regelmäßig überprüft?

B.2.2.4 Weitere Anforderung an Websites

B.2.2.4.1 Grundkonstruktion

Ist das technisch nötige Know-how nicht vorhanden, so wird die Erstellung einer Website[122] häufig an eine darauf spezialisierte Agentur gegeben. Mitunter wird auch auf sogenannte Website-Builder – wie etwa Wordpress, Jimdo, Wix etc. – zurückgegriffen. Dabei handelt es sich um webbasierte Software, die das selbständige Erstellen einer Website vereinfacht. In keinem dieser Fälle ist automatisch sichergestellt, dass die spätere Website datenschutzkonform ist. Auf die insoweit wesentlichen Punkte soll im Folgenden hingewiesen werden.

- Die Website muss **entsprechend dem aktuellen Stand der Technik** programmiert und betrieben werden. Die Verwendung eines veralteten Codes kann zu schweren Sicherheitsmängeln führen, die die Entwendung personenbezogener Daten einfach machen, und Haftungs- und Gewährleistungsansprüche auslösen können.
- Bei der Programmierung/Gestaltung einer Website/App ist dem Grundsatz **Privacy by Design** und **Privacy by Default** Genüge zu tun.[123] Es ist also sicherzustellen, dass die Gestaltung der Website so ausfällt, dass **keine oder nur so wenig personenbezogene Daten wie möglich** durch sie verarbeitet werden **(Datenminimierung)**. Diese Vorgabe entspricht dem Grundsatz, dass nur so viele personenbezogene Daten verarbeitet werden sollen, wie zur Erreichung des legitimen Zwecks erforderlich sind. Konfigurationsaufwand soll vermieden werden und ein ausreichendes Datenschutzniveau ohne Anpassungen von Vornherein gewährt sein.
- Das mit der Erstellung der Website beauftragte Unternehmen muss sich **schriftlich dazu verpflichten**, den aktuellen Stand der Technik einzuhalten und die Forderung nach Privacy by Design und Default zu erfüllen.
- Bei der **Abnahme der Leistung muss das überprüfend berücksichtigt** werden.

Mit der datenschutzkonformen Erstellung der Website ist es noch nicht getan. Die Website besteht nicht für sich selbst, sondern muss auf einem Webserver gehostet werden. Als per definitionem (grundsätzlich) öffentlich erreichbares System muss ein Webserver ebenfalls dem aktuellen Stand der Technik entsprechend gesichert sein. Die insoweit notwendige angemessene Konfiguration und Zertifizierung, etwa durch die Installation eines (kostenpflichtigen)[124] ssl-Zertifikats[125], sollte durch Fachkräfte erfolgen.

Falls die Einrichtung eines Servers nicht on-premises, also nicht im Unternehmen der Anbieterin selbst erfolgt, kann der Webserver auch gemietet werden. Professionelle Hosts bieten den datensicheren Betrieb solcher Systeme gegen Entgelt an. Bei der Auswahl sollte auf **einschlägige Zertifizierungen** geachtet werden, allen voran **nach ISO/IEC 27001**.

Trotz des Mietens eines Webservers trifft die Anbieterin weiterhin die volle datenschutzrechtliche Verantwortung, die durch Abschluss eines **Auftragsverarbeitungsvertrags** – einschließlich von Weisungsrechten – sicherzustellen ist (siehe C.1.1.1.5.1.3). Auf einen solchen Vertrag kann nur verzichtet werden, wenn es sich um eine statische Website handelt, die keinerlei Interaktion mit den Besuchern erlaubt.

Werden dagegen personenbezogene Daten verarbeitet (die Erhebung reicht dafür aus), muss der Datenaustausch zwi-

[121] Wird die Datenschutz-Folgenabschätzung zusätzlich veröffentlicht, ist diese zugleich ein Instrument der Vertrauensbildung gegenüber den Nutzer*innen.
[122] Eine Website (web = Netz (abgeleitet vom world wide web, also dem weltweiten Netz und site = Ort, Stätte, Platz, Stelle, Lage) ist die Gesamtheit der hinter einer Adresse stehenden Inhalte im Internet. Diese können über Browser angezeigt werden.
[123] Siehe dazu auch unten C.1.1.1.3.
[124] Auch eine kostenlose Zertifizierung kann möglich sein, wenn sie zuverlässig über das Hosting-Unternehmen angeboten wird.
[125] Ssl steht für secure sockets layer. Das Fehlen eines solchen Zertifikats führt mitunter dazu, dass den Nutzer*innen die Meldung „Diese Website ist nicht sicher“ angezeigt wird. Das kann dazu führen, dass Interessierte die Seite aufgrund mangelndem Vertrauen wieder verlassen.

schen den Nutzer*innen und dem Server ssl-**verschlüsselt**[126] erfolgen. Dies ist mittlerweile Standard und wird von professionellen Hosts regelmäßig angeboten.

Die Verarbeitung personenbezogener Daten muss immer eine **Einwilligung**, ein Opt-in voraussetzen, sofern kein **anderer gesetzlicher Grund** für die Verarbeitung gegeben ist. Ist ein anderer Grund gegeben, sollte die Verarbeitung nicht (zusätzlich) auf die Einwilligung gestützt werden, da deren Einholung anderenfalls das **Gebot der Fairness und Transparenz** verletzen könnte. Der Rechtsgrund für die Verarbeitung von Daten kann in der Durchführung des Vertrages oder in besonderen gesetzlichen Erlaubnistatbeständen liegen.

Bei personenbezogenen Daten besonderer Kategorien kann mit einer Einwilligung, aber auch mit den spezifischen Erlaubnistatbeständen gearbeitet werden, sofern diese im jeweiligen Anwendungsfall einschlägig sind. Dies ist sehr gewissenhaft zu überprüfen.[127]

B.2.2.4.2 Anforderungen nach Telemediengesetz und Telekommunikationsgesetz

Der für die Anbieter von Internetdiensten geltende Datenschutz-Rechtsrahmen befindet sich gegenwärtig im Umbruch. Durch die seit 25. Mai 2018 in allen Mitgliedstaaten unmittelbar geltende EU-Datenschutzgrundverordnung (DS-GVO), haben nationale Datenschutzgesetze, auch das Bundesdatenschutzgesetz (BDSG), an Bedeutung verloren. Die DS-GVO lässt nur einen eingeschränkten Gestaltungsspielraum für nationale Abweichungen.

Mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz vom 30. Juni 2017 hat der deutsche Gesetzgeber das Bundesdatenschutzgesetz im Hinblick auf die DS-GVO neu gefasst (BDSG 2018). Dabei kam es noch nicht zu einer vollen Anpassung des fachspezifischen Datenschutzrechts. Zwar ist mittlerweile auch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz in Kraft. Aber auch dieses hat noch nicht zu einer vollständigen Klärung der strittigen Fragen geführt. So ist noch unklar, inwieweit neben der DS-GVO auf Regelungen des TMG zurückgegriffen werden darf.

Vielfach, wenn nicht sogar überwiegend, wird davon ausgegangen, dass das TMG im Hinblick auf seine datenschutzrechtlich relevanten Vorschriften (§§ 11 bis 15a TMG) durch die DS-GVO weitestgehend verdrängt wird. Allerdings hat der BGH in einer kürzlich ergangenen Entscheidung, auf die sogleich noch zurückgekommen wird, die europarechtskonforme Geltung des § 15 Abs. 3 TMG ausbuchstabiert.[128] Die letztendliche Klärung durch den Gesetzgeber dürfte den Erlass der ePrivacy-Verordnung[129] voraussetzen, die derzeit auf europäischer Ebene noch ihrer Verabschiedung harrt, bevor sie den Datenschutz im Bereich der elektronischen Kommunikation neu regelt.

Die bei Betrieb einer Website neben den datenschutzrechtlichen Vorschriften möglicherweise relevanten Vorschriften des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) sollen dennoch im Folgenden beleuchtet werden. Bei der Anwendung des TMG (und des TKG) wird dabei der Standard der DS-GVO bzw. des DSG-EKD nicht unterschritten. Das heißt, dass etwaige Bereichsausnahmen oder sonstige Privilegierungen nicht durchgreifen. Lediglich dort, wo die DS-GVO keine Regelungen trifft (Auskunft ggü. öffentlichen Stellen, Modalitäten der Abrechnung, Aufbewahrungsfristen, Datenspeicherung zu Rechtsverfolgungszwecken), bleibt Raum für eine ergänzende Anwendung der nationalen Gesetze.

B.2.2.4.2.1 Impressum

Gemäß § 5 TMG haben die Anbieterinnen **umfangreiche Angaben** auf ihrer Website im Impressum zu hinterlegen. Dazu gehören ua. Name und Niederlassungsanschrift, die Rechtsform und Vertretungsberechtigung, Register und Registernummer, die zuständige Aufsichtsbehörde, Kontaktinformation und Umsatzsteueridentifikationsnummer.

Weitergehende Informationspflichten können sich **im Einzelfall** über § 5 Abs. 2 TMG auf **anderen Vorschriften** ergeben, etwa aus dem Fernabsatzrecht (§§ 312b ff. BGB), den Regelungen über den elektronischen Geschäftsverkehr (§ 312e BGB), dem Verbraucherstreitbeilegungsgesetz (§ 36 f. VSBG), der ODR-Verordnung (EU) Nr. 524/2013, dem Fernunterrichtsschutzgesetz, der Preisangabenverordnung oder aus gesellschaftsrechtlichen Angabepflichten.

Für die typische diakonische Anbieterin ist ggf. auch die Angabe einer presserechtlich inhaltlich verantwortlichen Person i.S.v. § 18 Abs. 2 MStV[130] und der Datenschutzbeauftragten erforderlich bzw. empfehlenswert. Zusätzlich kann die Verweisung auf die der Nutzung des Internetangebots gegebenenfalls zugrundeliegenden AGB angezeigt sein.

Die Pflichtangaben müssen „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar“ sowie stets aktuell, insbesondere sollten sie möglichst nicht mehr als ein Klick von jeder Unterseite entfernt sein.

[126] Eine ssl-Verschlüsselung wird im Browser als „https://“ signalisiert. Der Anzeige des Transportprotokolls „http“ wird also ein „s“ für secure/sicher angefügt.
[127] Siehe oben B.1.5.2.
[128] Urteil v. 28.5.2020, I ZR 7/16 – Cookie-Einwilligung II.
[129] Sie wird die ePrivacy-Richtlinie (2002/58EG) einschließlich ihrer Ergänzung durch die sogenannte Cookie-Richtlinie (2009/136/EG) abgelöst.
[130] Der Medienstaatsvertrag (MStV) soll bis Ende 2020 den Staatsvertrag für Rundfunk und Telemedien (RStV) ablösen. Die bisherige Regelung findet sich in § 55 Abs. 2 RStV. Wurde bisher die Information zu der redaktionell verantwortlichen Person im Impressum mit „Inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV“ eingeleitet hat, muss diese Formulierung nunmehr dahingehend angepasst werden, dass es zukünftig „Inhaltlich verantwortlich gemäß § 18 Abs. 2 MStV“ lauten muss.

B.2.2.4.2.2 Bestands- und Nutzungsdaten

Gemäß Art. 6 Abs. 1 b) DS-GVO, § 6 Nr. 5 DSG-EKD darf die Diensteanbieterin personenbezogene Daten der Nutzer*innen nur – unter entsprechender Aufklärung in Datenschutzhinweisen – erheben und verwenden, soweit diese **für den Abschluss des Vertrages** und dessen inhaltliche Ausgestaltung oder Änderung (**Bestandsdaten**) sowie Erfüllung (**Nutzungsdaten**) zwingend erforderlich sind.

Darüber hinausgehend darf die Diensteanbieterin personenbezogene Daten der Nutzer*innen gemäß Art. 6 Abs. 1 lit. f DS-GVO, § 6 Nr. 8 DSG-EKD nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien **tatsächlich zu ermöglichen und/oder abzurechnen (Nutzungsdaten)**, soweit die Datenschutzinteressen der Betroffenen im Einzelfall nicht höher zu bewerten sind. Erlaubt sind also zB. Datenverarbeitungen der IP-Adresse während der Dauer des reinen Surfens auf einer Website.

Zu den Nutzungsdaten, die ausschließlich zweckgebunden erhoben werden dürfen, können auch Merkmale zur Identifikation der Nutzer*innen, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die von den Nutzeri*innen in Anspruch genommenen Telemedien verarbeitet werden, wenn diese z. B. für Abrechnungszwecke erforderlich sind. Wird zum Beispiel ein bestimmtes Online-Angebot bei Inanspruchnahme nach Minuten abgerechnet, so stellen die Login-Daten der Nutzerin und die protokollierte Verbindungsdauer ein entsprechendes Nutzungsdatum dar.

Nutzungsdaten dürfen über das Ende des Nutzungsvorgangs hinaus verwendet werden, soweit sie für Zwecke der Abrechnung erforderlich sind (Abrechnungsdaten – § 15 Abs. 4 TMG) und – im Rahmen eines AV-Vertrags (§§ 28, 29 DS-GVO) – auch an andere Diensteanbieterinnen sowie Dritte übermittelt werden, soweit dies zur Ermittlung des Entgelts und seiner Abrechnung erforderlich ist (§ 15 Abs. 5 S. 1 TMG). Gemäß § 15 Abs. 6 TMG darf die Abrechnung aber nicht die Inanspruchnahme von Telemedien-Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einer Nutzerin/einem Nutzer in Anspruch genommener Telemedien erkennen lassen, es sei denn, die Nutzerin/der Nutzer verlangt einen Einzelnachweis.[131] Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf die Diensteanbieterin die Daten sperren (§ 15 Abs. 4 S. 2 TMG).

Im Ergebnis entspricht das Vorstehende nichts anderem als den Grundsätzen der Datenminimierung und Speicherbegrenzung sowie Zweckbindung und Rechtmäßigkeit. Daten dürfen nur soweit und solange gespeichert werden, wie es zur Erreichung des jeweils legitimen – durch Gesetz, Vertrag oder Einwilligung begründeten – Zwecks erforderlich ist.

B.2.2.4.2.3 Fernmelde-/Telekommunikationsgeheimnis

§ 88 TKG konkretisiert das in Art. 10 GG bereits verfassungsrechtlich verankerte Fernmeldegeheimnis (auch als sogenanntes Postgeheimnis bekannt). Geschützt ist die Vertraulichkeit der Nutzung des zur Nachrichtenübermittlung eingesetzten technischen Mediums, nicht aber das Vertrauen der Kommunikationspartner zueinander. Risiken, die nicht in der telekommunikativen Übermittlung, sondern in Umständen aus dem Einfluss- und Verantwortungsbereich eines der Kommunizierenden begründet sind, werden daher nicht erfasst. Hier greifen dann aber insbesondere die §§ 201 ff. StGB, die den Schutz der Vertraulichkeit strafbewehren.

Schon die Tatsache, dass jemand an einer Telekommunikation beteiligt war, unterfällt dem Fernmeldegeheimnis. Ruft jemand beispielsweise die Telefonseelsorge an, darf die Rufnummer der Anruferin/des Anrufers **grundsätzlich nicht gespeichert** werden, denn das Angebot ist ja kostenlos, so dass der Grund zur temporären Speicherung von Nutzungsdaten entfällt.[132]

B.2.2.4.3. Sonstige Anforderungen und Besonderheiten

B.2.2.4.3.1 Datenschutzerklärung/ -Information[133]

Websites benötigen eine Datenschutzerklärung. Zwar sind die Anforderungen an eine Unterrichtung der Nutzer durch die DS-GVO gestiegen. Viele der durch das Gesetz verlangten Informationen müssen für jede Funktion der Website gesondert bewertet werden. Daher bleibt es nicht aus, dass der Umfang der Datenschutzerklärungen weiter zunehmen wird. Da dies im Zweifel zu längeren Datenschutzerklärungen führt, birgt es die Gefahr, dass die damit bezweckte Transparenz der

[131] Zur Speicherdauer erklärt § 15 Abs. 7 und 8 TMG: Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten weiter gespeichert werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist. Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

[132] Etwas anderes kann dann gelten, wenn die Speicherung aus anderen Gründen erforderlich ist; etwa zum Führen einer Sperrliste, die vor missbräuchlichen Kontaktaufnahmen schützen soll.

[133] Siehe zu deren Erstellung die „Arbeitshilfe zur Umsetzung von Informationspflichten“ des Beauftragten für den Datenschutz der EKD (https://datenschutz.ekd.de/wp-content/uploads/2019/06/bfd_Handr-Infopflichten-dina5_Internet_01-2020.pdf – zuletzt abgerufen am 26. Juni 2020).

Datenverarbeitung mangels Kenntnisnahme durch die Nutzer nicht erreicht wird.

Eine gestufte Darstellung, etwa mit Einrückungen und Hervorhebungen (ein sogenannter **„layered approach“**), kann die Lesbarkeit verbessern und damit die Rechtswirksamkeit deutlich erhöhen. Je mehr Daten erhoben werden, desto umfänglicher muss informiert werden, und desto mehr muss in einem fortwährenden Überprüfungsprozess die Richtigkeit der Information sichergestellt werden.[134]

Im Falle von Verarbeitungen im Rahmen von Verträgen oder Einwilligungen sind die Informationen zusätzlich bereits vor Vortragsabschluss bzw. Einwilligung bereitzustellen. Die Informationen müssen gem. Art. 13 Abs. 1 DS-GVO spätestens aber „bei Erhebung“ der personenbezogenen Daten gegeben werden. Datenschutzerklärungen sollten – ebenso wie Impressen – regelmäßig **mit nur einem Klick erreichbar** sein.[135]

Praxistipp:
Datenschutzerklärungen orientieren sich in der Praxis häufig an der Struktur der Art. 13, 14 DS-GVO bzw. §§ 17, 18 DSG-EKD. Unter der Überschrift „Zwecke“ werden dann alle Zwecke sämtlicher Datenverarbeitungen zusammengefasst und entsprechend unter der Überschrift „Rechtsgrundlagen“ alle entsprechenden Rechtsgrundlagen usw. Dies dürfte eine transparente Information der Nutzer*innen häufig behindern.

Transparenter ist eine Datenschutzerklärung, die nach Zwecken differenziert und je Zweck jeweils die Rechtsgrundlage, den oder die Empfänger/Empfängerkategorie(n), die Frage der Drittlandübermittlung, die Speicherdauer bzw. Kriterien für die Speicherdauer etc. angeben. Angaben aber, die vom Zweck unabhängig sind, und als allgemeine Angaben „vor die Klammer“ gezogen werden können, sollten auch entsprechend konzentriert dargestellt werden: Das sind im Wesentlichen die Angabe

- der verantwortlichen Stelle (es sei denn, Teile der Datenverarbeitung sind Fälle von Gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO);
- des Datenschutzbeauftragten;
- das Beschwerderecht bei der Aufsichtsbehörde (und die [bundeslandspezifische] Angabe derer);
- die Rechte der betroffenen Person (ausgenommen aber die Information über das Widerspruchsrecht nach Art. 21 DS-GVO sowie über das Recht zum Widerruf einer Einwilligung Art. 13 Abs. 2 lit. c Art. 7 Abs. 3 S. 3 DS-GVO, weil diese Rechte nur bei bestimmten Rechtsgrundlagen der Verarbeitung gegeben sind).

Wenn über mehrere Arten von Datenverarbeitungen informiert werden soll, kann es sich anbieten, die Datenschutzerklärung teilweise (also hinsichtlich der zweckspezifischen Angaben) in tabellarische Form zu fassen. Das gilt insbesondere, wenn nach Art. 14 Abs. 1 lit. d DS-GVO auch über die Datenkategorien informiert werden muss. Als Spalten einer solchen Tabelle kommen beispielsweise uA. in Betracht (von links nach rechts):

- Zweck;
- (soweit nach Art. 14 Abs. 1 lit. d DSGVO erforderlich: Datenkategorien);
- Quelle (jedenfalls wenn die Quelle nicht der Nutzer selbst ist, siehe Art. 14 Abs. 2 lit. f DS-GVO);
- Rechtsgrundlage;
- Speicherdauer/Kriterien für die Speicherdauer;
- Empfänger/Empfängerkategorie(n);
- ggf. Information nach Art. 13 Abs. 1 lit. d, Art. 13 Abs. 2 lit. c DS-GVO sowie Information über das Widerrufsrecht.

Einen guten Leitfaden für die Erstellung einer gleichermaßen effektiven wie wirksamen Datenschutzerklärung/Datenschutzinformation bietet die „Arbeitshilfe zur Umsetzung von Informationspflichten“ des Beauftragten für den Datenschutz der EKD.[136]

Es sei betont, dass die Erfüllung der Informationspflichten nach Art. 12 – 14 DS-GVO bzw. §§ 16 – 18 DSG-EKD nicht mit dem Einholen einer Einwilligung nach Art. 6 Abs. 1 lit. a iVm. Artt. 7 und 8 DS-GVO/§ 6 Ziff. 2 iVm. §§ 11 und 12 DSG-EKD oder den ggf. zusätzlich notwendigen Nutzungsbedingungen (für den Telemediendienst) zu verwechseln sind. Die datenschutzrechtliche Einwilligung ersetzt auch ferner nicht die Notwendigkeit einer Einwilligung nach § 7 Unlauterer Wettbewerb-Gesetz (UWG) im Falle bestimmter Formen der werblichen Ansprache wie zB. durch Newsletter.[137]

Immer wieder übersehen Anbieterinnen, dass die Vermischung von Unterrichtung (Information), Einwilligung und ggf. Nutzungsbedingungen unter dem Begriff „Datenschutzerklärung“ schon im Hinblick auf Wirksamkeits- und Einbeziehungsrisiken problematisch ist. Während eine Einbeziehung der Datenschutzerklärung im Sinne von Art. 12–14 DS-GVO bzw. §§ 16 – 18 DSG-EKD in einen zu schließenden Vertrag als reine Unterrichtung

[134] Daten müssen grundsätzlich beim Betroffenen selbst erhoben werden. Stammen Sie dennoch aus anderen z. B. öffentlich zugänglichen Quellen, über die der Betroffene seine Daten selbst zugänglich gemacht hat (z. B. Social Media, Adress-/Telefon-Datenbanken, Mitarbeiter-Webseiten von Unternehmen), dann treffen die Datenverarbeiterin dennoch – nachträgliche – Informationspflichten (Art. 14 DS-GVO, § 18 DSG-EKD).

[135] Working Paper 260 der Artikel–29-Datenschutzgruppe, S. 8.

[136] https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-umsetzung-von-informationspflichten/ (zuletzt abgerufen am 26. Juni 2020).

[137] Gemäß § 7 Abs. 3 UWG ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post ausnahmsweise nicht anzunehmen, wenn 1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, 2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, 3. der Kunde der Verwendung nicht widersprochen hat und 4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

nicht notwendig ist, gelten für Einwilligungserklärungen die strengen Einbeziehungs- und Wirksamkeitsvoraussetzungen des Art. 7 DS-GVO bzw. § 11 DSG-EKD sowie – AGB-rechtlich – des § 305 Abs. 2 und 3 BGB. Ebenso unterliegt die Einbeziehung von Nutzungsbedingungen der Prüfung nach § 305 Abs. 2 und 3 BGB. Ein einfacher Hinweis am unteren Rand einer Website dürfte den gesetzlichen Anforderungen an die Einbeziehung nicht genügen.

B.2.2.4.3.2 Social-Media-Plugins

Social-Media-Plugins sollten **nicht direkt in die Website implementiert** werden, da sonst die IP-Adresse der Nutzer*innen bei Aufruf unmittelbar übermittelt wird. Über die **Zwei-Klick-Methode** kann eine sichere Einbindung erfolgen. Der erste Klick öffnet das Fenster mit den Datenschutzhinweisen und erst ein ggf. erfolgender zweiter, die notwendige Einwilligung beinhaltender Klick lädt das betreffende Plug-In. Der Einsatz von Social-Media-Plug-Ins ist in der Datenschutzerklärung vollständig und verständlich zu verdeutlichen.[138]

Zu beachten ist, dass die **Einbindung von Dritt-Inhalten** einen Beitrag der Website-Betreiberin als **aktiver Beitrag** zur Entscheidung über die Mittel der Verarbeitung darstellt und damit eine **datenschutzrechtliche (Mit-)Verantwortlichkeit** begründen kann. Nach Ansicht des EuGH kann allein daraus eine **gemeinsame Verantwortlichkeit** iSd. Art. 26 DS-GVO/§ 29 DSG-EKD für rechtswidrige Verarbeitungsvorgänge oder die nicht ausreichende Beachtung datenschutzrechtlicher Vorgaben durch den Dritt-Anbieter erwachsen.[139]

B.2.2.4.3.3 Newsletter

Sofern über die Website die Anmeldung für einen Newsletter möglich sein soll, welche stets einwilligungspflichtig sind, ist das Anmeldeformular datensparsam und datenschutzfreundlich und inklusive eines Datenschutzhinweises[140] zu gestalten. E-Mail-Adressen oder Mobilnummern sind dabei über das **Double-Opt-in-Verfahren** zu verifizieren. Checkboxen sollten **nicht vorangekreuzt** sein. Über die zum Versand ggf. genutzte Dienstleisterin ist in der Datenschutzerklärung entsprechend zu informieren. In jeder als Newsletter versandten E-Mail etc. ist die Möglichkeit zur **Austragung** aus dem Newsletter zu gewähren.

B.2.2.4.3.4 Gemeinsame Verantwortlichkeit

Wesentlich für Kooperationen ist zudem **die Regelung zur gemeinsamen Verantwortlichkeit**, Art. 26 DS-GVO, § 29 DSG-EKD. Hierzu ist eine **Vereinbarung zu schließen**.[141] Hieraus können sich gerade für Plattformen besondere Konsequenzen ergeben. So entschied etwa der EuGH, dass vor dem Hintergrund dieser Regelung ein Anbieter auch dann als verantwortlich gelten kann, wenn er die von jemand anderem bereitgestellte Plattform zum Anbieten der eigenen Leistung **lediglich nutzt**.[142]

Was zunächst nach einer umfassenden Mitverantwortlichkeit aussah, hat der EuGH mittlerweile zwar dergestalt konkretisiert, dass die Verantwortlichkeit auf den Vorgang bezogen wird, für den die Beteiligten **eine gemeinsame Entscheidung über die Zwecke und Mittel** treffen,[143] für den also die Anbieterin **immerhin faktisch (mit)entscheidet**. Daher seien die einzelnen Vorgänge, wie zB. das Erheben, das Erfassen, das Speichern der Daten etc. jeweils für sich für die Verantwortlichkeitszuteilung zu bewerten. **Nicht der gesamte Datendurchlauf unterliegt also automatisch der gemeinsamen Kontrolle und Verantwortlichkeit**. Allerdings sind die eine gemeinsame Verantwortlichkeit in der jeweiligen Konstellation möglicherweise begründenden Umstände und die daraus ggf. folgenden Konsequenzen **gut zu durchdenken**.[144]

Es ist anzunehmen, dass die Rechtsprechung des EuGH, der um die systemische Bedeutung von Plattformen weiß, und deren Nachvollziehung durch die einzelnen Datenschutzbehörden erhebliche Rückwirkung auf Plattformen haben werden. Schon bei der Entscheidung ob und ggf. welche Plattform zu Eigendarstellung und Angebot der Leistungen gewählt wird, müssen nun auch datenschutzrechtliche Erwägungen einfließen. Für die Anbieterinnen einer Plattform folgt daraus die Bestärkung der Verpflichtung, die Plattform datenschutzkonform und **risikoavers** auszugestalten.

Aber auch umgekehrt wird ein Schuh daraus. Denn die Begründung der gemeinsamen Verantwortlichkeit bedeutet im Ergebnis, dass die Plattformbetreiberin möglicherweise mitverantwortlich für die auf der Plattform durch Anbieterinnen angebotenen Anwendungen ist. Insoweit ist es wichtig, dass auch die Plattformbetreiberin die Anbieterinnen auf Datenschutzkonformität in Anspruch nimmt, um den eigenen **Sicherungspflichten** nachzukommen.

Aus der gemeinsamen Verantwortlichkeit ergeben sich auch Folgen für die Erfüllung der **Rechenschaftspflicht**[145], und zwar nicht nur der Form nach. Ist von einer gemeinsamen

[138] Siehe zur gemeinsamen Verantwortlichkeit ferner ausführlich unten B.2.2.4.3.4.
[139] Siehe die (kritische) Darstellung der Rechtsprechung des EuGH dazu bei Lee/Cross, (Gemeinsame Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites, MMR 9/2020, S. 559 ff. Siehe zur gemeinsamen Verantwortlichkeit ferner die Formulierungshilfe D.2.8: Vereinbarung Gemeinsam verantwortliche Stelle.
[140] Siehe hierzu B.1.5.3.
[141] Auf den Abschluss der in diesen Vorschriften bezogenen Vereinbarung haben die gemeinsam Verantwortlichen einen wechselseitigen Anspruch, und zwar bereits aufgrund § 26 DS-GVO/§ 29 DSG-EKD, die als unmittelbare Anspruchsgrundlage gelesen werden können.
[142] EuGH, NJW 2018, 2537 – Fanpage
[143] EuGH, BeckRS 2019, 15831 Rn. 85 – Fashion ID.
[144] Hierbei kann die Checkliste zur gemeinsamen Verantwortlichkeit des bitkom e.V. helfen: https://www.bitkom.org/sites/default/files/file/import/170515-Joint-Controllership-online.pdf (zuletzt abgerufen am 20. Oktober 2020).
[145] Die Rechenschaftsplicht aus § 5 Abs. 2 DSG-EKD/Art. 5 Abs. 2 DS-GVO beschreibt die Nachweispflicht der Datenverarbeiterin gegenüber den Datenschutzaufsichten, dass sie die Prinzipien eines effektiven Datenschutzes (Abs. 1) eingehalten hat.

Verantwortlichkeit auszugehen, so erstreckt sich die Nachweispflicht auch auf die betreffenden Anwendungen, die über die Plattform angebunden sind.

B.2.2.4.3.5 Mögliches Problem: Störerhaftung der Plattformbetreiberinnen

Auch wenn es im Rahmen der hier interessierenden möglichen Fallkonstellationen eher unwahrscheinlich ist, so soll der Vollständigkeit halber nicht unerwähnt bleiben, dass sich für Plattformbetreiberinnen in geeigneten Fällen eine Haftung für Rechtsverletzungen durch Nutzerinhalte ergeben kann. Zwar gelten entsprechende Pflichten des Netzwerkdurchsetzungsgesetzes (NetzDG) nur für Anbieter sozialer Netzwerke (wie etwa Facebook), § 1 Abs. 1 NetzDG. Als solche werden die hier interessierenden Konstellationen in aller Regel nicht gelten können.

Allerdings können sich ähnliche Pflichten auch aus **allgemeinen zivilrechtlichen Prinzipien wie der Störerhaftung**[146] ergeben, welchen der recht dichte Schutzschild der E-Commerce-Richtlinie Raum (RL 2000/31/EG) lässt. Denn gemäß Art. 14 Abs. 3 RL 2000/31/EG bleibt die **negatorische Haftung** der Plattformbetreiberinnen unberührt, also die Verpflichtung zur Beseitigung bereits eingetretener bzw. die Vermeidung zukünftiger Rechtsverletzungen im Rahmen der Löschung oder Sperrung rechtswidriger Informationen.

Spätestens aber mit Kenntnis eines möglicherweise rechtswidrigen User-Inhalts, die sich zB. aus Hinweisen auf bzw. Beschwerden über mögliche Rechtsverletzungen ergibt, hat seitens der Plattformbetreiberin eine rechtliche Prüfung sowie – bei festgestellter Rechtswidrigkeit – unverzügliche eine Löschung oder Sperrung des Inhalts zu erfolgen („Notice-and-take-down"-Prinzip). Denn ansonsten haftet die Plattformbetreiberin für den rechtswidrigen Drittinhalt umfassend wie für einen eigenen rechtswidrigen Inhalt.

Praxis-Tipp:
Wer diese Problematik gänzlich umgehen möchte, sollte die Verbreitung von Informationen durch Nutzer*innen entweder gar nicht oder nur moderiert zulassen.

B.2.2.4.3.6 Checkliste zu den (weiteren) Anforderungen an Websites

- Ist die Website entsprechend dem aktuellen Stand der Technik programmiert und betrieben?
- Sind bei Ihrer Programmierung/Gestaltung den Grundsätzen Privacy by Design und Privacy by Default genüge getan?
- Ist das mit der Erstellung der Website beauftragte Unternehmen schriftlich dazu verpflichtet worden, den aktuellen Stand der Technik einzuhalten und die Forderung nach Privacy by Design und Default zu erfüllen? Wird die Erfüllung bei Abnahme der Leistung überprüfend berücksichtigt?
- Werden über Formulare datenschutzkonform nur solche Daten abgefragt, die auch tatsächlich genutzt werden? Sind Pflichtfelder ggf. deutlich als Pflichtfelder gekennzeichnet? Werden nur diejenigen personenbezogenen Daten abgefragt, die zur Erreichung des jeweils legitimen – durch Gesetz, Vertrag oder Einwilligung abgesicherten – Zweckes notwendig sind?
- Sind die Informationen zur Verarbeitung persönlicher Daten im Vorfeld von Vertragsabschlüssen und Einwilligungen – und darüber hinaus auch die generelle Datenschutzerklärung – transparent, gut sichtbar eingebunden und leicht aufrufbar (maximal ein Klick)?
- Sind notwendige datenschutzrechtliche Einwilligungen wirksam und nachweisbar eingeholt?
- Ist die Datenschutzerklärung im Hinblick auf die zu gebenden Informationen vollständig (alle Verarbeitungen berücksichtigt, zB. auch Social Plug-ins) und dennoch übersichtlich gestaltet (ggf. „layered approach")?
- Ist die Seite hinreichend verschlüsselt (aktuelles ssl-Zertifikat) sowie alle Datenverarbeitungsprozesse durch die notwendigen TOM abgesichert?
- Sind ggf. Social-Media-Plugins sicher und transparent eingebunden und werden diese erst durch eine aktive und informierte Handlung der Nutzer*innen scharf geschaltet?
- Ist die Anbieterkennzeichnung (Impressum) vollständig und auf jeder Seite der Plattform vollständig verlinkt?
- Werden Skripte nur auf dem eigenen Server gespeichert und ist so ein Laden von Drittanbietern verhindert?
- Werden Fotos auf der Website grundsätzlich[147] nur bei Einwilligung der Abgebildeten verwendet (sofern diese erkennbar sind)?
- Sind alle Abbildungen rechtlich einwandfrei nutzbar (insbesondere hinsichtlich der Einhaltung von Urheberrechten [auch auf Zeitablauf von Lizenzen achten])?
- Ist die Anmeldung für einen Newsletter per Double-Opt-in gesichert? Können sich die Empfänger*innen in jedem Newsletter austragen und informiert die Datenschutzerklärung ggf. über die Newsletter-Dienstleisterin?
- Ist die professionelle Wartung der Website sichergestellt, um sie stets angriffssicher zu halten, wie das regelmäßige Backup?
- Ist eine möglicherweise gegebene gemeinsame

[146] Als Störer kann im Rahmen von Internetangeboten jeder gelten, der zur Verbreitung eines rechtlich zu beanstandenden Inhalts beiträgt. Die Weiterentwicklung des internetspezifischen Haftungsregimes führt aber mittlerweile zu einer Intensivierung der Haftung von Plattformbetreibern und so dazu, sich die Grenzen zwischen Störer- und Verletzerhaftung mehr und mehr aufzulösen. Hierzu Wagner, Haftung von Plattformen für Rechtsverletzungen (Teil 2), in GRUR 2020, S. 447 – 457.

[147] Zur Verwendbarkeit von Personenfotos ohne Einwilligung siehe § 23 Abs. 1 KUG.

Verantwortlichkeit hinreichend bedacht und das aus ihr ggf. folgende Risiko durch angemessene Vereinbarungen moderiert?
- Ist die Einbindung von datenverarbeitenden Drittdiensten durch Auftragsverarbeitungsverträge inkl. Weisungsrechten gegenüber dem Drittdienst abgesichert?
- Ist – soweit nötig – eine Datenschutz-Folgenabschätzung[148] durchgeführt worden?
- Ist die Möglichkeit der Störerhaftung gesehen worden und in die Planung eingeflossen?
- Werden ggf. Lieferbeschränkungen, Lieferzeiten, Versand- und Zusatzkosten sowie die Zahlungsmöglichkeiten korrekt und eingangs eines Bestellvorganges benannt?
- Sind die AGB rechtlich überprüft? Werden sie ggf. wirksam in über die Website begründete Vertragsverhältnisse einbezogen?
- Ist ggf. die Widerrufsbelehrung korrekt und auf der Bestellseite deutlich mit Hinweis auf das Widerrufsrecht verlinkt?
- Ist ggf. eine Leistungs- und Produktbeschreibung vollständig erfolgt (Merkmale einer vertraglich angebotenen Leistung bzw. eines Produkts inkl. der ggf. bestehenden Kennzeichnungspflichten)?
- Sind ggf. erfolgende Preisangaben (stets inkl. MwSt. und Versand- und sonstigen Kosten) vollständig und korrekt?
- Kommt ein Vertragsschluss ggf. informiert, transparent und widerspruchsfrei zustande?[149] Ist ein ggf. zugrundeliegender Bestellvorgang transparent ausgestaltet (inkl. einer klaren und verständlichen Bestellzusammenfassung vor Bestellabsendung und korrekter Button-Beschriftung)?
- Wird bei Bestellung ein ggf. erfolgender Vertragsschluss unverzüglich automatisiert per E-Mail inkl. aller notwendigen Informationen (AGB, Widerrufsbelehrung und sonstige Informationspflichten) bestätigt?

B.2.2.4.3.7 Exkurs: Onlinezugangsgesetz OZG

Das Onlinezugangsgesetz[150] und sein gleichermaßen überfälliger wie ambitionierter Umsetzungsplan[151] machen deutlich, dass schon bald (bis 2022) viele einschlägige Verwaltungsleistungen online abgerufen werden können. Dafür sollen zwei Digitalisierungsprogramme, eines auf Bundes- und eines auf Landesebene, sorgen.

§ 1 Abs. 1 OZG verpflichtet alle Behörden von Bund und Ländern (einschließlich Kommunen), ihre Verwaltungsleistungen den Nutzer*innen bis 2022 auch (barrierefrei) elektronisch und über Verwaltungsportale zur Verfügung zu stellen. Erfasst sind alle Verwaltungsträger und auch die Bereitstellung von bisher noch nicht online verfügbaren Verwaltungsleistungen. Nur solche Verwaltungsleistungen sind ausgenommen, deren digitale Umsetzung objektiv unmöglich ist. Dabei kommen technische, rechtliche und wirtschaftliche Unmöglichkeiten in Betracht.

Technisch ist die Umsetzung unmöglich, wenn es nach den Naturgesetzen oder nach dem Stand von Wissenschaft und Technik schlechterdings nicht möglich ist, die Verwaltungsleistung online anzubieten (zB. eine Impfleistung oder die Abfallbeseitigung). Rechtlich ist die Umsetzung unmöglich, wenn sie durch Rechtsgründe verhindert wird, etwa durch die gesetzliche Pflicht des persönlichen Erscheinens. Eine wirtschaftliche Unmöglichkeit ist indessen schwer denkbar. Diese wäre nur gegeben, wenn die Online-Zurverfügungstellung der Verwaltungsleistung einen Aufwand verlangte, der in einem groben Missverhältnis zum Ziel des OZG steht. Das kann im Ergebnis nur dann angenommen werden, wenn „kein vernünftiger Mensch“ die Umsetzung in Anbetracht der Kosten in Betracht zöge.

Vor dem Hintergrund der umfassenden Digitalisierung der Verwaltung wird eine Verknüpfung der eigenen digitalen Angebote mit den durch die Digitalisierung der Verwaltung neu entstehenden Pfaden immer attraktiver und damit – zumindest à la longue – auch nötiger. Bei der Anbindung ist **auf zweierlei besonders zu achten**. Zum einen auf die durch § 5 OZG thematisierte IT-Sicherheit, zum anderen auf die Bestimmungen des § 6 OZG zu den Kommunikationsstandards. Zu beiden insoweit von jeder Anbindung einzuhaltenden Standards sind vom Bundesministeriums des Innern, für Bau und Heimat ohne Zustimmung des Bundesrates zu erlassende Rechtsverordnungen zu erwarten.

Das Bundesinnenministerium gibt in einem OZG-Dashboard[152] einen Überblick über bereits online verfügbare Verwaltungsleistungen. Ferner bietet es ein mit dem OZG-Infoportal[153] einen Einblick in die Umsetzung von OZG-Leistungen.

[148] Siehe hierzu C.1.1.1.8.

[149] Sofern es sich um Beratungsangebote handelt, sollte nur eine verschlüsselte E-Mail-Kommunikation erfolgen. Diese kann auch über eine rein webbasierte E-Mail-Kommunikation, also etwa die (automatische) Bereitstellung eines Web-Postfaches mit einer eigens für die Nutzerin angelegten Adresse erfolgen, was nur noch einen Web-Login der Nutzerin in dieses Postfach voraussetzt.

[150] Gemeinsam mit dem EGovG und dem Regierungsprogramm „Digitale Agenda 2020“ soll es die notwendigen Voraussetzungen für die Überführung der staatlichen Verwaltung in die Digitalära schaffen.

[151] https://informationsplattform.ozg-umsetzung.de/iNG/app/fullsearch?search=umsetzungskatalog&offset=0 (Anmeldung notwendig – zuletzt abgerufen am 17. Juli 2020). Insgesamt sind dort rund 600 gemäß OZG zu digitalisierende Verwaltungsleistungen (sogenannte OZG-Leistungen) identifiziert. Sie sind im Umsetzungskatalog in Leistungen in 35 Lebens- und 17 Unternehmenslagen gebündelt und 14 übergeordneten Themenfeldern (zum Beispiel „Familie & Kind“) zugeordnet. Der OZG-Umsetzungskatalog orientiert sich dabei nicht an behördlichen Zuständigkeiten, sondern an der Nutzerperspektive von Bürger*innen sowie Unternehmen.

[152] https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/dashboard/ozg-dashboard/ozg-dashboard-node.html (zuletzt abgerufen am 05. Dezember 2020).

[153] https://informationsplattform.ozg-umsetzung.de/iNG/app/intro (zuletzt abgerufen am 05. Dezember 2020).

Aufgrund des eID-Karte-Gesetzes soll zudem nicht-deutschen EU/EWG-Bürgern ein Zugang zu deutschen Verwaltungsportalen mittels einer elektronischen ID-Karte ermöglicht werden.

B.2.2.4.3.7.1 Checkliste OZG

- Ist bei der Entwicklung einer Anwendung die Anbindung an den öffentlichen Portalverbund nach OZG geprüft und ggf. beachtet?
- Werden bei der Entwicklung der Anwendung die Standards der nach §§ 5 und 6 OZG durch das Bundesministerium des Innern, für Bau und Heimat zu erlassenden Rechtsverordnungen berücksichtigt?

B.2.2.5 Verantwortung und Haftung für Inhalte im Internet

B.2.2.5.1 Einführung

Die Frage, wer Verantwortung für Inhalte im Internet übernehmen muss, wird umso wichtiger, je größer die Bedeutung des Mediums für die Gesellschaft wird. Gerade in den letzten Jahren ist daher auch die Diskussion um die Verteilung von Verantwortung immer stärker in den Vordergrund getreten. Dies umso mehr, je mehr sich abzeichnete, wie verletzlich das gesellschaftliche Miteinander den Möglichkeiten der neuen digitalen Medien gegenübersteht. Insbesondere im Hinblick auf Hass und Hetze ist einiges zu tun, will man den gesellschaftlichen Frieden sichern. Insoweit ist der Druck auf Gesetzgeber wie auch Justiz stetig gestiegen und sind die damit korrespondierenden Anforderungen an Akteure im Internet stetig gewachsen.

Dem Bedürfnis nach Rechtssicherheit ist der europäische wie nationale Gesetzgeber durch Erlass einiger wichtiger Regelungen (zB. des Telemediengesetz [TMG][154] auf deutscher Ebene) nachgekommen. Einen bedeutenden Anteil an einer juristischen Lösungsfindung hat allerdings die Rechtsprechung. In den letzten anderthalb Jahrzehnten hat der BGH immer wieder zu wesentlichen Fragestellungen des Internetrechts, insbesondere zu Fragen der Verantwortlichkeit, Entscheidungen getroffen, die wesentliche Regeln aufstellten und diese wie auch die ihnen zugrundeliegenden gesetzlichen Vorgaben weiter konkretisierten.

Vor diesem Hintergrund ist das **Haftungsrisiko** für Provider als Diensteanbieter, die fremde Informationen speichern, zum Abruf bereithalten oder durchleiten, in der Praxis erheblich gewachsen. Ganz gleich, ob es sich um **Content-, Access-, Cache- bzw. Usenet- oder Hostprovider** handelt –[155] fast alle verarbeiten erhebliche Mengen an Daten, die sich schon aufgrund ihres Umfanges einer verantwortungsvollen inhaltlichen Prüfung zu entziehen scheinen. Demgemäß hoch ist das Bedürfnis, sich gegen potentielle Haftungsrisiken abzusichern.

Wesentlich sind insoweit die bereits angesprochenen Regelungen des TMG, die zugunsten der Internetakteure Haftungsbeschränkungen normieren. Das TMG **regelt aber die Anspruchsgrundlagen nicht selbst**. Da es an einer weiteren spezialgesetzlichen Normierung fehlt, finden insoweit und im Übrigen die **allgemeinen gesetzlichen Regelungen Anwendung**, die auch in der analogen Welt Geltung beanspruchen. Hinzu tritt die schon angesprochene umfangreiche Kasuistik der Gerichte, insbesondere die des BGH. Daher kann von einer **halbwegs gesicherten Rechtslage** ausgegangen werden

Der Gesetzgeber wird das **Normengefüge in naher Zukunft indes weiter ausgestalten bzw. überarbeiten**, etwa durch die **E-Privacy-Verordnung** (dazu unter B.2.2.3) sowie den Digital Services Act (siehe dazu B.2.2.5.6), was besonders zu beobachten ist.

B.2.2.5.2 Eigene und fremde Inhalte

Die Unterscheidung, ob es um selbst eingestellte Inhalte geht, oder um solche, die von Dritten stammen und anderen Nutzer*innen „nur“ zur Verfügung gestellt werden, hat entscheidende Bedeutung. § 7 Abs. 1 TMG betont zunächst den – ohnehin und selbstverständlich – geltenden Grundsatz, dass jede und jeder für das eigene Handeln (dazu gehören Tun wie Unterlassen) verantwortlich ist. Dabei besteht keinerlei Unterschied zwischen der analogen und der digitalen Welt – weder bezüglich der möglichen Anspruchsgrundlagen der Betroffenen noch der Rechtsfolgen, die sich aus ihnen ergeben. Es **haftet also der Internetprovider für eigene, aber auch zu eigen gemachte Inhalte vollumfänglich nach den allgemeinen Gesetzen**, wobei es nicht darauf ankommt, ob diese Inhalte auf eigenen oder fremden Servern vorgehalten werden. Umfasst sind insbesondere Ansprüche und Sanktionen aus dem allgemeinen Zivilrecht, dem Immaterialgüterrecht (zB. dem Urheberrecht) und dem Strafrecht. Und natürlich ist auch unerheblich, ob die Anbieterin eine Privatperson, eine Unternehmerin oder eine Körperschaft ist. Ebenso wenig spielt eine Rolle, ob das Angebot gewerblicher oder gemeinnütziger Natur ist.

[154] Das TMG hat das Teledienstegesetz (TDG) und den Mediendienstestaatsvertrag (MDStV) im Jahre 2007 abgelöst.

[155] Content-Provider stellen eigene Inhalte selbst zur Verfügung, wogegen ein Host-Provider fremde Informationen und Inhalte auf seinem eigenen Webserver und den eigenen Seiten einstellt. Access-Provider vermitteln dagegen fremde Informationen im Internet oder anderen Netzen bzw. leiten sie durch bzw. ermöglichen überhaupt rein technisch den Zugang zum Internet. Als Usenet-Provider bezeichnet man gemeinhin Betreiberinnen eines Netzwerkes von Diskussionsforen im Internet, die die Daten nur im Wege des „Mirrorings“ redundant speichern. Als Oberbegriff wird gemeinhin „Internetprovider“ gewählt.

Eigenen Inhalten nach der Rechtsprechung gleichgestellt sind solche, die zwar fremden Ursprungs sind, die sich der Provider zu eigen gemacht hat. Ein **Zueigenmachen** liegt insbesondere vor, wenn der Provider die fremden Inhalte so übernimmt, dass er dem Gesamtbild nach erkennbar für sie die Verantwortung übernehmen will,[156] was bereits aus einer gezielten Verlinkung, insb. Deep-Links, von Webinhalten Dritter folgen kann.[157]

Diesen allgemeinen Teil vorausgeschickt, können im Folgenden die im vorliegenden Zusammenhang interessierenden Haftungsbereiche genauer betrachtet werden.

B.2.2.5.3 Die Haftungserleichterungen der E-Commerce-Richtlinie (RL 2000/31/EG); §§ 7ff. TMG

Die Plattformbetreiberin als Gatekeeper für fremde Inhalte hat **keine allumfassende Verantwortung für durch Dritte begangene Rechtsverletzungen**. Sie haftet insoweit nicht wie für eigene Inhalte. Eine vollumfängliche Haftung der Internet-Intermediäre für rechtsverletzende Inhalte Dritter würde nach dem EGMR darauf hinauslaufen, „exzessive und unpraktikable Voraussicht zu verlangen, welche die Freiheit untergraben kann, im Internet Informationen zu verbreiten."[158]

Vor diesem Hintergrund hat die (mittlerweile) durch das TMG (diesbezüglich in §§ 7ff.) nachvollzogene E-Commerce-RL in ihrem Art. 15 Abs. 1 Zugangsanbieter, die lediglich die Verbindung mit dem Internet herstellen (Access-Provider), sowie Speicherplatzanbieter, die sich darauf beschränken, virtuelle „Gastgeber" (Hosts) für die Inhalte ihrer Nutzer zu sein (Host-/Service-Provider), ausdrücklich von der Verpflichtung freigestellt, die gespeicherten Daten vor ihrer Zugänglichmachung auf Rechtsverletzungen hin zu überprüfen (vgl. § 7 Abs. 3 TMG). Auch außerhalb des Anwendungsfeldes der E-Commerce-RL hat der BGH diese Privilegierung nachvollzogen.[159] Ebenso sieht der EuGH in seinen Entscheidungen zur DSGVO die Anbieterinnen lediglich in der Pflicht, rechtswidrige Inhalte auf Antrag der Rechteinhaber zu löschen.[160] Und das BVerfG liegt ebenfalls auf dieser Linie.[161]

Steht nach Überprüfung einer Beanstandung, deren Berechtigung sich ohne großen Aufwand überprüfen lassen muss, aber eine „klare Rechtsverletzung" fest, hat die Plattformbetreiberin also **positive Kenntnis**, muss sie **unverzüglich reagieren** und den inkriminierten Inhalt vom Netz nehmen (**notice and take down**).[162] Daneben tritt automatisch die Verpflichtung, im Rahmen des Zumutbaren die Wiederholung derselben und gleichartiger Rechtsverletzungen zu verhindern (**stay down**).[163] Eine derartige an die Kenntnis der Rechtsverletzung geknüpfte Intensivierung der Sorgfaltspflichten der Plattformbetreiberin harmoniert durchaus mit allgemeinen haftungsrechtlichen Grundsätzen;[164] und sie steht auch mit der europarechtlichen Vorgabe des Art. 15 Abs. 1 der E-Commerce-RL in Einklang. Es spielt auch keine Rolle, ob die Rechtsverletzerin selbst greifbar ist.[165] Privilegiert – sprich befreit von einem generellen Stay-down-Prinzip nach einem einmal erfolgten Hinweis – sind allerdings Suchmaschinenbetreiberinnen. Diese müssen grundsätzlich nur nach konkreten Hinweisen auf erkennbar rechtswidrige Suchergebnisse diese unverzüglich bereinigen.[166]

Die hier beschriebene Haftungsprivilegierung nach dem Notice-and-take-down-Prinzip gilt aber nur für fremde, **nicht für eigene Inhalte**. Im Gegensatz zu fremden Inhalten ist die Plattformbetreiberin für eigenes Verhalten, also insbesondere für eigene Inhalte, selbstverständlich v**ollumfänglich verantwortlich**. Denn jede und jeder ist verpflichtet, das eigene Verhalten so einzurichten, dass Gefahren für Rechtsgüter Dritter im Rahmen des Zumutbaren vermieden werden. Das heißt, dass eine bloße nachträgliche Kontrolle dann von vornherein ausscheidet, wenn es um eigenes Verhalten und eigene Inhalte geht. Dem stehen die Privilegierungen der E-Commerce-RL sowie das TMG nicht entgegen.

Bei fremden Inhalten kann sich – wie oben bereits angesprochen – zudem eine unbeschränkte **Haftung wie für eigene Inhalte** dann ergeben, wenn sich die Plattformbetreiberin diese **zu eigen gemacht hat**. Ein solches Zueigenmachen liegt nach der Rechtsprechung vor, wenn der Intermediär **nach außen zu erkennen gegeben** hat, dass er die inhaltliche Verantwortung für die von ihm bereit gehaltenen Fremdinhalte übernommen oder sich mit ihnen **identifiziert** hat.[167]

Ob dem so ist, ist nach Maßgabe des objektiven Empfängerhorizonts zu beurteilen, wobei im Zweifel nicht von einem Zueigenmachen auszugehen ist.[168] Dennoch sollten zur Qualitätssicherung, aber auch zur eigenen rechtlichen Absicherung eingebundene sowie verlinkte fremde Inhalte[169] grundsätzlich auf ihre Rechtmäßigkeit überprüft werden. Spätestens wenn **Fremdbeiträge kuratiert** werden, kann jedenfalls von einer Zueigenmachung ausgegangen werden. Im vorliegenden Zusammenhang wird ein Zueigenmachen im genannten Sinne wohl oft in Betracht kommen.

[156] Sobola, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Rz. 11 zu § 42.
[157] Siehe etwa BGH, Urteil vom 18.6.2015 - I ZR 74/14.
[158] EGMR NJW 2017, S. 2091 Rz. 82
[159] BGH GRUR 2018, S. 642 Rz. 34 – Internetforum; siehe auch OLG Dresden NJW-RR 2019, S. 676 Rz. 11.
[160] EuGH GRUR 2014, S. 895 Rz. 94 – Google Spain. Siehe auch § 7 Abs. 4 TMG.
[161] BVerfG GRUR 2020, S. 88 Rz. 113 – Recht auf Vergessenwerden II.
[162] BGHZ 158, S. 236 (252) = GRUR 2004, GRUR 2004, S. 860 – Internet-Versteigerung; BGH GRUR 2007, S. 708 Rz. 45 – Internet-Versteigerung II; BGH GRUR 2013, S. 370 Rz. 28 – Alone in the Dark.
[163] BGHZ 158, S. 236 (252) = GRUR 2004, GRUR 2004, S. 860 – Internet-Versteigerung; BGH GRUR 2007, S. 708 Rz. 45, 47 – Internet-Versteigerung II; BGH GRUR 2013, S. 370 Rz. 29ff. – Alone in the Dark; BGH GRUR 2015, S. 485 Rz. 52 – Kinderhochstühle im Internet III.
[164] Wagner, Haftung von Plattformen für Rechtsverletzungen (Teil 2), GRUR 2020, S. 447 (448).
[165] BGH Urt. v. 27.3.2007 – VI ZR 101/06, CR 2007, 586. Eine Unterordnung der mittelbaren Haftung der Plattformbetreiberin etwa im Sinne von § 59 Abs. 4 S. 1 RStV n.F. scheidet so aus.
[166] Zur Haftung von Suchmaschinen siehe etwa BGH, Urteil v. 27.02.2018, Az. VI ZR 489/16.
[167] BGH GRUR 2016, S. 855 Rz. 17 – www.jameda.de; GRUR 2010, S. 616 Rz. 24 – marions-kochbuch.de; NJW 2012, S. 2345 Rz. 11; NJW 2015, S. 3443 Rz. 25; NJW 2017, S. 2029 Rz. 18.
[168] Wagner, aaO. (Fn. 93), S. 449.
[169] Zur Haftung für verlinkte Inhalte siehe etwa BGH, Urteil vom 18.6.2015 - I ZR 74/14.

Praxis-Tipp:
Die Anbieterinnen eingestellter Inhalte sollten vertraglich auf die Überprüfung der Inhalte auf Rechtsverletzungen Dritter hin verpflichtet werden. Zusätzlich sollten sie zur Haftungsfreistellung zugunsten der Plattformbetreiberin verpflichtet werden, falls diese von Dritten in Anspruch genommen wird.

Die Betreiberinnen von Internet-Plattformen speichern die Angebote und Beiträge von Nutzer*innen, indem sie die diesbezüglichen Daten und Informationen für die Nutzer*innen selbst und für Dritte bereithalten. Sie sind damit hinsichtlich dieser Nutzerinhalte als **Hostprovider** tätig. Nach § 10 TMG und Art. 14 E-Commerce-RL kommt es für eine entsprechende Qualifizierung allein auf das **Abspeichern** der Inhalte an.[170] Sie können – mit Ausnahme ihrer eigenen sowie zu Eigen gemachter Inhalte – das Haftungsprivileg des § 10 TMG geltend machen. Anders als bloße Access-Provider, die Daten lediglich durchleiten, können sie sich hingegen nicht auf das umfassendere Privileg des § 8 TMG (das auf Art. 12 E-Commerce-RL gründet) berufen.[171]

In Rechtsprechung und Literatur besteht im Hinblick auf die gesetzliche Ausprägung der **Haftung insoweit Einigkeit, als eine Haftung einer Forumsbetreiberin in jedem Falle deren positive Kenntnis von der Rechtswidrigkeit der infrage stehenden Inhalte voraussetzt**, beispielsweise durch ein Anwaltsschreiben, das über die betreffenden Umstände unterrichtet bzw. durch Mitteilung durch die Rechteinhaber*innen selbst. Der Umfang der durch die Kenntnis begründeten Prüfpflichten bestimmt sich gemäß den **Grundsätzen der Störerhaftung** nach der **Zumutbarkeit**. Und um diese Zumutbarkeit der Prüfungs- und Kontrollpflichten rankt sich die **Einzelfallrechtsprechung** des BGH.

Der BGH stellt dabei insbesondere klar, dass nach § 7 Abs. 2 S. 1 TMG eine **allgemeine Vorab-Überwachungspflicht ausscheidet**.[172] Allerdings geht das nicht so weit, dass das maßgebliche Erforschen von Tathinweisen zu kerngleichen Fällen nach Kenntnis eines konkreten Verstoßes im Sinne einer „besonderen Überwachungspflicht“ ausgeschlossen wäre.[173] Im Rahmen des Zumutbaren sind daher Wiederholungen derselben und gleichartiger Rechtsverletzungen möglichst zu unterbinden (**stay down**).[174]

Dagegen schließt der BGH aber beispielsweise aus, dass die **Betreiberin eines Bewertungsportals** grundsätzlich verpflichtet wäre, die von den Nutzern ins Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen.[175]

B.2.2.5.4 Keine Spezialitäten bei Sozialen Netzwerken

Die Haftung von Betreiberinnen **sozialer Netzwerke**, also Netzwerken, bei denen auch die Nutzer*innen die Inhalte mitgestalten, unterscheidet sich inhaltlich nicht von dem oben Beschriebenen. Im Rahmen der beschriebenen Grundsätze der Störerhaftung, sofern es sich also nicht um eigene oder zu eigen gemachte Inhalte handelt, haften auch sie nur im Rahmen des Zumutbaren.

[170] Eine Einordnung als Access-Provider nach § 8 TMG dürfte regelmäßig ausscheiden. Der grundsätzliche Haftungsausschluss des Zugangsproviders nach § 8 TMG beruht darauf, dass die Tätigkeit beim bloßen Durchleiten von Daten automatisch erfolgt und der Provider damit keine Kenntnis der weitergeleiteten oder kurzzeitig zwischengespeicherten Informationen hat. Dagegen speichern Anbieterinnen von Plattformen, etwa Foren und Chatrooms etc. die Information der Nutzer*innen oder weiteren Anbieterinnen, zumindest kurzfristig, so dass ein Hosting im Sinne des § 10 TMG anzunehmen ist (siehe Sobola, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rz. 181f. zu § 42). Die Fälle der Durchleitung (§ 8 TMG/Art. 12 E-Commerce-RL) und des Cachings (§ 9 TMG/Art. 13 E-Commerce-RL) sind innerhalb des vorliegend interessierenden Themenkreises dagegen wohl kaum relevant und werden daher nicht eigens behandelt.

[171] Aber auch Access-Provider können insbesondere zur Sperrung verpflichtet sein, vgl. hierzu die Grundsatzentscheidung des BGH vom 26. November 2015 - I ZR 174/14. Nach Inkrafttreten des 3. TMÄndG stellte sich die Frage, ob der neu aufgenommene § 7 Abs. 4 TMG auch für solche Access-Provider gälte, die den Zugang nicht (allein) über WLAN gewähren. Vgl. zu der Thematik und insofern ergangenen neueren Entscheidungen die Anmerkung von Müller zum Urteil des LG München vom 07. Juni 2019 – 37 O 2516/18 – in MMR 8/2019, S. 539 ff.

[172] BGH Urt. v. 12. Juli 2007 – I ZR 35/04, CR 2007, S. 728 – Jugendgefährdende Medien bei e-Bay, Rz. 39, 41, 43.

[173] BGH Urt. v. 12.7.2007 – I ZR 35/04, CR 2007, 728 = BGHReport 2007, 1043 – Jugendgefährdende Medien bei e-Bay, Tz. 44.

[174] BGHZ 158, S. 236 (252) = GRUR 2004, GRUR 2004, S. 860 – Internet-Versteigerung; BGH GRUR 2007, S. 708 Rz. 45, 47 – Internet-Versteigerung II; BGH GRUR 2013, S. 370 Rz. 29ff. – Alone in the Dark; BGH GRUR 2015, S. 485 Rz. 52 – Kinderhochstühle im Internet III.

[175] BGH Urt. v. 1.3.2016 – VI ZR 34/15, GRUR 2016 – jameda.de.

B.2.2.5.5 Vertiefung: Prüfungsfolge zu einem Persönlichkeitsrechte verletzenden Blogeintrag in sozialen Netzwerken/Foren

Der Sache nach kommt eine Haftung regelmäßig aufgrund der Verletzung von Persönlichkeitsrechten in Betracht. Bezüglich dieser hat die Rechtsprechung des BGH mittlerweile die Prüfung etwas ausdifferenziert:

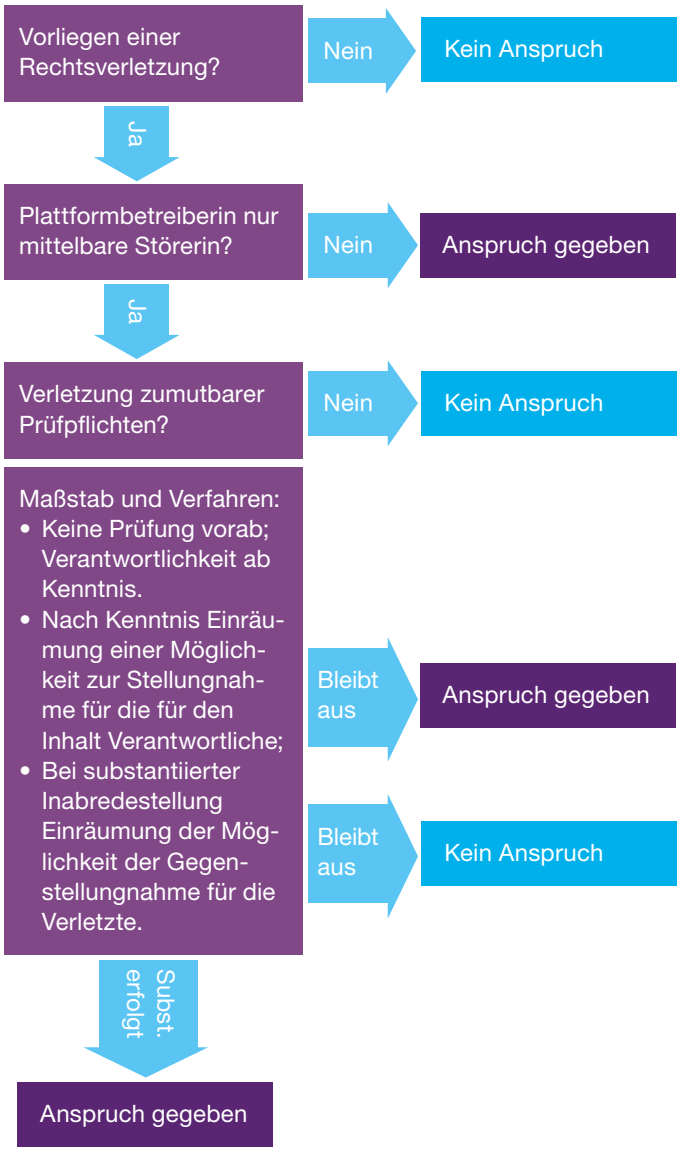


Fig. B.7. Vereinfachte Darstellung der Prüfungsfolge einer Verletzung des Persönlichkeitsrechts bei Plattformbetrieb

Im Einzelfall möglicherweise interessant ist noch die Konstellation des Cache-, insbesondere des **Usenet-Providers**.[176] Dabei geht es um Foren, deren Beiträge vom Provider nur „gespiegelt" („Mirroring"), also redundant gespeichert werden. Usenet-Provider gelten (lediglich) als Cache-Provider im Sinne des § 9 TMG, können regelmäßig dessen Haftungsbeschränkungen für sich in Anspruch nehmen und sich auch ex post weitreichend entpflichten, wenn eine Überprüfung technisch nicht möglich oder zumutbar ist.[177]

B.2.2.5.6 Exkurs: Digital Services Act (DSA – Gesetz für digitale Dienste)

Noch steht der Inhalt des Digital Services Act, der quasi eine Überarbeitung der E-Commerce-RL ist, nicht fest. Fest steht aber bereits, dass die Erwartungen an das Gesetz hoch sind. Die Präsidentin der Europäischen Kommission Ursula von der Leyen hat das Gesetz zu einem Leuchtturmprojekt erklärt.[178]

Das Gesetz soll zur **Vereinheitlichung der im Binnenmarkt geltenden Vorschriften**[179] führen und so einheitliche Verpflichtungen für Diensteanbieterinnen normieren. Möglicherweise wird das Gesetz im Sinne einer Art **Accountabilty-Framework** auch einer neuen EU-Aufsichtsbehörde den Weg ebnen, die die Durchsetzung der Regelungen zentral steuert und diese Aufgabe nicht – wie bei der DS-GVO – nationalen Autoritäten überlässt. Ferner soll der DSA den **fairen Wettbewerb** sichern und Eingriffsmöglichkeiten schaffen, die bereits greifen bevor eine Plattform eine **marktdominante Stellung** erreicht hat („ex-ante-Regulierung").[180] Zudem kann es die Pflicht zur **Interoperabilität** vorsehen, die Pflicht also, die eigenen Dienste dergestalt zu öffnen, dass sie mit anderen kompatibel werden. Beispielsweise könnte so WhatsApp gezwungen werden, Nachrichten auch mit anderen Apps wie Telegram oder Signal auszutauschen.

Schließlich ist damit zu rechnen, dass ein potenteres Haftungsregime eingeführt wird. Die bereits zwei Jahrzehnte alte E-Commerce-Richtlinie schützt – wie oben unter B.2.2.5.3 dargestellt – Diensteanbieterinnen bislang durch das sogenannte **Providerprivileg** vor einer direkten Haftung für Inhalte, die Nutzer*innen auf der Plattform hinterlassen. Im Rahmen des Notice-and-take-down-Verfahrens laufen Diensteanbieterinnen erst dann Gefahr, die Haftungsbefreiung zu verlieren, wenn sie offenkundig rechtswidrige Inhalte nach einem Hinweis nicht unverzüglich entfernen. Es ist aber ein all-

[176] Das Usenet ist ein weltweites elektronisches Netzwerk, das vom World Wide Web zu unterscheiden ist und lange vor ihm entstand. Es stellt in sogenannten Newsgroups fachliche Diskussionsforen aller Art in reiner Textform zur Verfügung, an welchen teilzunehmen grundsätzlich jedem offensteht. Dazu verwenden die Teilnehmenden üblicherweise einen Newsreader. Eine Parallelstruktur ist das Binary Usenet, das auch Binärdateien als Anhänge mitverteilen kann.

[177] Vgl. dazu etwa das Urteil des OLG Düsseldorf vom 15. Januar 2008, I-20 U 95/07.

[178] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (S. 13 – zuletzt abgerufen am 16. Juli 2020).

[179] Den Wildwuchs bilden beispielsweise das NetzDG in Deutschland und das französische Avia-gesetz, das allerdings vom französischen Verfassungsgericht zwischenzeitlich aufgehoben wurde.

[180] Das DSA soll dem Vernehmen nach ein „competition tool" beinhalten, das ein sog. „market tipping" (also das „Kippen" eines Marktes in ein Monopol eines Anbieters) verhindern soll.

gemeiner Trend feststellbar, nach welchem die **Verantwortung von Plattformbetreiberinnen zunehmend intensiviert** wird.[181] Die Haftungsprivilegien der E-Commerce-RL wanken und die Unterscheidung zwischen Störerin und Verletzerin verschwimmt zunehmend. Die Ausbildung eines kohärenten Haftungssystems scheint jedenfalls immer nötiger.

Es ist zu hoffen, dass der DSA das im Internet noch immer dominierende Geschäftsmodell der umfassenden Verwertung der von den Nutzer*innen hinterlassenen Daten einhegen wird. Und bei aller Notwendigkeit der Anpassung des Haftungsregimes muss die Reform darauf achten, das Problem privater Rechtsdurchsetzung nicht weiter zu verschlimmern.

B.2.2.5.7 Netzwerkdurchsetzungsgesetz (NetzDG)[182]

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) normiert Compliance-Regeln betreffend den Umgang mit Nutzer*innen-Beschwerden über **strafbare Hasskriminalität und Fake News im Netz** für Anbieter großer sozialer Netzwerke, genauer für Telemediendienste, die Plattformen betreiben, die dazu bestimmt sind, dass Nutzer*innen beliebige Inhalte mit anderen Nutzer*innen teilen oder der Öffentlichkeit zugänglich machen.[183] Zu den **Pflichten** gehören eine **vierteljährliche Berichtspflicht**, Vorgaben für ein **wirksames Beschwerdemanagement einschließlich von strengen Frist zur Löschung von strafbarem/n Hatespeech und Fake News**, die Benennung eines **inländischen Zustellungsbevollmächtigten** sowie der **Auskunftsanspruch** zugunsten von Opfern von Persönlichkeitsverletzungen im Netz auf Auskunft über Bestandsdaten der verletzenden Person (bei Vorliegen einer gerichtlichen Anordnung).

Für die im vorliegenden Zusammenhang interessierenden Anwendungen dürfte das NetzDG **keine bzw. nur eingeschränkte Bedeutung** besitzen. Dies liegt schon daran, dass die Kernpflichten zu Berichterstattung und Beschwerdemanagement (§§ 2 und 3 NetzDG) gemäß § 1 Abs. 2 NetzDG dann keine Anwendung finden, wenn das betreffende Netzwerk im Inland **weniger als zwei Millionen registrierte Nutzer*innen** hat. Allerdings bleibt auch im Fall der Unterschreitung der Erheblichkeitsgrenze die **Pflicht zur Bestellung eines inländischen Zustellungsbevollmächtigten** nach § 5 NetzDG bestehen.

Diese ist nur dann ausgeschlossen, wenn die Plattform **allein der Individualkommunikation oder der Verbreitung „spezifischer Inhalte“** oder selbst verantworteter journalistisch-redaktioneller Inhalte dient. Dazu können zB. Fachportale gehören, die sich nur an einen bestimmten Kreis von Nutzer*innen richten.

Im Übrigen setzt die Anwendbarkeit des NetzDG voraus, dass die Plattform eine **Gewinnerzielungsabsicht** verfolgt, wovon (nur) bei gewerblichen Unternehmen regelmäßig auszugehen ist.[184] An einer Absicht der Gewinnerzielung kann es auch fehlen, wenn eine Dauerhaftigkeit und Nachhaltigkeit des Dienstangebotes nicht vorliegt.[185]

Ein Reformgesetz zum NetzDG, welches für eine effektivere Rechtsdurchsetzung, aber auch bessere Nutzerrechte sorgen soll, befindet sich derzeit im Gesetzgebungsverfahren.[186]

Zudem soll in einem weiteren Gesetz für bestimmte strafbare, vor allem volksverhetzende Inhalte eine Meldepflicht der Plattformen gegenüber den Strafverfolgungsbehörden eingeführt werden.[187]

B.2.2.5.8 DSM-Richtlinie – Urheberrecht

Am 06. Juni 2019 ist die viel beachtete Directive on Copyright in the Digital Single Market (so genannte DSM-Richtlinie) in Kraft getreten; die zweijährige Umsetzungsfrist der Richtlinie in nationales Recht läuft.[188] Ziel der Richtlinie ist es, das Urheberrecht in der Union an die Erfordernisse der fortschreitenden Digitalisierung anzupassen, um die Rechteinhaber besser zu schützen. Im hier interessierenden Zusammenhang werden die Regelungen **kaum wesentliche Bedeutung** haben. So regelt Art. 17 DSM-RL die täterschaftliche Haftung von Online-Plattformen wie zB. Youtube, die ihren Nutzern das Speichern und die öffentliche Wiedergabe von urheberrechtlich geschützten Inhalten ermöglichen,[189] was inhaltlich im vorliegenden Zusammenhang wenig relevant sein dürfte.

Da sich die Regelungen der DSM-Richtlinie im Wesentlichen auf Plattformen mit einem erheblich erhöhten urheberrechtlichen Gefährdungspotenzial beschränken, sei daher nur kurz auf sie eingegangen. Gemäß Art. 17 Abs. 1, UAbs. 2 DSM-RL hat die Plattformbetreiberin zunächst die Pflicht, die Einwilligung der Rechteinhaberinnen einzuholen. Bei Nichterteilung

[181] Wagner, aaO. (Fn. 93), S. 453.
[182] Die Überarbeitung des NetzDG war zum Zeitpunkt des Redaktionsschlusses noch nicht abgeschlossen.
[183] E-Mail- und Messengerdienste fallen daher von vornherein nicht in den Anwendungsbereich.
[184] EuGH EuZW 2014, 672, 674.
[185] vgl. BVerwG ZfBR 2013, 45, 47.
[186] https://www.bundestag.de/dokumente/textarchiv/2020/kw19-de-netzwerk-durchsetzungsgesetz-692664 (zuletzt abgerufen am 5. Dezember 2020).
[187] Wegen verfassungsrechtlicher Bedenken hat der Bundespräsident bisher das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität nicht gezeichnet.
[188] Der jeweils aktuelle Umsetzungsstand kann hier eingesehen werden: https://www.urheberrecht.org/topic/Umsetzung-DSM/ (zuletzt abgerufen am 5. Dezember 2020).
[189] Diensteanbieter, die nicht unter die DTO-Definition von Art. 2 Ziff. 6 DSM-RL fallen, werden nicht nach dem Haftungsregime des Art. 17 DSM-RL geprüft. Bei den der Definition Unterfallenden handelt es sich um Anbieterinnen, bei denen „der Hauptzweck bzw. einer der Hauptzwecke darin besteht, eine große Menge an von seinen Nutzern hochgeladenen, urheberrechtlich geschützten Werken oder sonstigen Schutzgegenständen zu speichern und der Öffentlichkeit Zugang hierzu zu verschaffen, wobei dieser Anbieter diese Inhalte organisiert und zum Zwecke der Gewinnerzielung bewirbt“.

ist die Haftung für die nicht-lizenzierten Inhalte grundsätzlich begründet. Allerdings kann die Plattformbetreiberin dieser begegnen, indem sie (kumulativ) nachweist, sich nach Möglichkeit um eine Lizenzierung bemüht zu haben (lit. a), die nach Maßgabe hoher branchenüblicher Standards zu bemessende Sorgfalt aufgebracht hat, um rechtsverletzende Inhalte zu sperren, nachdem die betroffenen Rechteinhaber den Betreiber der Plattform von ihren Werken informiert haben (lit. b), und nach Verschaffung der Kenntnis von Rechtsverletzungen durch die Rechteinhaber unverzüglich gehandelt hat, um den Zugang zu den geschützten Werken zu verhindern, sowie alle Anstrengungen unternommen hat, um das künftige Hochladen dieser Werke zu unterbinden (lit. c).

Die Erwägungsgründe der Richtlinie verdeutlichen indes, dass der europäische Gesetzgeber hiermit über den herkömmlichen Grundsatz des notice and take down hinausgeht und so die Anbieterinnen von Content-Sharing Diensten – in gewissem Umfang – dazu zu verpflichten wollte, unabhängig von der Erlangung der Kenntnis von einer Rechtsverletzung in gewissen Umfang präventive Maßnahmen zum Schutz der Rechteinhaber zu treffen.[190]

Ein kostengünstiger, aber im grundrechtlichen Sinne nicht ungefährlicher Weg sind sogenannte Upload-Filter. Allerdings stellt Art. 17 Abs. 8 UAbs. 1 DSM-RL klar, dass eine Pflicht zur allgemeinen Überwachung nicht eingeführt werde.

B.2.2.5.9 Zusammenfassung zu Haftung und Verantwortung

Summa Summarum kann festgehalten werden:

- Grundsätzlich trifft die Provider hinsichtlich fremder Inhalte keine generelle Überwachungs- und Nachforschungspflicht ex ante. Einer Haftung für fremde Rechtsverletzungen können sie in der Regel entgehen, wenn sie ab Kenntnis von einem Rechtsverstoß unverzüglich – ex post – alles ihnen Mögliche und Zumutbare unternehmen, um den Verstoß zu beseitigen (notice and take down); es sei denn, es handelte sich um eine für den Provider von vornherein offensichtliche Rechtsverletzung.
- Eine Intensivierung der Sorgfaltspflichten kann sich insbesondere dann ergeben, wenn ein Rechtsverstoß bereits bekannt ist und wiederholt zu werden droht (stay down). Dies kann ggf. geeignete technische Vorkehrungen und – je nach Art der Plattform und des Rechtsverstoßes – sogar manuelle Überprüfungen zur Verhinderung gleichartiger Rechtsverstöße erfordern.
- Für eigene, d. h. selbst eingestellte oder – z. B. durch einen Deep-Link – zu eigen gemachte fremde Inhalte ist keine besondere Haftungsbeschränkung möglich; die Inhalte und Links müssen sorgfältig ausgewählt bzw. gesetzt und unverzüglich entfernt werden, wenn sich eine Rechtsverletzung abzeichnet.
- Es ist darauf zu achten, dass sich die Anbieterin nur solche fremden Inhalte – ggf. auch durch eine gezielte Linksetzung – zu eigen macht, die inhaltlich geprüft sind.
- Usenet-Provider gelten (lediglich) als Cache-Provider im Sinne des § 9 TMG, können regelmäßig dessen Haftungsbeschränkungen für sich in Anspruch nehmen und jedenfalls dann exkulpieren, wenn eine Überprüfung technisch nicht möglich oder zumutbar ist.
- Eine Verschärfung der Haftungsregelungen (Provider-Privileg) durch die kommende E-Privacy-Verordnung und den Digital Services Act ist möglich. Eine Verschlechterung der Situation für die hier interessierenden Konstellationen ist dabei ebenfalls möglich aber eher unwahrscheinlich. Dies sollte aber beobachtet werden.
- Eine Haftung nach dem NetzDG kommt im Rahmen der vorliegend interessierenden Konstellation aufgrund seiner relativ hoch liegenden Anwendungsschwelle nur ausnahmsweise in Betracht.
- Auch die Umsetzung der DSM-Richtlinie[191] dürfte im vorliegend interessierenden Zusammenhang keine zusätzliche Verschärfung der Haftungssituation begründen. Die allgemeine zivilrechtliche Haftung für Urheberrechtsverletzungen bleibt aber unberührt.

B.2.3 SPEZIFISCHER ANWENDUNGSFALL: ONLINE-BERATUNG

B.2.3.1 Definition von Online-Beratung

Das Internet eröffnet als interaktive Kommunikationsplattform auch für die Beratung umfangreiche neue Möglichkeiten, die als Online-Beratung zusammengefasst werden können.

In der Beratung von Hilfesuchenden lässt sich zwischen der **Methode der Beratung** und ihrem Format unterscheiden. Sowohl im Hinblick auf die Methode als auch auf das Format können vielfältige Unterschiede bestehen. Für die Frage aber, ob es sich bei einem bestimmten Angebot um Online-Beratung handelt, ist weniger die Frage der Methode, sondern des Formates ausschlaggebend. Denn eine Methode (zB.

[190] Je nach Art der Inhalte können unterschiedliche Mittel angemessen und verhältnismäßig sein, um zu verhindern, dass nicht genehmigte urheberrechtlich geschützte Inhalte verfügbar sind, weshalb es nicht ausgeschlossen werden kann, dass die Verfügbarkeit nicht genehmigter Inhalte in manchen Fällen nur vermieden werden kann, wenn die Rechteinhaber den Anbieter benachrichtigt haben." (ErwG Nr. 66 II DSM-RL, ABl. L 130, 107).

[191] Die Umsetzung wird demnächst im Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) erfolgen.

Psychodrama oder Gestalttherapie) kann in unterschiedlichen Formaten (etwa im Rahmen einer persönlichen Begegnung im physischen oder eben im virtuellen Raum, in welchem die gegebene räumliche Distanz vermittels digitaler Kommunikationsmedien „online“ überbrückt wird) angewendet werden. Auf der Grundlage dieser Begriffszuordnung definiert die DGOB Online-Beratung

„als Setting, das sich in unterschiedliche Präsentationsformen differenziert, z.B. schriftgestützte Präsentationen (webbasierte Mailberatung, Chat- und Forenberatung) oder Präsentationen, die audiovisuelle Kanäle nutzen (z.B. Videoberatung etc.).“[192]

Damit vermittelt die Online-Beratung dem Ratsuchenden einen alternativen **Zugang** zu den Beratungsleistungen, der allerdings den Einsatz von **internetbasierten digitalen Telemedien** voraussetzt. Die Methode bleibt dadurch grundsätzlich unberührt. Damit ist also gleichzeitig klargestellt, dass es sich bei der Online-Beratung nicht etwa um eine neue Methode, sondern nur um einen neuen Modus handelt, in dem die üblichen Methoden angewendet werden können.

Praktische Einschränkungen (der Methode) können sich durch die technischen Besonderheiten der Vermittlung ergeben. Zum Beispiel ist Körperkontakt bei rein digitaler Vermittlung naturgemäß ausgeschlossen.

	Setting (Manifestation)	
	Offline	Online
Raum-zeitliche Distanz	Distanz zum Angebot in kmh	Distanz zum Angebot in Millisekunden
Physikalische Distanz	(physische) Anwesenheit	(physische) Abwesenheit
Zeitliche Distanz	Synchronizität	A-Synchronizität
Kommunikative Distanz	Unmittelbarkeit	Mittelbarkeit

Fig. B.8. Übersicht über die Unterschiede der Beratung offline/online; Quelle: DGOB

Die Tatsache, dass die Online-Beratung ohne physische Nähe auskommt, bedeutet natürlich nicht, dass die an sie zu stellenden Anforderungen geringer ausfallen. Im Gegenteil: Gerade durch die zu beachtenden technischen Besonderheiten liegen die Anforderungen in einigen Aspekten mitunter sogar höher. Das kann etwa die Fragen des Datenschutzes und der Datensicherheit betreffen, wovon noch zu sprechen sein wird. Sollen digitale Lösungen zur Anwendung kommen, ist festzustellen, ob die eingesetzte Technik und die dem Angebot zugrundeliegende Organisation eine vertrauliche Kommunikation gewährleisten. Online-Beratung sollte daher nur unter der Bedingung angeboten werden, dass die dazu notwendigen fachlichen und technischen Kenntnisse und Kompetenzen vorliegen. Einschlägige Fort- und Weiterbildungen können hierbei helfen. Sie setzt auch ihre Sicherung durch die Einhaltung der notwendigen technisch-organisatorischer Maßnahmen (TOM) voraus.[193]

In jedem Falle aber liegt die Entscheidung für das Format der Beratung in der Hoheit des Ratsuchenden. Mögliche Grenzüberschreitungen können durch die professionelle Bereitschaft zu kontinuierlicher Hinterfragung des eigenen Angebots und Auftretens weitgehend verhindert werden.

Die zu gewährleistende Vertraulichkeit der Kommunikation verlangt im Regelfall den Einsatz spezialisierter, auf den Einsatzbereich angepasster Software. Diese garantiert insbesondere

- die sichere Verschlüsselung und
- die Vermeidung von Kommunikation außerhalb abgesicherter webbasierter Systeme (so wäre beispielsweis der Einsatz von [unverschlüsselter] E-Mail **unzulässig** und berufsethisch **nicht** vertretbar (dazu näher B.2.3.4.1) sowie
- die Einhaltung der sonstigen Anforderungen der DS-GVO (bzw. des BDSG und des DSG-EKD);
- dass keine Sammlung und Weitergabe von Metadaten erfolgt, was idR. von kostenfreien sozialen Netzwerken für deren Nutzung vorausgesetzt wird; und
- dass nur Medien genutzt werden, die dem Fernmeldegeheimnis nach § 88 TKG unterfallen,[194] und bei deren Nutzung die strengen Vorgaben des TKG[195] beachtet werden.

Die Verantwortung für die Nutzung unsicherer und unzulässiger Verbindungswege kann – unabhängig ihres Verstoßes gegen das Berufsethos – nicht auf die Ratsuchenden rechtlich wirksam abgewälzt werden.

[192] Vorstandspapier 01/2018 der DGOB zur Definition von Online-Beratung, https://dg-onlineberatung.de/wp-content/uploads/2020/03/Definition-Online-Beratung-Website.pdf (zuletzt abgerufen am 22. Mai 2020). Allen gemein ist, dass die Beratung selbst immer internetbasierend erfolgt. Nichtvirtuelle Anbahnungs-, Zwischen- oder Abschlussphasen sind aber möglich. Inhaltlich lassen sich die Phänotypen der Beratung nach Zielgruppenausrichtung, Themenfeld (rechtlich, psychologisch, pädagogisch) und Beratungskonzepten (Fachberatung oder Prozessberatung) unterscheiden.

[193] Dazu sogleich näher unter C.1.1.1.5.1

[194] Der Begriff Telekommunikation wird in § 3 Nr. 22 TKG definiert. Telekommunikation ist danach der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“. Der Begriff der Telekommunikationsanlage ist wiederum in § 3 Nr. 23 definiert. Dabei handelt sich um „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“. Zugunsten einer möglichst weiten und umfassenden Definition wurde auf eine Auflistung bestimmter Kommunikationsarten verzichtet. Der Schutzbereich des Fernmeldegeheimnisses erstreckt sich somit nicht nur auf klassische Sprachtelefonie, sondern auch auf moderne Datenübertragungsformen, also insbesondere auch die digitale Nachrichtenübertragung zwischen Computern, da unter § 3 Nr. 23 auch Server oder Router zur Steuerung und Vermittlung von Online-Kommunikation und die Einwahlknoten von Internetprovidern fallen. § 88 schützt demnach jede Art der individuellen Nachrichtenübermittlung, zB. auch über Voice over IP (VoIP)-Dienste. Um eine individuelle Kommunikation handelt es sich aber natürlich nicht, wenn sich die Inhalte, wie etwa beim Rundfunk, dezidiert an die Öffentlichkeit richten.

[195] Siehe hierzu B.1.5.4

B.2.3.2 Exkurs: Digitalisierung und Fachlichkeit der Anwender*innen

Im Rahmen der Veränderung von Prozessen bringt es die Digitalisierung ebenfalls mit sich, dass auch neue Formen der Fachlichkeit entstehen müssen, und zwar umso mehr, je stärker die digitalisierte Fachanwendung Aufgaben im Bereich der Diagnostik, Planung, Dokumentation und Evaluation von Hilfen übernimmt. Hybride Arbeitsformen dringen weiter vor, womit die Professionalität der Dienstleistung Schritt zu halten hat, und zwar im Sinne fachlichen Handelns in und mit sozio-technischen Konstellationen.

Vor diesem Hintergrund kann Professionalität im Sinne der Fachlichkeit „über das Ausmaß an Reflexivität in Verbindung mit Dimensionen des a) Wissens und b) Könnens, c) beruflicher Haltungen sowie dem verfügbaren – oder verfügbar gemachten – Spielraum hinsichtlich d) der Berechtigungen des eigenen beruflichen Handelns“[196] definiert werden.

a) Wissen

In Sachen Wissen geht es um eine **breitere Data Literacy und technische Bildung**, die grundlegende Fragen des Datenschutzes und möglicherweise betroffener Persönlichkeitsrechte umfasst.

b) Können

Neben das kognitive Wissen tritt das praktische Können, das auf Erfahrung basiert. Nur wenige Bereiche der Digitalisierung – etwa in der Online-Beratung – verfügen über ansatzweise tradierte Erfahrungswerte, die wissens- und erfahrungsbasierte Elemente miteinander verbinden können. Diese den Mitarbeitenden zugänglich zu machen, kann etwa im Rahmen des **Peer Learning/ Coaching** erfolgen, die strukturierte Lern- und Erfahrungsräume ergänzen. Die effektive Weitergabe des Könnens hängt jedenfalls wesentlich von einer entsprechenden Organisationskultur ab.

c) Haltung

Je weiter die digitale Anwendung die Rechte ihrer Adressat*innen und Anwender*innen betrifft, desto wichtiger wird neben dem Wissen und Können auch eine entsprechende professionelle Haltung, die um die **Möglichkeiten wie auch die Risiken der Anwendung** weiß und damit **reflektierend** umgeht. Dies sowohl dergestalt, dass eine unberechtigte Sorglosigkeit bei der Anwendung wie auch ein teilhabeausschließendes Vorenthalten vermieden wird. Zielkonflikte, Widersprüche und Ambivalenzen werden nicht ausgeblendet, sondern verantwortungsvoll wahrgenommen und gehandhabt.

d) Berechtigungen

Sind die vorgenannten drei Punkte voll ausgebildet, ist die erfolgreiche Interaktion zwischen der digitalen Anwendung und ihren Anwender*innen noch nicht endgültig garantiert aber gut vorbereitet. Die erfolgreiche Anwendung setzt weiter voraus, dass die die konkrete Nutzung bestimmenden Rechte der Anwender*innen so definiert werden, dass sie das richtige Maß an **Gestaltungsspielraum** einräumt. Die fachlichen Konzepte der Profession müssen dafür hinreichend abgebildet sein. Andererseits können restriktive Vorgaben dazu führen, die Compliance der Arbeitsprozesse zu forcieren.

B.2.3.3 Nutzungsbedingungen und Datenschutzerklärung in der Online-Beratung

B.2.3.3.1 AGB/Nutzungsbedingungen

Es empfiehlt sich, im Rahmen der Online-Beratung die Verwendung von Nutzungsbedingungen. Dies gilt sowohl im Hinblick auf die Nutzer*innen (dazu Muster D.2.5) als auch im Hinblick auf die Mitarbeiter*innen (dazu Muster D.2.6). Die Muster können grundsätzlich auch für die Beratung per App eingesetzt werden.

B.2.3.3.2 Datenschutzerklärung

Auf die Arbeitshilfe zur Erstellung einer Datenschutzerklärung des Datenschutzbeauftragten der EKD wird hingewiesen.[197] Das Muster einer Datenschutzerklärung wird im Anhang D.2.2 mitgeliefert.[198]

B.2.3.4 Datenschutzrechtliche Spezifika

Auf die bereits zu (Beratungs-)Apps gemachten Hinweise, insbesondere zur Einwilligung (B.1.5.2) sowie zu den Vorschriften des TKG (B.1.5.4) wird hier ergänzend hingewiesen. Diese gelten im übertragenen Sinne auch im Zusammenhang mit entsprechenden Online-Beratungsangeboten.

[196] Polutta, Sozialpädagogische Fachlichkeit und Professionalität Sozialer Arbeit in der Migrationsgesellschaft, in: Blank, Gögercin, Sauer und Schramkowski (Hrsg.), Soziale Arbeit in der Migrationsgesellschaft, Wiesbaden 2018, S. 243 – 253, S. 245.

[197] https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-erstellung-einer-datenschutzerklaerung/ (zuletzt abgerufen am 28. August 2020).

[198] Als Orientierung bietende und anzupassende Vorlage kann ferner auch die Datenschutzerklärung der Caritas Online-Beratung (https://www.caritas.de/hilfeundberatung/onlineberatung/datenschutz) dienen.

Wo immer möglich, sollte die Beratung **anonym** erfolgen. So lässt sich der Aufwand im Hinblick auf den Datenschutz deutlich reduzieren. Die Einwilligung Beratungsinteressierter sowie die Aushändigung von Datenschutzinformation (siehe dazu oben unter B.2.3.3.2 und das Muster D.2.2) sind aber immer erforderlich. Zur Einwilligung Minderjähriger siehe oben B.1.5.2.2.

B.2.3.4.1 Verschlüsselte E-Mails

Eine Verschlüsselung von E-Mails, die über eine bloße Transportverschlüsselung hinausgeht (also eine Ende-zu-Ende-Verschlüsselung), verlangt den zuverlässigen Einsatz technischer Hilfsmittel **auf beiden Seiten**. Mailprogrammen ist die Fähigkeit der Verschlüsselung grundsätzlich nicht von vornherein eigen, sondern muss regelmäßig über Plugins **nachgerüstet** werden. Da die Anwendung solcher Plugins auch aufgrund des technischen Aufwands bislang **nicht weit verbreitet** ist, muss im Regelfall also davon ausgegangen werden, dass sie auf der Gegenseite nicht zum Einsatz kommen. Dadurch müssen die Berufsgeheimnisträger*innen auch davon ausgehen, dass anvertraute Geheimnisse nicht ausreichend geschützt sind und daher im Sinne des § 203 StGB strafbar offenbart werden können. Zudem sind alle technischen Lösungen grundsätzlich auch mögliche Schwachstellen, bedürfen also der Pflege, wie etwa des regelmäßigen Updates und der Überwachung ihrer Sicherheit. Aber auch E-Mails selbst, und ganz besonders unverschlüsselte, können Einfallstore für digitale Angriffe (zB. über Viren, Würmer und Trojaner) sein. Keylogger haben in der Vergangenheit nicht nur zu datenschutzrechtlichen Problemen, sondern auch zu Erpressungen geführt.

Im besten Fall sollte bei Eingang einer unverschlüsselten E-Mail mit einer Antwort wie der folgenden reagiert werden:

„Vielen Dank für Ihre Nachricht! Wir möchten Sie darüber informieren, dass wir in unserer Funktion als Berufsgeheimnisträger*innen zum Schutz der Sie betreffenden Informationen verpflichtet sind. Da eine ausreichend vertrauliche Kommunikation über E-Mail nicht sichergestellt werden kann, bitten wir Sie, unsere Antwort über folgenden Link einzusehen, wodurch ein geschützter Kommunikationskanal zwischen uns eröffnet wird. Bitte klicken Sie dafür hier[199].“

Der vorbezeichnete Link kann etwa auf die verschlüsselte Kommunikation über eine Website (https) führen. Der verschlüsselte Zugriff auf dort hinterlegte Daten kann entweder über einen ssl-verschlüsselten Webserver erfolgen, auf dem die Daten eingesehen werden können. Oder es wird eine verschlüsselte E-Mail-Verbindung zwischen dem Server und der Berufsgeheimnisträgerin eingerichtet.[200]

Zusammenfassend ist festzuhalten, dass eine E-Mail nur unter besonderen Bedingungen ein geeignetes Medium der Beratung darstellen kann und damit **im Regelfall nicht ohne Weiteres zum Austausch vertraulicher Informationen genutzt werden sollte**. Dadurch sind zwar Nachteile im Sinne der Spontanität der Kontaktaufnahme verbunden. Deren Inkaufnahme lohnt in Anbetracht der schweren Sicherheitsbedenken allerdings regelmäßig nicht.

Wenn die E-Mail als Medium fest installiert werden soll, sind ausschließlich solche Formate zu wählen, die

1) die Vertraulichkeit durch Verschlüsselung, also eine verschlüsselte Ende-zu-Ende-Kommunikation gestatten,

2) die Vertraulichkeit durch Datenintegrität sicherstellen, dass also eine Manipulation der übermittelten Informationen erkannt werden kann, etwa durch den Einsatz qualifizierter elektronischer Signaturen[201].

B.2.3.4.2 Exkurs: WhatsApp

WhatsApp ist ein sogenannter Instant-Messenger-Dienst, der es erlaubt, zwischen registrierten Nutzern Text- und Sprachnachrichten sowie Fotos, Videos, Audiodateien und Kontaktdaten auszutauschen und via IP-Telefonie über das Internet zu telefonieren. Der Dienst wurde 2009 gegründet; der Sitz des Unternehmens ist in Santa Barbara, Kalifornien, in den USA. Im Oktober 2014 wurde WhatsApp von dem Sozialen Netzwerk Facebook übernommen, mit dem es seine Daten teilt. Ca. 70% aller deutschen Bürgerinnen und Bürger nutzen WhatsApp. Der Facebook Dienst ist derzeit damit der meistgenutzte Messengerdienst in Deutschland.

Neben der Frage des Datenaustauschs war eine WhatsApp-Nutzung insbesondere hinsichtlich dreier Aspekte problematisch:

- Vertraulichkeit der Kommunikation,
- WhatsApp fungiert als Anbieter außerhalb des Geltungsbereichs europäischer Datenschutzvorschriften,
- regelmäßige Übertragung von Kontaktdaten aus dem Adressbuch des Smartphones, auf dem WhatsApp installiert ist.

Die Verschlüsselung der Kommunikation scheint dem Stand der Technik zu entsprechen. WhatsApp hat aber jedenfalls Zugriff auf die Metadaten der Kommunikation (Absender, Empfänger, Zeitpunkt, Größe etc.), was bereits ein berufsethisches Problem auslöst. Ein schweres Problem besteht ferner in der Übermittlung von Daten in die USA. Zwar war nach dem Angemes-

[199] Der Link zum geschützten Angebot ist zu hinterlegen.

[200] Die Einrichtung eines ssl-verschlüsselten Servers sollte einem nach ISO/IEC 27001 zertifizierten Unternehmen überlassen werden. Die Anwendung zertifizierter Branchensoftware kann sich ebenfalls empfehlen.

[201] Der Begriff der elektronischen Signatur geht auf die Richtlinie 1999/93/EG v. 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 v. 19.1.2000, zurück. 2014 hat die Europäische Kommission mit Wirkung zum Juni 2016 die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung bzw. IVT) verabschiedet. Bei Stärkung und Erweiterung der bisherigen Rechtsvorschriften ersetzt diese Verordnung die Signaturrichtlinie.

senheitsbeschluss der Europäischen Kommission bei einer Datenverarbeitung durch Unternehmen, die sich dem EU-US-Datenschutzabkommen (Privacy Shield)[202] unterworfen haben, zunächst ein ausreichendes Datenschutzniveau anzunehmen. Dabei handelte es sich aber nur um eine formale Angemessenheit, da das Privacy Shield mit erheblichen Mängeln behaftet war. Wie das Vorgänger-Abkommen Safe-Harbor wurde auch beim Privacy Shield den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang eingeräumt, womit durch die Zugriffsmöglichkeiten der US-Behörden – insbesondere auch der US-Geheimdienste – die Anforderungen an den Datenschutz nicht gewährleistet sind. Dementsprechend hat der EuGH den Privacy Shield für unzureichend befunden.[203] WhatsApp dürfte zudem auch nicht bereit sein, Standardvertragsklauseln zu unterzeichnen, da sie – zumindest bislang – auch nicht dazu bereit waren, hinreichende Auftragsverarbeitungsverträge abzuschließen (Art. 28 Abs. 3 bzw. 7 DS-GVO, § 30 DSG-EKD – siehe dazu C.1.1.1.5.1.3). Aus all diesen Gründen **sollte WhatsApp nicht als Kommunikationsmittel gewählt** werden.

Dennoch ist WhatsApp als Messenger-Dienst nach Auffassung einiger Experten (uA. des Landesdatenschutzbeauftragten in Rheinland-Pfalz) nicht in jedem Fall a priori datenschutzwidrig. Probleme resultierten weniger aus der Gestaltung des Dienstes, sondern aus dessen Einsatzbedingungen in der Praxis.

Wird also trotz all der vorgenannten Mängel dennoch eine Kommunikation über WhatsApp gewählt, sollte immerhin auf Folgendes geachtet werden:

- Einsatz aktueller Software-Versionen, um eine technisch einwandfreie Verschlüsselung der Kommunikationsinhalte zu gewährleisten;
- Einsatz dienstlicher/geschäftlicher Mobiltelefone; nur ausnahmsweise und verbunden mit tragfähigen Container-Lösungen kommt die Nutzung privater Endgeräte in Betracht;
- Nutzung eines „one-record-Adressbuchs“ mit ausschließlich der Telefonnummer des Dienstanbieters oder einer Sperre des Adressbuchzugriffs durch WhatsApp;
- Deaktivierung von Cloud-Backups;
- Sicherstellung, dass Chat-Anhänge nicht in der Mediathek des Mobiltelefons gespeichert werden bzw. Dritt-Applikationen keinen Zugriff darauf haben;
- ausreichende Absicherung der Endgeräte (Zugriffssperre, Verschlüsselung).

Die Kommunikation über WhatsApp sollte sich auf das Wesentlichste beschränken und umgehend auf einen datenschutzkonformeren Kanal umgestellt werden. Darüber hinaus sollte, wo es tatsächlich genutzt wird, die **Verantwortlichkeit dafür klar geregelt** werden. Die Geschäftsführung steht insoweit in der Pflicht, die mit der Anwendung beauftragten Mitarbeitenden zu entlasten.

B.2.3.5 Strafrechtliche Aspekte in der Online-Beratung

B.2.3.5.1 § 203 StGB

B.2.3.5.1.1 Allgemeines, insb. Verschwiegenheitspflichten

Ratsuchende müssen sich in jedem Falle darauf verlassen können, dass mit den von Ihnen gemachten Angaben zuverlässig professionell umgegangen wird. Das besonders schützenswerte Verhältnis zwischen den Berufsgeheimnisträgern und ihren Klient*innen darf durch die Digitalisierung gerade nicht gefährdet werden. Daher hat sich jede digitale Entwicklung auch diesem Thema zu stellen und es als maßgebend einzubeziehen.

Neben den allgemeinen Bestimmungen zum Datenschutz[204] tritt bei Berufsgeheimnisträgern zusätzlich eine nach § 203 StGB **strafbewehrte Verschwiegenheitsverpflichtung** hinzu, die sie einseitig verpflichtet. § 203 StGB normiert die Verschwiegenheitspflicht nicht selbst, sondern setzt ihr Bestehen voraus. Dieses wird regelmäßig durch die jeweils einschlägige Berufsordnung begründet.

War noch unter Geltung des Bundesdatenschutzgesetzes der alten Fassung (in § 1 Abs. 3 BDSG aF.) ein Vorrang der berufsrechtlichen Verschwiegenheitspflichten vor dem Datenschutzrecht gegeben – die Datenschutzgesetze waren also auf die Verarbeitung personenbezogener Daten durch gesetzlichen Schweigepflichten unterliegende Berufe nicht anwendbar –, sieht die DS-GVO keine Bereichsausnahme für die Datenverarbeitung durch Berufsgeheimnisträger mehr vor. Die Regeln laufen parallel nebeneinander. Daher ist eine mögliche Entbindung von der Schweigepflicht strikt von der datenschutzrechtlichen Einwilligung nach Datenschutzrecht zu trennen (unterschiedliche Rechtsbereiche). Letztere ist daher – zusätzlich zur Entbindung – für eine beabsichtigte Offenlegung von personenbezogenen Daten einzuholen, die dem Berufsgeheimnis unterliegen.

Im Gegensatz zu den Bestimmungen des Datenschutzrechts, die als schwerste Waffe – besonders hohe – Bußgelder vorsehen, ist ein Verstoß gegen die Verschwiegenheitspflicht sogar strafbewehrt. Allerdings handelt es sich bei § 203 StGB um ein sogenanntes Sonderdelikt, dh. die Strafdrohung gilt nur gegenüber solchen Personen, die im Sinne des § 203 StGB zur Begehung einer Verschwiegenheitspflichtverletzung qua

[202] https://www.privacyshield.gov/welcome (zuletzt abgerufen am 10. Juni 2020).
[203] Urteil vom 16. Juli 2020 - C-311/18. Den Einsatz von Standardvertragsklauseln hat er EuGH aber nicht beanstandet.
[204] Siehe hierzu B.1.4, B.2.2.3, B.2.2.4.3 und C.1.1.

ihres Berufsstandes qualifiziert sind. Insoweit handelt es sich um ein besonderes persönliches Merkmal. Die Norm listet eine Reihe von Berufsträgern auf, darunter Ärzte und Angehörige anderer Heilberufe, Ehe, Familien-, Erziehungs- und Jugendberater, Berater für Suchtfragen in einer Beratungsstelle, staatlich anerkannte Sozialarbeiter und Sozialpädagogen.

Die Auflistung verdeutlicht, dass die Vorgaben des § 203 StGB neben dem medizinischen Bereich auch in vielen Bereichen der sozialen Arbeit unmittelbare Anwendung finden. Zwar ist der Katalog dem Grunde nach abschließend. Das verfassungsrechtliche Bestimmtheitsgebot (Art. 103 Abs. 2 GG) bringt dies mit sich. Die Auslegung der Norm innerhalb der Wortlautgrenze bezieht mitunter aber auch Tätigkeitsfelder mit ein, die nicht unmittelbar erkennbar sind, so etwa im Bereich der Altenpflege. Dies wird aber durch die einschlägigen Berufsordnungen auch widergespiegelt.

Durch die Digitalisierung von Leistungen ergeben sich hieraus aber keine sachlichen Veränderungen. Wer der Verschwiegenheitspflicht unterliegt, sollte dies wissen, auch ohne Leistungen digital zu erbringen.[205]

B.2.3.5.1.2 Ausnahmen, insbesondere § 138 StGB, Suizid

Neben den verschiedenen Pflichten zur Verschwiegenheit gibt es aber auch Fälle, in denen das Schweigen gebrochen werden muss oder jedenfalls gebrochen werden darf. Das kann in der Praxis vor allem dann der Fall sein, wenn Mitarbeitende der Beratungsstelle von einer anrufenden Person einen Hinweis auf eine konkrete geplante Straftat des Katalogs des § 138 StGB erhält. Dazu gehören

- Hoch- und Landesverrat oder Gefährdung der äußeren Sicherheit (§§ 81-83, Abs.1, 94-96, 97a oder 100)
- Geld- oder Wertpapierfälschung (einschl. Euroscheck und Scheckkarten) (§§ 146, 151, 152, 152b)
- Menschenhandel, Zwangsprostitution (§§ 232, 232a)
- Mord, Totschlag oder Völkermord (§§ 211, 212, 220a)
- Menschenraub (§ 234), Verschleppung (§ 234a), erpresserischer Menschenraub (§ 239a), Geiselnahme (§ 239b)
- Raub, schwerer Raub und Raub mit Todesfolge (§§ 249-251), räuberische Erpressung (§ 255)
- gemeingefährliche Straftaten, wie
  - Brandstiftung (§§ 306-306f)
  - Herbeiführen einer Explosion durch Kernenergie (§ 307)
  - Herbeiführen einer Sprengstoffexplosion (§ 308)
  - Missbrauch ionisierender Strahlen (§ 309)
  - Vorbereitung eines Explosions- oder Strahlungsverbrechens (§ 310)
  - Herbeiführen einer lebensgefährdenden Überschwemmung (§ 313)
  - Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr (§ 315, Abs. 3)
  - Gefährliche Eingriffe in den Straßenverkehr (§ 315b, Abs. 3)
  - Räuberischer Angriff auf Kraftfahrer (§ 316a)
  - Angriff auf den Luft- und Seeverkehr (§ 316c)
  - gemeingefährliche Vergiftung (§ 314)

Die Anzeigepflicht besteht nur, wenn Mitarbeitende **glaubhaft** von der geplanten Straftat erfahren. **Konkretisiert** ist die Tat, wenn die anrufende Person die Personen oder Objekte, an denen sie selbst oder Dritte die Straftat begehen will bzw. begangen haben will, mitgeteilt hat. Die Tat bzw. der Eintritt ihres Erfolges muss in zeitlicher Hinsicht **noch abwendbar** sein.

Allem voran gilt aber: Die Beratungsstelle ist nicht die Polizei! Sie hat kein Mandat zur Verhinderung oder Verfolgung von Straftaten. Die Geheimhaltung ist ein hohes Gut, die Durchbrechung darf deshalb nur in wirklichen Ausnahmefällen erfolgen. Mitarbeitende der Beratungsstelle müssen sich wohl oder übel an den Gedanken gewöhnen, dass sie möglicherweise mehr Übel hätten verhindern können, es aber aus Interesse an der Geheimhaltung der mitgeteilten Gesprächsinhalte nicht getan haben.

Hinsichtlich **bereits begangener** Straftaten existiert eine Anzeigepflicht nur, sofern eine **Wiederholungsgefahr** in Bezug auf die in § 138 StGB genannten Straftaten besteht.

Teilt eine Person der Beratungsstelle ihren Entschluss mit, einen **Suizid** begehen zu wollen, muss die betreffende Mitarbeitende zunächst klären, ob sie die Mitteilung für **glaubwürdig** hält. Im Zweifel sollte allerdings von der Ernsthaftigkeit dieser Mitteilung ausgegangen werden. Da Berater*innen wie jedermann zur Hilfeleistung nach § 323c StGB verpflichtet sind, ist auch hier die Pflicht zur Hilfeleistung gegeben. „Erforderliche Hilfe“ (nach § 323c StGB) kann sowohl das seelsorgerlich-beratende Gespräch als auch die Verständigung von Rettungsdiensten oder der Polizei sein.

Die bloße Ankündigung eines Suizids ist indes noch kein Unglücksfall iSd. § 323c StGB. Ein solcher ist erst dann anzunehmen, wenn die betreffende Person bereits einen Geschehensablauf in Gang gesetzt hat, die im ununterbrochenen Fortgang zum Tod oder zu einer schwerwiegenden Verletzung führen kann (beispielsweise nach Tabletteneinnahme oder Besteigen eines Hochhausdachs).

[205] Schwangerschaftskonfliktberater*innen, Berater*innen für Fragen der Betäubungsmittelabhängigkeit in einer anerkannten Beratungsstelle haben entsprechend ihrer strafrechtlichen Verschwiegenheitsverpflichtung ein Zeugnisverweigerungsrecht über alles, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist (§ 53 Abs. 1 Nr. [3a, 3b] StPO, § 383 Abs. 1 Nr. 6 ZPO). Als Berufsgeheimnisträger*innen werden diese Berater*innen auf dieses Recht nicht gesondert hingewiesen; sie müssen es also selbst kennen und beachten. Wird dennoch auf Fragen des Gerichts oder der Polizei geantwortet, kann dies strafbar sein. Andere Berater*innen sind zwar nach § 203 StGB ebenfalls grundsätzlich zur Verschwiegenheit verpflichtet – doch es gibt Ausnahmen. Als Zeuge im Zivil- oder Verwaltungsprozess besteht ein Zeugnisverweigerungsrecht über alles, für das die Verschwiegenheitspflicht gilt (§ 383 Abs. 1 Nr. 6 ZPO). Anders im Strafprozess: Nach § 53 StPO haben nur Betäubungsmittel- und Schwangerschaftsberater ein automatisches Zeugnisverweigerungsrecht. Für alle nicht dort genannten Berufsgruppen besteht nur ausnahmsweise ein Zeugnisverweigerungsrecht. Allerdings kann in besonderen Einzelfällen aus verfassungsrechtlichen Gründen dennoch ein Aussageverweigerungsrecht bestehen, etwa wenn es um intime Informationen von Klient*innen geht und nur leichte Kriminalität in Rede steht. Dann darf die Aussage verweigert werden. In solchen Fällen sollte aber zuvor rechtsanwaltliche Beratung eingeholt werden. In kritischen Fällen kann zudem die Beiordnung eines Zeugenbeistands nach § 68 Abs. 2 StPO, möglichst rechtzeitig vor der Vernehmung, beantragt werden. Vor den Zivil-, Verwaltungs-, Sozial- und Finanzgerichten bestehen sogar noch ausgedehntere Zeugnisverweigerungsrechte.

Lässt sich der Suizident von seinem Entschluss nicht abbringen, muss die Mitarbeiterin der Beratungsstelle eine Abwägung treffen, ob sie die Polizei verständigt. Lässt sich aus der Kommunikation erkennen, dass die Klientin fremder Hilfe gegenüber offen ist, diese vielleicht sogar sucht („Hilferuf“), deutet dies auf eine Einwilligung in die Weitergabe des Geheimnisses hin. In diesem Fall entfällt die Schweigepflicht. Aber auch der Bruch der Schweigepflicht ist in einschlägigen Fällen durch den Rechtfertigenden Notstand gerechtfertigt. Vor der Verständigung von Rettungsdiensten und/oder Polizei, ist allerdings auch abzuwägen, ob nicht genau dies zu einer Verschärfung der Situation der Klientin führen könnte. Der Kontakt könnte abbrechen und die Person direkt zum Suizid schreiten. Ist die Verständigung der Polizei geboten, sollte die Mitarbeitende versuchen, von der Klienten Namen und Aufenthaltsort zu erfahren.

In Fällen eines geplanten erweiterten Suizids oder der Schädigung bzw. Gefährdung Dritter ist die Polizei einzuschalten.

B.2.3.5.1.3 Einbindung anderer Mitarbeitenden und von Gehilfen

In der Beratungsarbeit ist es in gewissem Umfang erforderlich und auch zulässig, Gesprächsinhalte mit anderen Mitarbeitenden oder den Supervisor*innen zu besprechen. Nimmt die empfangende Person „noch unmittelbar an dem konkreten Vertrauensverhältnis teil“, liegt eine unbefugte Offenbarung eines Geheimnisses nicht vor. In diesem Fall kann von einer schlüssig erklärten Einwilligung ausgegangen werden. Dies dürfte regelmäßig der Fall sein, wenn sich die Klientin nicht ausdrücklich an eine bestimmte Person, sondern eine Institution (die Beratungsstelle) gewandt hat und das Geheimnis in dem Ausmaß, wie es für die Bearbeitung des Vorganges notwendig ist, innerhalb der Institution weitergegeben wird. Dies schließt auch die Weitergabe an Supervisor*innen ein, da die Betreuung der Mitarbeitenden durch Supervisor*innen Bestandteil der Beratungsarbeit ist; dies zumindest, wenn dies auch öffentlich angezeigt ist bzw. als bekannt gelten kann.

Die Weitergabe ist allerdings auf das unbedingt notwendige Maß zu beschränken, zB. sind die Angaben zu anonymisieren. Weitergegeben werden darf das Geheimnis auch nur an Mit-arbeitende und Supervisor*innen, die ebenfalls zur Verschwiegenheit verpflichtet wurden.

Erklärt allerdings die Klientin ausdrücklich, auch mit einer internen Weitergabe des Geheimnisses im Rahmen der ordnungsgemäßen Bearbeitung nicht einverstanden zu sein, und lässt sie sich von der Notwendigkeit der (begrenzten) Weitergabe nicht überzeugen, muss die Weitergabe tatsächlich unterbleiben oder ggf. das Gespräch abgebrochen werden. Auf jeden Fall dürfen dem Anrufer gegenüber keine Zusagen über den Fortgang des Verfahrens gemacht werden, die nachher nicht eingehalten werden.

Gehilfen oder bei den Schweigepflichtigen zur Vorbereitung auf den Beruf tätigen Personen dürfen die Schweigepflichtigen die Geheimnisse gegenüber offenbaren, da anderenfalls ein ordnungsgemäßer Betriebsablauf bzw. eine ordnungsgemäße Ausbildung nicht möglich wäre. Diese Begrenzung der Schweigepflicht kann aber nur dann gerechtfertigt werden, wenn diese zusätzlichen Personen ebenfalls der Schweigepflicht unterworfen werden. Dafür sorgt § 203 Abs. 4 S. 1 1. Var. StGB.[206]

Hierüber und über den Umfang der (auch datenschutzrechtlichen) Schweigepflicht – sollten die Berufsgeheimnisträger*innen die Hilfspersonen – nicht zuletzt auch zu Zwecken der Dokumentation – in gegenzuzeichnender Weise umfassend schriftlich aufklären und die Hilfspersonen über das Dienstverhältnis hinaus zum Schweigen verpflichten.

Ob Gehilfen haupt- oder ehrenamtlich tätig sind, ist unerheblich. Wesentlich ist lediglich, dass die Person, der sie zugeordnet sind, in ihrer jeweiligen zur Verschwiegenheit verpflichteten Funktion ein Geheimnis erfährt. Zudem muss die unterstützende Tätigkeit in einem inneren Zusammenhang mit der besonderen zur Verschwiegenheit verpflichtenden Tätigkeit stehen und mit der Kenntnisnahme von Geheimnissen verbunden sein. Im Rahmen der Online-Beratung dürfte dies wohl nur ausnahmsweise vorkommen.

B.2.3.5.1.4 Einbindung Dritter (Dienstleister)

Gerade im Bereich der Digitalisierung ergeben sich Folgeprobleme. So etwa wenn es um die Einbindung externer Dienstleister geht, die Teile der Datenverarbeitungen wie beispielsweise die Speicherung von Daten übernehmen oder im Rahmen der Systempflege mit geschützten personenbezogenen Daten in Kontakt kommen.

Seit dem Inkrafttreten des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen im Jahre 2017 ist die Problemlage aber wesentlich entschärft worden. Seither unterliegt das Offenbaren von geschützten Geheimnissen nicht mehr der Strafbarkeit, wenn

- die Offenbarung für eine ordnungsgemäße Durchführung der Leistungen des Dritten erforderlich ist,
- der Dritte der Anwendung der DS-GVO unterworfen ist (und bestenfalls eine Zertifizierung nach der ISO/IEC 27000-er-Reihe nachweisen kann sowie seine Technik innerhalb der EU betreibt),
- die Zusammenarbeit mit dem Dritten vertraglich geregelt ist (Datenverarbeitung im Auftrag, Auftragsverarbeitungs-Vertrag (AVV – siehe dazu C.1.1.1.5.1.3), Art. 28 Abs. 3 DS-GVO, § 30 DSG-EKD), wobei der Dritte geeignet auf die Einhaltung der Auflagen und deren Umsetzung in technisch-organisatorische Maßnahmen (TOM) sowie

[206] Zusätzlich sollten die Schweigeverpflichteten – zur Absicherung ihren eigenen Schweigeverpflichtung sowie zu Dokumentationszwecken – gegenüber den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen sowie Gehilfen eine schriftliche und gegenzuzeichnende Belehrung über die Verschwiegenheitsverpflichtungen vornehmen (D.2.3 und D.2.4).

- auf die Verschwiegenheitspflicht umfassend hingewiesen und explizit verpflichtet werden muss (ein Muster dessen findet sich im Anhang unter D.2.3 und D.2.4), und
- die Ratsuchenden im Rahmen ihrer Einwilligung gemäß des Transparenzgebots der DS-GVO aufgeklärt werden, für welche Zwecke und in welcher Weise die persönlichen Daten verarbeitet, ggf. weitergegeben und gespeichert werden und wann eine Löschung der Daten erfolgt und wie die Einwilligung widerrufen werden kann.

Gleichwohl gilt allgemein, dass der Einsatz technischer Maßnahmen rechtlich und berufsethisch nur gerechtfertigt werden kann, wenn diese der gesetzlich geforderten, zumutbaren Datensicherheit entsprechen (Art. 25 DS-GVO, §§ 64 und 35 BDSG, §§ 27, 28 DSG-EKD).[207] Neben den gesetzlichen Verpflichtungen verpflichtet bereits das Eigeninteresse hierzu, nach dem das Vertrauen der Öffentlichkeit in die Beratungsangebote der Freien Wohlfahrt besonders zu schützen und zu pflegen ist.

B.2.3.5.1.5 Einverständnis/Einwilligung

Es ist möglich – wenn auch nur in gut begründeten Ausnahmefällen zu empfehlen – mit einem ausdrücklichen, informierten und dokumentierten Einverständnis (Opt-in) der/des Berechtigten die Befugnis zur und damit die Straflosigkeit der Offenbarung des Privatgeheimnisses herzustellen. Mitunter wird das genutzt, wenn sich die Berechtigten über einen ungeschützten Kanal (beispielsweise E-Mail oder ein Messenger wie WhatsApp) bei der Beratungseinrichtung melden und um Beratung bitten. Auch wenn damit die strafrechtliche Verantwortlichkeit ausgeräumt werden kann, bliebe dies aus berufsethischen Gründen fragwürdig.

Zudem wirft dies datenschutzrechtliche Probleme auf. Daher sollte die Verwendung ungeschützter Kanäle, soweit sie überhaupt erfolgt, auf das absolut notwendige Minimum beschränkt und, sobald wie möglich, wieder auf einen verschlüsselten Kommunikationsweg gewechselt werden (siehe B.2.3.4.1).

B.2.3.5.2 § 202a StGB

Seit Inkrafttreten der letzten Änderung in 2007 stellt § 202a StGB eine der wichtigsten **praxisrelevanten Normen des sogenannten IT- und Datenstrafrechts** dar. Als klassisches Lehrbuchbeispiel kann der „Hackerangriff“ gelten, bei dem extern auf die IT-Systeme zugegriffen wird. Allerdings erschöpft sich die Bedeutung der Vorschrift darin nicht und wird **häufig durch Unternehmensleitungen unterschätzt**. Ist den Mitarbeitenden beispielsweise die **private Nutzung von Betriebs-IT (etwa Laptops) gestattet**, kann **jeder unbefugte Zugriff** des Arbeitgebers ein Ermittlungsverfahren zur Folge haben, wenn die Mitarbeiter selbst einen Zugriffsschutz eingerichtet haben. Das Sich-Verschaffen des Zugangs zu den dergestalt geschützten Systemen kann auch ohne die Absicht, von Daten tatsächlich Kenntnis zu nehmen, strafbar sein.

Ist die private Nutzung eines zur Betriebs-IT gehörenden Gerätes also gestattet, sollte der Zugriff durch den Arbeitgeber grundsätzlich nicht ohne Abstimmung erfolgen.

B.2.3.5.2.1 EXKURS: BYOD (Bring Your Own Device)

In vielen Branchen ist das BYOD-Modell ein wichtiger Trend. Mit dem Begriff ist gemeint, dass Mitarbeitende ihre eigenen IT-Geräte (wie etwa Laptops oder Smartphones) benutzen, um betriebliche Daten zu verarbeiten. Dieses Modell hat Vor- und Nachteile für beide Seiten, sowohl die Arbeitnehmer- als auch die Arbeitgeberseite. Für die Arbeitgeberseite ist freilich die Frage Kostenreduktion besonders interessant. Allerdings muss diese Frage sorgfältig in jedem Einzelfall aufgrund einer individuellen Analyse beantwortet werden.

Aus juristischer Sicht ist insbesondere wichtig zu betonen, dass der Arbeitgeber auch dann verantwortliche Stelle im Sinne des Datenschutzes bleibt, wenn die Mitarbeitenden private Geräte beruflich für die Verarbeitung betrieblicher Daten einsetzen. In der Folge müssen die ergriffenen Maßnahmen zur Datensicherheit ebenso anspruchsvoll konzipiert sein als würden die Daten mit betrieblicher IT verarbeitet. Es lässt sich leicht erkennen, dass dies gleichermaßen leistungsfähige Vereinbarungen mit den Mitarbeitenden voraussetzt[208] wie auch eine durchdachte Implementation von technischen Sicherungen auf aktuellem Stand. Vor dem Hintergrund dessen sollte immer gut geprüft sein, ob die Zurverfügungstellung von betriebseigener IT nicht doch der im Ergebnis sicherere, einfachere und auch kostengünstigere Weg ist, da er allein die volle technische und rechtliche Kontrolle über Geräte und Daten ermöglicht. Das hängt namentlich von der Arbeitsweise des jeweiligen Unternehmens wie auch seiner technischen Infrastruktur ab.

Sollte aber die Nutzung privater Geräte angestrebt werden, dürfte eine MAM-Lösung in vielen Fällen die beste Lösung sein. MAM steht für Mobile Application Management, das die Isolierung der betrieblichen Anwendungen von privaten erlaubt. So kann etwa ein virtueller Desktop erzeugt werden, der die betrieblichen Anwendungen in eine eigene, cloudbasierte Systemumgebung einkleidet und von den weiteren Anwendungen im privaten Betriebssystem trennt (Sandboxing).

Falls die Entscheidung zugunsten des BYOD ausfällt,[209] bedarf deren Einführung einer einzelvertraglichen

[207] Siehe dazu näher unter B.2.3.4.

[208] So z.B. die Klärung folgender Frage: Was geschieht etwa mit privaten Daten auf den Geräten der Mitarbeitenden, die auf der Unternehmens-IT gesichert werden? Können die Mitarbeitenden auf ihren Geräten vorhandene Unternehmensdaten in private Backups ihrer Geräte einbeziehen? Was geschieht mit privaten E-Mails, die von privaten Geräten über Systeme des Unternehmens laufen?

oder kollektivrechtlichen Grundlage. Bei Fehlen dieser besteht nicht nur das unkontrollierbare Risiko der Vermengung betrieblicher und privater Daten. Auch kann der Arbeitgeber seiner datenschutzrechtlichen Pflicht zur Umsetzung geeigneter technisch organisatorischer Maßnahmen mitunter nicht nachkommen. Denn ihm obliegt es nicht nur, solche zu ergreifen, sondern auch, sie auf Ihre Effektivität zu überprüfen.

a) Individualabrede

Eine individuelle Vereinbarung mit den Mitarbeitenden bietet die Möglichkeit zu sehr spezifischen und präzisen Regelungen. Es empfiehlt sich dabei, Art und Umfang der Nutzung der betreffenden Software und deren lizenzrechtliche Grundlagen so konkret wie möglich zu regeln. Eine Regelung zur klaren Trennung von betrieblichen und privaten Daten ist ebenfalls essentiell, da ohne diese Trennung die Einhaltung der datenschutzrechtlichen Pflichten schlechterdings nicht möglich sein wird.

Kann eine Virtualisierung der betrieblichen Anwendungen (ggf. über VPN) und eine organisatorische Trennung der betrieblichen von privaten Daten nicht erfolgen, zB. weil im Rahmen der Nutzung sozialer Netzwerke eine solche Trennung nicht vorgesehen ist, ist es notwendig, dem Arbeitgeber und dem betrieblichen Datenschutzbeauftragten vertraglich das Recht einzuräumen, zum Zwecke der datenschutzrechtlichen Kontrolle auch von privaten Daten Kenntnis zu erlangen. Eine Verschwiegenheitsabrede sollte klarstellend begleitend getroffen werden. Schließlich sollte in der Vereinbarung auch geregelt werden, wie nicht mehr benötigte betriebliche Daten gelöscht werden. Insbesondere ist dabei die Herausgabe bzw. Löschung von Daten im Falle der Beendigung des Arbeitsverhältnisses zu regeln.

b) Kollektivrechtliche Regelung

Die Mitbestimmungsrechte des Betriebsrates nach § 87 Abs. 1 BetrVG bzw. § 40 MVG-EKD sind im Falle der Nutzung privater Geräte und Software zu betrieblichen Zwecken berührt. Einen besonderen Problempunkt stellt dabei vor allem die datenschutzrechtlich gebotene Kontrolle der Einhaltung des Datenschutzes dar. Sie birgt nämlich die Möglichkeit der Verhaltens- und Leistungskontrolle i. S. d. § 87 Abs. 1 Nr. 6 BetrVG/§ 40 lit. j MVG-EKD.

Auch kann die betriebliche Nutzung privater Geräte auf die individuelle Verfügbarkeit der Mitarbeitenden ein- und sich auf Arbeitszeit und betriebliche Ordnung auswirken. Die **Mitbestimmung des Betriebsrates** dürfte daher auch auf § 87 Abs. 1 Nr. 1 oder 2 BetrVG/§ 40 lit. d oder k MVG-EKD zu stützen sein.

Eine Betriebsvereinbarung ist in ihren Wirkungen allerdings per se begrenzt. Sie kann nur in abstrakt-genereller Weise innerhalb des Betriebes eine einheitliche Regelung für die betriebliche Nutzung privater Geräte begründen. Sie reicht aber keinesfalls in die private Sphäre der Mitarbeitenden und kann so etwa niemanden verpflichten, privat angeschaffte Geräte tatsächlich betrieblich zu nutzen.

B.2.3.5.3 § 201 StGB

Auch an § 201 StGB ist zu denken, an das Verbot des Abhörens und Aufzeichnens von Gesprächen. Zwar ist das bloße Mithören grundsätzlich nicht erfasst, insbesondere nicht, wenn – es beispielsweise zu Ausbildungszwecken geschieht und – mit vorheriger **Einwilligung der geschützten Person**. Wenn diese aber auf die absolute Vertraulichkeit ausdrücklich besteht, könnte die Strafandrohung aktiviert sein. Nach gleicher Maßgabe ist auch ein Mitschnitt des Gespräches zulässig bzw. unzulässig.

Bei einer ausnahmsweisen Einwilligung ist zudem stets auf eine strenge Konformität des Vorgehens und der Verarbeitung mit der DSG-VO/DSG-EKG zu achten.

Nicht-gesprochene Medien sind nicht durch § 201 StGB erfasst. So unterfällt etwa ein Live-Chat nicht dem § 201 StGB, wohl aber dem § 203 StGB (s.o.).

B.2.3.5.4 § 223 StGB

Eine weitere in strafrechtlicher Hinsicht relevante Vorschrift ist § 223 StGB. Danach ist strafbar, wer „einen anderen körperlich misshandelt oder an der Gesundheit beschädigt“. Da mit der Digitalisierung neue Verfahrens- und Behandlungswege eröffnet werden, ist eine Körperverletzung, die beispielsweise auch durch psychisch zugefügte Schmerzen begründet werden kann, auch auf digitalem Wege möglich.

Sofern innovative, digitale Wege der Behandlung erfolgen sollen, können an die Aufklärungspflicht erhöhte Anforderungen zu stellen sein. Alle relevanten Vor- und Nachteile (zB. der Einsatz einer neuen und noch nicht endgültig erprobten Methode) sind dann im Zuge der Aufklärung der Klientin/des Klienten umfassend darzustellen, so dass eine informierte eigenverantwortliche Entscheidung getroffen werden kann. Die technische Innovation darf keinesfalls zu einer Beeinträchtigung der Rechte der Klient*innen bzw. Patient*innen führen, deren Selbstbestimmung ein kaum zu überschätzendes Gut darstellt.

[209] Siehe zu einer hilfreichen Basis-Checkliste vor Einführung eines BYOD-Modells: https://www.eicar.org/wp-content/uploads/2018/05/Leitfaden_BYOD_Finale_Einzelseiten.pdf, S. 33ff. (zuletzt abgerufen am 21. Mai 2020).

B.2.3.5.5 Exkurs: Selbstbestimmungsrecht in der Medizin

Der Begriff des Selbstbestimmungsrechts entstammt der Moralphilosophie und wurde Ende des 19. Jahrhunderts zu einem politische Forderungen zunehmend bestimmenden Faktor. Daraus folgt beispielsweise, dass ein ärztlicher Eingriff in die körperliche Unversehrtheit nicht per se gerechtfertigt sein kann, sondern immer eine informierte Einwilligung seitens der Patientin/des Patienten voraussetzt. Es ist unabdingbarer Bestandteil des grundgesetzlich (in Art. 2 Abs. 1 GG) geschützten Rechts auf freie Persönlichkeitsentfaltung, über das Ob und das Wie der eigenen Heilung zu verfügen.

Dem Selbstbestimmungsrecht unterfällt aber auch die informationelle Selbstbestimmung, dh. der Schutz vor der unbefugten Verarbeitung von Daten. Hier wird es ergänzt durch das sogenannte IT-Grundrecht, das explizit die in informationstechnischen Systemen verarbeiteten persönlichen Daten schützt.[210] Auch unterfällt ihm auch das Recht auf Nichtwissen der genetischen Prägung sowie auf Dokumentation und Rechenschaft über ärztliche Behandlung und Einsichtnahme in die entsprechenden Akten. Es schützt ferner die Freiwilligkeit der Angabe von (Notfall-)Daten auf einer Gesundheitskarte. Eine Verletzung des Selbstbestimmungsrechts kann zivilrechtliche (Schadensersatz) wie auch strafrechtliche Auswirkungen haben (wie gesehen etwa nach §§ 203, 223 StGB).

B.2.3.5.6 Exkurs: Ärztliches Berufsrecht

Im Zusammenhang mit Digitalisierungsvorhaben können auch Normen des ärztlichen Berufsrechts wesentlich sein. Bei diesen handelt es sich um landesspezifisches Satzungsrecht, das sich weitgehend an der von der Bundesärztekammer vorgegebenen Musterberufsordnung orientiert. In dieser sind die grundlegenden Pflichten des Berufsstandes festgelegt.[211] Im Rahmen der Digitalisierung besonders wichtig sind §§ 2, 7, 8 und 9 MBO-Ä.

Entscheidungen durch KI

So heißt es in § 2 Abs. 4 MBO-Ä: „Ärztinnen und Ärzte dürfen hinsichtlich ihrer ärztlichen Entscheidungen keine Weisungen von Nichtärzten entgegennehmen.“

Diese Vorschrift könnte Schwierigkeiten im Umgang mit KI-Lösungen bereiten, wenn und soweit diese Vorgaben für die Behandlung macht. Die Vorschrift möchte die fachliche[212] Unabhängigkeit der ärztlichen Entscheidung sichern. Zwar ist klar, dass einer KI die von der Vorschrift implizit vorausgesetzte Personenqualität fehlt, dass also eine KI per se kein „Nichtarzt“ im Sinne der Vorschrift sein kann.

Auch ist klar, dass eine Grenze überschritten sein wird, wenn eine KI – etwa eine Medical App – ohne zwischengeschaltete Plausibilitätskontrolle durch eine Ärztin oder einen Arzt eine ärztliche Entscheidung trifft und diese unmittelbare Umsetzung findet. Autonome Entscheidungen eines technischen Systems mit unmittelbaren Auswirkungen auf die Patienten sind nach aktuellem Verständnis berufsrechtlich ausgeschlossen.

Probleme können sich beispielsweise aber dann ergeben, wenn die Weisung der nichtärztlichen Unternehmensleitung die Befolgung der von einer KI unterbreiteten Handlungsvorgaben verlangte. Eine nähere Regelung solcher Konstellationen durch die Bundesärztekammer ist wünschenswert, so dass für die Anwender*innen einer KI Rechtssicherheit geschaffen wird.

Festzuhalten ist aber, dass die Berufsausübungsgrundsätze des § MBO-Ä wie auch die Wertentscheidungen des § 1 MBO-Ä kein statisches Programm schaffen, sondern inhaltlich vielmehr einer dynamischen Entwicklung gegenüber offen sind. Technisierung in der Medizin ist Teil des Fortschritts, mit dem die MBO-Ä mithalten kann.

Fernbehandlung

§ 7 Abs. 4 MBO-Ä regelt die Fernbehandlung: „Ärztinnen und Ärzte beraten und behandeln Patientinnen und Patienten im persönlichen Kontakt. Sie können dabei Kommunikationsmedien unterstützend einsetzen. Eine ausschließliche Beratung oder Behandlung über Kommunikationsmedien ist im Einzelfall erlaubt, wenn dies ärztlich vertretbar ist und die erforderliche ärztliche Sorgfalt insbesondere durch die Art und Weise der Befunderhebung, Beratung, Behandlung sowie Dokumentation gewahrt wird und die Patientin oder der Patient auch über die Besonderheiten der ausschließlichen Beratung und Behandlung über Kommunikationsmedien aufgeklärt wird.“

Entgegen des früheren Fernbehandlungsverbots ist es durch die Neuregelung dieser Vorschrift nun unter näher bestimmten Umständen der Sicherstellung der Qualität

[210] Grundlegend BVerfG, Urteil vom 27. Februar 2008 _ 1 BvR 370/07.

[211] Zum Zeitpunkt des Redaktionsschlusses gilt die MBO-Ä 1997 in der Fassung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt, geändert durch Beschluss des Vorstandes der Bundesärztekammer am 14.12.2018.

[212] Unternehmerische und organisatorische Weisungen, etwa zur Arbeitszeit etc. sind hiervon also nicht umfasst.

erlaubt, eine Beratung und Behandlung ausschließlich über Kommunikationsmedien durchzuführen.

Durch die Bedingtheit der Erlaubnis werden hohe Anforderungen an eine entsprechende Dokumentation der Bedingungen sowie die Aufklärung der Patient*innen gestellt. Die Nichterfüllung dieser sich mittelbar ergebenden Pflichten kann einen ärztlichen Haftungsfall begründen. Die sich bei Übersetzung der Vorschrift in das Landessatzungsrecht ergebenden Spezifika sind in jedem Fall besonders zu beachten.

B.2.3.5.7 Checkliste Strafrechtliche Aspekte (insbesondere der Online-Beratung)

- Ist bekannt, welche Mitarbeiter*innen der besonderen Verschwiegenheitsverpflichtung unterfallen und sind diese hinsichtlich der Konsequenzen umfassend informiert und hierauf verpflichtet?
- Ist sichergestellt, dass alle Arbeitsprozesse auf die Verpflichtung zur Verschwiegenheit angemessen und effektiv Rücksicht nehmen?
- Ist die ggf. erfolgende Einbindung Dritter nach dem obenstehenden Katalog rechtssicher gestaltet?
- Wird nur in sehr gut begründeten und dokumentierten Ausnahmefällen mit der Einwilligung/dem Einverständnis der betroffenen Person gearbeitet?
- Ist ein eventuelles Mithören von vertraulichen Informationen durch weitere Berufsgeheimnisträger durch Einwilligung/ Einverständnis gesichert?
- Ist der Einsatz digitaler Behandlungsmethoden durch eine umfassende und dokumentierte Aufklärung der Betroffenen über sämtliche Risiken begleitet, so dass diese eine informierte, eigenverantwortliche Entscheidung treffen können?

TEIL C

In den vorangehenden Kapiteln wurde bereits anhand der Besonderheiten der jeweils gewählten Anwendungsart (App oder Online-Plattform/-Beratung) auf spezifische Fragestellungen eingegangen. Ziel dieses Abschnittes ist es, diejenigen Fragen näher zu beleuchten, die sich für beide gleichermaßen stellen.

C.1 DATENSCHUTZ UND IT-SICHERHEIT

Zentrale Bedeutung im Rahmen von Digitalisierungsprojekten haben freilich Datenschutz und IT-Sicherheit. Für die beiden sich ergänzenden Rechtsgebiete steht die Verhinderung des unberechtigten Zugriffs auf schützenswerte Daten im Vordergrund, wobei die Vorschriften zur IT-Sicherheit – im Gegensatz zum Datenschutz – auch den Schutz nicht personenbezogener Daten sowie der Infrastruktur bezwecken.

Der präventive Ansatz beider Rechtsgebiete lässt eine leistungsfähige Governance damit vom **Vorsorgegedanken** bestimmen. Im Folgenden soll der rechtliche Rahmen einer solchen vorsorgeorientierten Plattform- bzw. Anwendungs-Governance abgesteckt werden, zunächst aus datenschutzrechtlicher (1) und dann aus IT-sicherheitsrechtlicher (2) Perspektive.

C.1.1 DATENSCHUTZ[213]

Ging es dem Datenschutz zum Zeitpunkt seiner erstmaligen Diskussion in den 1970er Jahren noch vornehmlich um technische Aspekte wie den Schutz der Daten vor Verlust, so hat sich mit der zunehmenden Verbreitung und Vernetzung von Computern und deren persönlicher Nutzung der Schutz der Persönlichkeitsrechte als immer relevanter gezeigt.

Der Schutz der Privatsphäre unterfällt dem **allgemeinen Persönlichkeitsrecht**, das in Art. 2 Abs. 1 GG (Freie Entfaltung der Persönlichkeit) iVm. Art. 1 Abs. 1 GG (Menschenwürde) als verankert gilt. In seinem für das heutige Datenschutzrecht elementar wichtigen Volkszählungsurteil[214] prägte das Bundesverfassungsgericht bereits 1983 das **„Recht auf informationelle Selbstbestimmung“** und führte dazu aus:

„Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechno-

[213] Auf die umfangreichen Informationen, die der Beauftragte für den Datenschutz der EKD in seiner Infothek (https://datenschutz.ekd.de/infothek/) bereitstellt, sei hier bereits allgemein verwiesen. Die Seiten liefern vielfältige hilfreiche Informationen, Orientierungen und Muster. Im jeweiligen Zusammenhang wird darauf im Folgenden auch vereinzelt verwiesen.

[214] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

logien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Damit hat das Bundesverfassungsgericht verdeutlicht, dass die Angabe personenbezogener Daten **nie belanglos** ist. Daher muss jede gewählte digitale Lösung, da sie in aller Regel mindestens die Verarbeitung personenbezogener IP-Adressen umfasst, auch datenschutzrechtlich sicher sein. Es gibt allerdings keinen Grund, sich vor dem Datenschutzrecht zu fürchten. Wird der Datenschutz schon **von Beginn der konkreten Planung an mitgedacht, können Schwierigkeiten weitestgehend vermieden** werden (Stichwort: Privacy by Design und Default[215]).

Seit dem 25. Mai 2018 gilt die DS-GVO, die die bisherige deutsche Regelungspraxis im Wesentlichen fortschreibt,[216] allerdings einen verstärkt risikobasierten Ansatz verfolgt.[217] Über die Öffnungsklausel des Art. 91 DS-GVO[218] hat die EKD von der Möglichkeit Gebrauch gemacht, sich ein **eigenes Datenschutzrecht** zu geben. Vom Schutzniveau bleibt dieses aber nicht hinter den Vorgaben der DS-GVO zurück. Im Folgenden wird auf die Vorschriften beider Rechtskreise Bezug genommen.

Zunächst sollen die Grundzüge dargestellt werden. Besonders wesentliche Aspekte werden nachfolgend noch vertieft.

C.1.1.1 Einzelne Aspekte

Das Datenschutzrecht ist so konzipiert, dass es durch Beherrschungsasymmetrien ggf. entstehende informationelle Benachteiligungen der Nutzer*innen möglichst zu **verhindern bzw. ausgleichen** sucht. Es knüpft dafür zunächst an dem Begriff der Datenverarbeitung an. Als solche gilt nach Art. 4 DS-GVO

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

Im Ergebnis lässt sich damit sagen, dass jeglicher Vorgang im Zusammenhang mit personenbezogenen Daten eine Verarbeitung in diesem Sinne ist.[219]

C.1.1.1.1 Verbotsprinzip

Zentraler Aspekt des Datenschutzrechts ist es, dass **jegliche Datenverarbeitung** grundsätzlich verboten ist. Eine Ausnahme von diesem Grundsatz lassen die DS-GVO – und mit ihr alle weiteren Datenschutzvorschriften – nur zu, sofern und soweit eine Rechtsgrundlage die Datenverarbeitung erlaubt oder die betroffene Person einwilligt.

Die Datenverarbeitung auf Plattformen und sonstigen Anwendungen können vor allem auf der Basis

- einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a iVm. Art. 4 Nr. 11 und Artt. 7 und 8 DS-GVO (§ 6 Ziff. 2 iVm. § 4 Ziff. 13 und §§ 11 und 12 DSG-EKD),
- der Erfüllung eines Vertrages nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO (§ 6 Ziff. 5 DSG-EKD) oder
- einer Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (§ 6 Ziff. 3 und 4 DSG-EKD),

rechtmäßig erfolgen.

Das Merkmal **„Erfüllung des Vertrages"** ist weit zu verstehen und umfasst grundsätzlich auch die Begründung[220], die Änderung, Durchführung und die Beendigung von Verträgen

[215] Siehe C.1.1.1.3.
[216] Eine Ausnahme gilt für den Schutz von Beschäftigtendaten. Im Rahmen der europäischen Rechtsetzung war es nicht möglich, das hohe Schutzniveau, das Beschäftigtendaten in Deutschland genießen, transnational festzuschreiben. Als Kompromiss hat Deutschland über die DS-GVO hinausgehende Regelungen in § 26 BDSG getroffen.
[217] Im Ergebnis schließt der Gesetzgeber die lange zwischen Datenschutz und Informationssicherheit/IT-Sicherheit klaffende Lücke auf zukunftsfähige Weise.
[218] Dieser nimmt im Kern Rücksicht auf Art. 140 GG, nach welchem der Regelungsgehalt einzelner Artikel der Weimarer Reichsverfassung (hier insbesondere Art. 137 Abs. 3 WRV) zugunsten der Religionsgemeinschaften fortgelten.
[219] DiSpiecker genannt Döhmann: Digitale Mobilität: Plattform Governance, GRUR 2019, S. 341, 345.
[220] Vorvertragliche Maßnahmen werden von § 6 Ziff. 5 DSG-EKD klarstellend als mitumfasst benannt.

sowie die nachvertraglichen Sorgfaltspflichten; erfasst sind auch vertragsähnliche Konstellationen.[221]

Im Hinblick auf die **Interessenabwägung** ist hervorzuheben, dass hierdurch im Einzelfall auch die Nutzung der Daten für weitere Anwendungen[222], die Weiterentwicklung der Technik sowie Abwehr, Prävention und Nachverfolgung von IT-Sicherheitsattacken gehören kann.

Der **Einwilligung** kommt aber – jedenfalls im vorliegenden Zusammenhang – die wesentlichste Bedeutung zu. Liegt sie vor, steht einer angemessenen Datenverarbeitung kaum etwas im Wege, wenn auch freilich die Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 2. Hs. DS-GVO (§ 5 Abs. 2 iVm. § 27 Abs. 1 S. 1 DSG-EKD), die Informationspflichten nach Art. 12 ff. DS-GVO sowie die sonstigen Rechte der Betroffenen nach Art. 16 ff. DS-GVO (§ 16ff. DSG-EKD) zu beachten sind.

Aufgrund ihrer weitreichenden Wirkung sind an das Vorliegen einer wirksamen Einwilligung aber hohe Anforderungen, insbesondere an ihre **Freiwilligkeit** und **Informiertheit** sowie die **Zweckbestimmtheit und –beachtung** zu stellen. Vor allem darf das Zustandekommen eines Vertrags nicht von einer Einwilligung in eine dafür nicht erforderliche Verarbeitung (zB. Newsletter oder Werbetracking) abhängig sein (Kopplungsverbot).

Das **Kopplungsverbot** nach Art. 7 Abs. 4 DS-GVO lässt die Freiwilligkeit der Einwilligung umso unwahrscheinlicher werden, je geringer die Wahlmöglichkeiten der Nutzer*innen ausfallen. So darf insbesondere ein Monopolist keine eigennützigen Folgen an die Einwilligung seiner Nutzer*innen binden. Die Einwilligung muss freiwillig erfolgen. Macht man das Zustandekommen des Vertrags von einer Einwilligung zu einer dafür nicht erforderlichen Verarbeitung (zB. Newsletter) abhängig, liegt eine unzulässige Kopplung vor.

Flankierend unterbindet auch das AGB-Recht übermäßige (Weiter-)Verwendungen der Einwilligung im Sinne überraschender Klauseln. Es ist also allenthalben erforderlich, dass die vorgesehenen Verwendungen vollständig vorhersehbar und nachvollziehbar beschrieben und nicht unbotmäßig sind. Wenn eine vielseitige Verwendung für durchschnittliche Nutzer*innen nicht mehr überschaubar ist, wird eine hierfür eingeholte Einwilligung unwirksam sein.

Praxis-Hinweis:
Es ist zu beachten, dass die Verarbeitung sich nicht alternierend auf eine Einwilligung oder einen anderen rechtlichen Grund stützen darf. Die Verantwortliche kann also nicht einfach einen anderen rechtlichen Grund dann heranziehen, wenn die Einwilligung nicht gegeben oder widerrufen wird. Das würde der notwendigen Transparenz und Fairness nicht gerecht. Es ist daher immer dann, wenn andere rechtliche Gründe zur Verarbeitung bestehen, **nicht** mit der Einwilligung zu arbeiten.

C.1.1.1.2 Zweckbindung und -änderung

Die Daten dürfen grundsätzlich nur zu dem Zweck verarbeitet werden, zu welchem sie ursprünglich rechtmäßig erhoben wurden. Die Datenverarbeiterin ist an den originären Zweck der Datenverarbeitung bei allen weiteren Schritten grundsätzlich gebunden. Die Festlegung eines neuen Zwecks (die „Umwidmung“ der Verarbeitung) ist grundsätzlich ausgeschlossen.

Die **Zweckänderung** muss sich selbst wieder durch einen gesetzlichen Erlaubnistatbestand[223] oder eine Einwilligung rechtfertigen lassen. Das ist entweder der Fall, weil sie sich auf einen eigenen Rechtsgrund stützen kann (etwa Einwilligung, Interesse oder gesetzliche Verpflichtung) oder – in eng begrenzten Fällen – der ursprüngliche Zweck auch die Zweckänderung trägt (Art. 5 Abs. 1 lit. b 2. HS iVm. Art 6 Abs. 4 DS-GVO bzw. § 7 Abs. 2 DSG-EKD).

Konsequenterweise bestimmt § 7 Abs. 5 DSG-EKD, dass die Verarbeitung von besonderen Kategorien personenbezogener Daten für andere Zwecke nur rechtmäßig ist, wenn die Voraussetzungen vorliegen, die nach § 13 Abs. 2 DSG-EKD an eine Verarbeitung solcher Daten zu stellen sind.

C.1.1.1.3 Privacy by Design und Privacy by Default

Lauschende Geräte und Anwendungen sollten der Vergangenheit angehören. Die (DS-GVO Artt. 5 DSGVO, 25, vgl. § 71 BDSG) und das DSG-EKD (§ 28 DSG-EKD) verlangen, dass dem Datenschutz bereits bei der Gestaltung der Technik (by design) und der Voreinstellungen von zB. Apps und Webseiten (by default) Rechnung getragen wird. Das erfordert, dass sich die Verantwortliche schon sehr früh, nämlich bereits in der **Planungsphase** mit dem Thema Datenschutz umfassend beschäftigt und dessen Prinzipien einbezieht. Dabei ist dem Grundsatz der Datenminimierung zu entsprechen, Konfigurationsaufwand zu vermeiden und ein ausreichendes Datenschutzniveau zu gewähren. Jede Anwendung darf nur die für ihre Funktion essentiellen Daten erheben. Die Datenverarbeitung muss jederzeit für die Nutzer*innen transparent

[221] Albers/Veit, in: Wolff/Brink (Hrsg.); BeckOK Datenschutzrecht, 31. Ed., Rz. 30f. zu § 6 DS-GVO.
[222] Nachträgliche Zweckänderungen der Datenverarbeitung ohne Einwilligung des Betroffenen sind allerdings nur in engen Grenzen möglich (Art. 6 Abs. 4 DS-GVO, § 7 DSG-EKD, §§ 23, 24 BDSG).
[223] Nachträgliche Zweckänderungen sind ohne Einwilligung des Betroffenen nur in engen Grenzen möglich (Art. 6 Abs. 4 DS-GVO, § 7 DSG-EKD, §§ 23, 24 BDSG).

und steuerbar sein und möglichst anonymisiert und, wenn dies im Rahmen der legitimen Zwecke nicht umsetzbar ist, möglichst pseudonymisiert erfolgen.

Die Dienstleisterin, die die Anwendung entwirft, muss **vertraglich verpflichtet** werden, Privacy by Design und Default als Leitlinie zu beachten, und sollte dies nach Umsetzung **schriftlich bestätigen**, das getan zu haben. Bei der Abnahme ist dies **überprüfend zu berücksichtigen**.

Hervorzuheben ist, dass Privacy by Design ein integraler Bestandteil des SDLC (Software Development Lifecycle) des Change-Managements ist. Privacy by Design ist bei Veränderungen der Gegebenheiten immer mitzudenken, zB. wenn eine Änderung der Strategie auch die Nutzung von Marketing-Cookies einbezieht. Bei der Gestaltung von Veränderungsmaßnahmen müssen also ihre datenschutzrechtliche Relevanz geprüft und die Grundsätze der Privacy by Design und Privacy by Default in organisatorische, prozessuale und technische Anforderungen übersetzt werden. Ergänzend sollte eine Datenschutz-Folgenabschätzung[224] erfolgen oder zumindest deren Notwendigkeit gründlich eruiert werden.

C.1.1.1.4 Transparenzgebot

Eine der wesentlichsten Aspekte der durch das Datenschutzrecht verfolgten Selbstbestimmung des Einzelnen ist es, für Transparenz der Datenverarbeitungen zu sorgen. Bestimmendes Kalkül hierfür ist, dass die gut informierte Person eine bessere Kontrolle über ihre Daten erreicht. Dem liegt wiederum der Gedanke zugrunde, dass die freiheitliche Grundordnung im Sinne einer freiheitlichen Gesellschaft in Zeiten zunehmender Digitalisierung anders nicht, insbesondere nicht langfristig gesichert werden kann.

Für die Verantwortlichen folgt daraus, dass der betroffenen Person in **angemessener Weise Informationen zur jeweiligen Datenverarbeitung zu geben** sind. Abhängig davon, wer die Daten erhoben hat, ist **umfassend zu informieren**. Durch leicht zugängliche Informationen sollen insbesondere die in Betracht kommenden **Datenströme – auf eine verständliche Art und Weise – nachvollziehbar** werden.

Praxishinweis:
Die bisherige Praxis langer, inhaltlich und zeitlich kaum zu erfassender Texte, dürfte dem nicht genügen. Eine **gestufte Darstellung**, etwa mit Einrückungen und Hervorhebungen, kann die Lesbarkeit verbessern und damit die Rechtswirksamkeit erhöhen (**layered approach**). Je mehr Daten erhoben werden, desto umfänglicher muss informiert werden, und desto mehr muss in einem fortwährenden Überprüfungsprozess die Richtigkeit der Informationen sichergestellt sein.

C.1.1.1.5 Dokumentationspflicht und fortlaufende Evaluation (Datenschutzkonzept/Datenschutzmanagement)

Darüber hinaus haben die Verantwortlichen im Falle einer anlassbezogenen oder auch anlasslosen Überprüfung durch die Autoritäten, insb. die behördlichen Datenschutzbeauftragten, ein **wirksames Datenschutzmanagement (Datenschutzkonzept) nachzuweisen**. De facto bedeutet das eine Beweislastumkehr: Ist der Nachweis eines organisierten, dokumentierten und regelmäßig kontrollierten Umgangs mit Datenschutz und Informationssicherheit nicht möglich, ist ein ggf. schadenersatzpflichtiger Verstoß nicht auszuräumen.

Ein DS-GVO-konformer **Datenschutz setzt ein Datenschutzmanagement-Systems auf Basis eines PDCA-Zyklus (Demingkreis)** voraus. Prozesse sind nicht nur einmalig zu definieren und etablieren, sondern **permanent zu überprüfen und ggf. anzupassen**. Art. 32 Abs. 1 lit. d DS-GVO bzw. § 27 Abs. 1 Ziff. 4 DSG-EKD fordern dieses aus dem Qualitätsmanagement bekannte Vorgehen ausdrücklich.

Spätestens mit der Einführung digitaler Lösungen empfiehlt es sich, ein **Datenschutzkonzept** zu etablieren.[225] Nach § 5 Abs. 2 DSG-EKD ist dies ohnehin notwendig. Folgende rechtliche Punkte sollten als Mindestinhalt vom Konzept umfasst sein:

Aktuelle Rechtslage seit Mai 2018

- **§ 5 Abs. 2** = Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können **(Rechenschaftspflicht)**.
- **§ 17** Informationspflicht bei unmittelbarer Datenerhebung
- **§ 27** Technische und organisatorische Maßnahmen, IT-Sicherheit
- **§ 31** Verzeichnis von Verarbeitungstätigkeiten
- **§ 32** Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
- **§ 34** Datenschutz-Folgenabschätzung

Das Konzept sollte schließlich zu einem lebendigen und belastbaren **Datenschutzmanagement-System** (DSM) ausgearbeitet werden. Gemäß § 27 DSG-EKD hat die Verantwortliche Stelle unter Berücksichtigung des Kontextes, des Risikos und der Eintrittswahrscheinlichkeit Maßnahmen zu planen, umzusetzen, zu überprüfen und bei Bedarf zu verbessern. Dies entspricht dem **Demingkreis/PDCA-Zyklus**, der ein etabliertes Prinzip sorgfältigen Managements darstellt. Er gehört zu den konstituierenden Elementen eines funktionierenden Datenschutzmanagement-Systems.

[224] Siehe unter C.1.1.1.8.

[225] Siehe dazu näher auch die Hinweise des BfD-EKD https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-erstellung-eines-datenschutzkonzeptes/ (zuletzt abgerufen am 13. Juli 2020).

Fig. C.1: Illustration eines PDCA-Zyklus (Demingkreis)

Das Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder[226] sowie das (noch zu erarbeitende) kirchliche Standard-Datenschutzmodell bieten geeignete Anleitungen, um die rechtlichen Anforderungen der DS-GVO/DSG-EKD in **systemische Bedingungen** zu überführen. Zu diesem Zweck erfasst etwa das SDM zunächst die rechtlichen Anforderungen der DS-GVO/DSG-EKD und ordnet sie anschließend den Gewährleistungszielen Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit zu.

Daran anschließend beschreibt es **die praktische Umsetzung der Anforderungen sowie die notwendigen organisatorischen Rahmenbedingungen**. Das SDM überführt damit die rechtlichen Anforderungen der DS-GVO/DSG-EKD über die Gewährleistungsziele in **technische und organisatorische Maßnahmen**, die im Referenzmaßnahmen-Katalog des SDM detailliert beschrieben werden; so beispielsweise die regelmäßige Überprüfung der Verschlüsselungs-Algorithmen auf ihre **Aktualität**, die Anpassung der **Belastungstests** an die Benutzerzahlen und die Absicherung der Zugangs- und Zugriffssicherung durch **Penetrationstests**.

Es unterstützt somit die **Transformation abstrakter rechtlicher Anforderungen in konkrete technische und organisatorische Maßnahmen**. Auf der Grundlage eines derart erarbeiteten Systems kann ein geordneter Datenschutzmanagement-Prozess aufgesetzt werden. Ein solcher Prozess dient der Verantwortlichen bei der systematischen Planung, dem dauerhaften Betrieb und der regelmäßigen Überprüfung der Datenschutzkonformität sowie der ggf. notwendigen Anpassung und Verbesserung der Datenverarbeitungsprozesse. Damit schafft er die **notwendige Transparenz** sowohl für die Verantwortliche selbst als auch für die ggf. prüfende Behörde.

Fig. C.2. Vereinfachte Darstellung des Wirkungszusammenhangs eines Datenschutzmanagementsystems

C.1.1.1.5.1 Vertiefung: Technisch-Organisatorische Maßnahmen (TOM)[227]

In §§ 27, 28 DSG-EKD (Art. 32 DS-GVO) wird relativ ausführlich beschrieben, nach welchen Kriterien TOM zu wählen sind, um ein ausreichendes Schutzniveau sicherzustellen. Um überhaupt feststellen zu können, was ein im jeweiligen Einzelfall ausreichendes Sicherheitsniveau bedeutet, muss die verantwortliche Stelle Klarheit über den Schutzbedarf der relevanten personenbezogenen Daten besitzen, was durch eine Risikoanalyse ermittelt und bewertet werden kann.

Dabei sollte sich die Risikoanalyse an den **etablierten Standards aus der IT-Sicherheit/Informationssicherheit** orientieren, insbesondere an den BSI-Standard der 200er-Serie sowie dem Standard aus der ISO 27000er-Reihe (insbesondere 27005, ggf. ergänzt durch ISO 31000).[228] Wo möglich, sollte die Risikobewertung auf im Unternehmen bereits bestehenden Risikobewertungssystemen aufsetzen, so dass nicht nur Synergien erzielt, sondern der Umgang mit Datenschutzrisiken in das Management der allgemeinen Unternehmensrisiken eingegliedert wird.

Unter Berücksichtigung der ITSVO[229] (über § 27 Abs. 6 DSG-EKD) kann nach unterschiedlichen Schutzstufen (normal, hoch und sehr hoch) unterschieden werden.

[226] https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode_V20b.pdf (zuletzt abgerufen am 12. Juli 2020).
[227] Unter IT-Sicherheit (C.1.2) wird das Thema weiter vertieft.
[228] Dazu genauer unter C.1.2.
[229] https://www.kirchenrecht-ekd.de/document/32147 (zuletzt abgerufen am 26. Juni 2020)

Dabei sind objektive Kriterien für Eintrittswahrscheinlichkeit und Schwere des Risikos[230] für Rechte und Freiheiten natürlicher Personen festzulegen und diese ins Verhältnis zu setzen. Bei der auf dieser Abschätzung gründenden Auswahl geeigneter TOM ist einerseits auf den **Stand der Technik** und andererseits auf die **Verhältnismäßigkeit des dazu notwendigen Aufwands** abzustellen.

Generell sind TOM bestenfalls:

1. auf einer Risikobetrachtung basierend;
2. nachweisfähig;
3. berücksichtigen den Kontext;
4. entsprechen dem Stand der Technik und
5. werden regelmäßig überprüft und ggf. aktualisiert.

Inhaltlich sind die Risiken für die Rechte und Freiheiten der potentiell betroffenen Personen zu berücksichtigen, wobei neben materiellen auch moralische Schäden einzubeziehen sind.

Nach Art. 32. Abs. 1 lit. b DS-GVO/§ 27 Abs. 1 Ziff. 2 DSG-EKD ist als Kern der IT-Sicherheit die Vertraulichkeit, Integrität, **Verfügbarkeit und Belastbarkeit der Systeme** sicherzustellen. Da die Begriffe gesetzlich nicht näher definiert werden, ist es sinnvoll, sich an den Definitionen aus der IT-Sicherheit (z. B. BSI) zu orientieren.

Damit sind **Maßnahmen zum Schutz der Vertraulichkeit** ua. die sichere Authentifizierung sowie Datenverschlüsselung bei Speicherung und Transport. Auch durch Pseudonymisierung kann die Vertraulichkeit geschützt werden. Als Maßnahmen zum **Schutz der Verfügbarkeit** kommen ua. Backup-Systeme und Redundanzen der technischen Infrastruktur in Betracht. Die **Integrität** kann beispielsweise durch kryptographische Hash-Verfahren gesichert werden. Hierdurch können mögliche Manipulationen frühzeitig erkannt und verhindert werden. Bei der **Belastbarkeitsprüfung** wird dem Umstand Rechnung getragen, dass Systeme von einer Vielzahl von Anwender*innen gleichzeitig genutzt werden können. Zu beachten ist, dass im Hinblick auf all die Parameter nicht nur die eingesetzte Software und Kern-Hardware zu überprüfen sind, sondern das **gesamte Netzwerk und Schnittstellen**.

Schließlich fordert der Gesetzgeber mit Art. 32 Abs. 1 lit. c DS-GVO/§ 27 Abs. 1 Ziff. 3 die Fähigkeit, die personenbezogenen Daten nach einem Zwischenfall rasch **wiederherzustellen**. Nicht nur die technische Seite der Wiederherstellung ist dabei zu berücksichtigen. Vielmehr geht es auch darum, wie die in der Zwischenzeit erhobenen Daten nach dem Zwischenfall geordnet in das System wieder eingespielt werden können. Insbesondere Krankenhäuser bedürfen insoweit geeigneter Ausfallsysteme.

Typische TOM sind etwa die **Zugriffs- bzw. Zutrittskontrolle (sog. Zugangskontrolle)**, die Datensicherung, Datenlöschung, Pseudonymisierung bzw. Anonymisierung etc. Häufig werden TOM dergestalt missverstanden, dass zu ihnen nur schlicht technische Einrichtungen gehören. Dabei gehen sie weit über diese hinaus. Etwa auch die **Verpflichtung der Mitarbeitenden zur Verschwiegenheit und entsprechender Schulung** kann dazu gehören (Art. 32 Abs. 4 DS-GVO bzw. § 27 Abs. 5 DSG-EKD).

Die Verantwortliche muss zudem den Nachweis führen können, dass sie ihre Pflichten einhält (Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO bzw. § 5, 27 DSG-EKD). Dieser **Nachweispflicht** kann am geeignetsten nachgekommen werden, wenn die Mitarbeitenden eine **schriftliche Erklärung** zur Verpflichtung abgeben.[231] Um aber zu verhindern, dass die Mitarbeitenden das Formular nicht einfach nur unterschreiben, ohne entsprechende Merkblätter gelesen zu haben, sollte auf eine **begleitende mündliche Unterrichtung** nicht verzichtet werden, obwohl Art. 39 Abs. 1 lit. a DS-GVO bzw. § 38 S. 2 Ziff. 3 DSG-EKD eine mündliche Unterrichtung nicht vorschreibt. Die Belehrung sollte arbeitsplatzbezogen erfolgen. Eine regelmäßige Wiederholung ist auch vor dem Hintergrund der Nachweispflichten zu empfehlen.

Die Definition, Umsetzung, Dokumentation sowie die Sicherstellung von Kontrolle und Anpassung häufig umfangreicher TOM setzt – wie zuvor gezeigt – die Etablierung eines geordneten Datenschutzmanagement-Systems voraus, für das **Zertifizierungen** zunehmend an Bedeutung gewinnen werden.

Einige **Fragestellungen**, die eine Näherung an notwendige technische und organisatorische Maßnahmen erlauben:

- Ist es möglich, die notwendigen Daten von Beginn an anonymisiert/pseudonymisiert zu erheben (vor allem dann, wenn besondere Kategorien i.S. des Artikels 9 DS-GVO erhoben werden)?
- Welche technischen Vorkehrungen erlauben die verschlüsselte Speicherung personenbezogener Daten bei der Auftragsverarbeiterin?
- Wie ist der Zugang zum Cloud-System geregelt (ausreichend sicheres Passwort, getrennte Zugänge für weitere berechtigte Benutzer*innen)?
- Wer hat bei Auftraggeberin und der Auftragsverarbeiterin Zugang zu den Daten und wie ist der Zugang geregelt? Kann der Zugang protokolliert werden und wenn ja, in welcher nachprüfbaren und manipulationsgeschützten Form?
- Wie sind die Schreib- und Leserechte geregelt, wenn mehr als eine Person Zugang zu den in der Cloud gespeicherten Daten hat und wer hat das

[230] Siehe dazu auch näher das ausführliche Papier #09 des Beauftragten für den Datenschutz der EKD (https://datenschutz.ekd.de/wp-content/uploads/2018/04/09-Kurzpapier-Risiko.pdf - zuletzt abgerufen am 26. Juni 2020).

[231] Siehe dazu die Hinweise des Datenschutzbeauftragten der EKD: https://datenschutz.ekd.de/infothek-items/verpflichtungserklaerung-von-mitarbeiten-den-auf-das-datengeheimnis/ (zuletzt abgerufen am 11. September 2020).

Recht, diese Rechte zu administrieren (Rollen-/Rechtekonzept)?
- Wie werden Datenzugriffe und Datenänderungen fälschungssicher protokolliert?
- Wie wird die Verfügbarkeit des (Cloud-)Systems sichergestellt (z.B. bei Stromausfall, technischen Wartungsarbeiten etc.)? Wie wird das (Cloud-)System gegen technische Fehler und Angriffe von außen geschützt (Vulnerabilität/Stabilität)?
- Ist die komplette Wiederherstellung der gespeicherten Daten im Falle technischer Fehler, von externen Angriffen oder bei Zerstörung sichergestellt, durch welche Maßnahmen (Back-up, Redundanzen)?
- Wie erfolgt die Dokumentation der technisch-organisatorischen Maßnahmen (elektronisch, papiergestützt)?
- Wie erfolgt die regelmäßige Überprüfung, Bewertung, Evaluierung und Aktualisierung des geforderten Sicherheitsniveaus und der Wirksamkeit der eingesetzten technischen Verfahren?

C.1.1.1.5.1.1 Rollen und Berechtigungskonzept

Ein Rollen- und Berechtigungskonzept beschreibt, welche **Zugriffsregeln** für einzelne Benutzer oder Benutzergruppen auf die Daten eines IT-Systems gelten. Ferner regelt es die die Benutzerrechte betreffenden Prozesse, wie etwa das Anlegen von Usern oder die **regelmäßige Überprüfung** des Ist-Zustands anhand eines festgelegten Soll-Zustand. Es reicht daher typischerweise von Passwortrestriktionen über Rollendefinitionen bis hin zu Prozessbeschreibungen.

Inhalte sind daher insbesondere:

- Rollen
- Berechtigungen
- Zugriffsregelungen
- Dokumentationen
- Prozessdefinitionen
- Kontrollen

Für die Anlage des Konzepts empfiehlt es sich mit der Neuanlage von Benutzern zu beginnen. Hierzu muss ein Prozess zur Neuanlage definiert werden. Dabei ist insbesondere festzulegen, wer diese beantragen darf, genehmigt und ausführt. Es muss ferner bestimmt werden, wie ein Kennwort in Länge und Komplexität auszusehen hat und ob Kennwörter nach einer bestimmten Zeit ablaufen.

In einem weiteren Schritt werden die möglichen Berechtigungen definiert und wie sie vergeben werden. Dazu kann gehören, dass sich die Berechtigungen zu Rollen aggregieren lassen. Die Bezugnahme auf Rollen kann eine **wesentliche Vereinfachung** gegenüber der granulierten Vergabe von Berechtigungen darstellen. Dies insbesondere, wenn sich die Rollen an Funktionen knüpfen lassen. Dies lässt auch häufig eine einfachere Begründung von Berechtigungen zu. Für Vertretungsfälle sollte zudem ein Prozess erarbeitet bzw. die insoweit notwendige (zeitweise) Rechteübertragung entsprechend festgelegt werden.

Schließlich sollte das Konzept selbst festlegen, wie es in einem **fortlaufenden Prozess stets aktuell** gehalten wird.

C.1.1.1.5.1.2 Löschkonzept

Oft wird die Notwendigkeit, sich mit der **vorgeschriebenen Löschung** personenbezogener Daten konzeptionell zu beschäftigen, nicht beachtet oder diese nur unzureichend beantwortet. Insbesondere zur Umsetzung der datenschutzrechtlichen Prinzipien der Speicherbegrenzung und Datenminimierung kommt solchen Konzepten aber eine hervorgehobene Bedeutung zu.

Ein gelungenes Löschkonzept stellt insoweit die Auflösung des Konflikts zwischen den genannten Prinzipien und dem Speicherinteresse, das t**eilweise auch gesetzlich begründet ist**,[232] her.

Praxis-Hinweis:
Es ist nicht so, dass die Daten in jedem Falle nach Entfallen des eigentlichen Zweckes ihrer Verarbeitung automatisch gelöscht werden müssen. Es kann nämlich sein, dass die weitere Verarbeitung aus einem anderen Grund – etwa aus gesetzlicher Verpflichtung – notwendig wird.[233] Insbesondere die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[234], aber auch steuerrechtliche Gründe können eine **fortdauernde Verarbeitung rechtfertigen**. Dann kann es statt der Löschung angezeigt sein, den Zugriff zu beschränken.

Als echte Alternative zur Löschung kann sich im Einzelfall auch die (nicht mehr legaldefinierte) **Anonymisierung** empfehlen. Diese liegt vor, wenn die Daten nicht mehr mit machbarem Aufwand als personenbezogen interpretiert werden können. Sie sind dann dem Anwen-

[232] Dann ist das Interesse nach Art. 6 Abs. 1 S. 1 lit. c DS-GVO bzw. § 6 Ziff. 1 DSG-EKD begründet. Daneben kann ein berechtigtes Interesse angenommen werden.
[233] Zu beachten ist, dass die Betroffenen in der Datenschutzinformation schon in Vorhinein darauf umfassend hingewiesen werden müssen.
[234] Siehe dazu auch unter C.2.

dungsbereich der DS-GVO und des DSG-EKD entzogen. Die **Pseudonymisierung** (Art. 4 Nr. 5 DS-GVO/§ 4 Ziff. 6 DSG-EKD) und Einschränkung der Verarbeitung (Art. 4 Nr. 3 DS-GVO mit ErwG 67 DS-GVO bzw. § 4 Ziff. 4 DSG-EKD) werden die Löschung nur in besonderen Einzelfällen ersetzen können.

Das Löschkonzept sollte mit dem ihm inhaltlich in Verbindung stehenden Themen wie dem **Rollen- und Rechtekonzept, dem Identity/Access Management und der Umsetzung der Betroffenenrechte** (insbesondere Art. 15 ff. DS-GVO, wie die Rechte auf Auskunft, Berichtigung und Vergessenwerden, der Einschränkung der Verarbeitung sowie der Datenportabilität) abgestimmt sein. Seine Erstellung sollte namentlich folgende Punkte umfassen:

§ 1 Festlegung des Anwendungsbereiches und der Ziele

Zunächst erfolgt die Festlegung des Umfangs und der Detailtiefe des Konzepts. Dabei gilt es, das Ziel der möglichst vollständigen Compliance mit dem praxisnahen Gebot des risikoorientierten Ansatzes abzuwägen.

§ 2 Abwägung von Lösch- und Aufbewahrungsinteressen

Sodann sind die im Einzelfall einschlägigen gesetzlichen Aufbewahrungspflichten zu identifizieren. Darüber hinaus sind aber auch möglicherweise selbst nach Ablauf der Aufbewahrungspflicht verbleibende Aufbewahrungsinteressen zu identifizieren. Denn auch nach Ablauf der gesetzlichen Aufbewahrungsfrist kann ein legitimes Aufbewahrungsinteresse fortbestehen (zB. Abwehr von Rechtsansprüchen).

Umgekehrt kann schon vor Ablauf der Fristen die Anonymisierung/Pseudonymisierung oder die Einschränkung der Verarbeitung angezeigt sein. Darüber zu entscheiden, ist nicht immer eine rein rechtliche Frage, sondern dies sollte unter Einbeziehung der Geschäftsleitung und IT-Abteilung geklärt werden.

§ 3 Definition von Datenkategorien und ihren Aufbewahrungsfristen

Im nach § 1 festgelegten Anwendungsbereich sind basierend auf dem Abwägungsergebnis aus § 2 nun Datenkategorien[235] zu bilden, denen jeweils konkrete Fristen für die Löschung und/oder für die Einschränkung der Verarbeitung zugeordnet werden. Dafür muss feststehen, zu welchem Zweck die Daten verarbeitet werden.

§ 4 Definition der für die Löschung Verantwortlichen

Zudem muss konkret festgelegt werden, wer die jeweilige Löschung oder Anonymisierung bzw. die Pseudonymisierung oder Einschränkung der Verarbeitung umzusetzen hat. Diese Prozesse können manuell oder auch durch einen IT-gestützten Prozess automatisiert erfolgen.

§ 5 Einbettung in verwandte Themen

Das Löschkonzept ist immer Teil eines größeren Datenschutzmanagement-Systems. Daher weist es auch Bezüge zu benachbarten Themen des Datenschutzes auf und sollte auf die insoweit notwendigen Schnittstellen achten. Dazu gehören vor allem:

1. der Umgang mit individuellen Löschanträgen durch betroffene Personen nach Art. 17 Abs. 1 DS-GVO, die jenseits der standardisierten ggf. automatisierten Prozesse behandelt werden müssen;
2. die mit den weiteren Rechten der Betroffenen zusammenhängenden Prozesse und Berechtigungen, insbesondere zum Recht auf Auskunftserteilung, Berichtigung, Vergessenwerden, Einschränkung der Verarbeitung und der Datenportabilität sowie der Erteilung von Auskünften an Polizei und Strafverfolgungsbehörden;
3. dem Berechtigungskonzept (Rollen- und Rechtekonzept), das granuliert und konkret regelt, welche Personen Zugriff auf welche Daten haben. Dazu gehört auch ein funktionsfähiges Identity-&-Access-Management (IAM). Dieses stellt beispielsweise sicher, dass ausgeschiedenen Mitarbeitern automatisch Zutritts- und Zugangsrechte entzogen und die Berechtigungen bei Tätigkeits- oder Abteilungswechseln entsprechend geändert werden;
4. die Einbindung in ein vollständiges Informationssicherheitskonzept, das Berechtigungen und Löschungen auch bezüglich nicht-personenbezogener Informationen regelt,
5. die wesentlichen rechtlichen und auch technischen Aspekte bezüglich einer vollständigen also endgültigen Löschung;[236]
6. die Dokumentation der Zwecke, zu denen Daten erhoben, gespeichert oder anderweitig verarbei-

[235] Eine Datenkategorie oder Datenart bezeichnet eine Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird. Es empfiehlt sich, die unterschiedlichen Gruppen in einer Data Map zu sammeln und überschaubar zu machen. Zur Bestimmung der Datenarten erfolgt eine Orientierung an Rechtsvorgaben sowie an den Verwendungszwecken und an der Sensitivität der Daten. Unterschieden werden kann beispielsweise in Buchhaltungsdaten, Vertragsdokumente, Bewerberdaten, Standortdaten, Abrechnungsdaten, Gesundheitsdaten.

[236] Neben den rechtlichen Aspekten sind auch die IT-seitigen Aspekte der wirksamen Durchführung einer Löschung auf Speichermedien und in Datenbanken wichtig. Nicht selten werden Daten nur vermeintlich gelöscht, sind also nicht irreversibel „aus der Welt“. Siehe hierzu u. a. Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Sicheres Löschen magnetischer Datenträger.

tet werden. Deren Kenntnis ist eine elementare Voraussetzung für die Bemessung der Speicherfrist, da sie nach Ablauf der gesetzlichen Aufbewahrungsfristen noch einen von diesen unabhängigen Verarbeitungsgrund liefern können.

§ 6 Standards

Zur Sicherstellung der Compliance kann, wie generell bei der Datenschutz-Compliance, auf den Standard zu Compliance-Management-Systemen nach IDW PS 980 zurückgegriffen werden. Darüber hinaus setzt DIN 66398 Leitlinien zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Die Norm macht Vorschläge zum Aufbau eines Löschkonzepts und empfiehlt eine Vorgehensweise, nach der Regeln zum Löschen von personenbezogenen Daten abgeleitet werden können.

Praxis-Hinweis:
Häufig ist zu sehen, dass Verantwortliche Daten im Hinblick auf die Rechtsgründe der Art. 6 Abs. 1 lit. f bzw. Art. 9 Abs. 2 lit. f/§ 21 Abs. 3 Ziff. 5 DSG-EKD (**Verteidigung von Rechtsansprüchen**) und in Ansehung des § 199 Abs. 2 BGB für einen Zeitraum von dreißig Jahren speichern wollen. Dies ist problematisch. Zwar kann eine solche Speicherdauer durchaus in einzelnen Fällen angezeigt sein. Sie ist es aber sicher nicht in allen Fällen. Wenn also pauschal eine derart lange Speicherung von Daten erfolgt, dürfte dies rechtswidrig sein.

Zu empfehlen ist eine derart lange Speicherung nur in solchen Fällen, in denen Anhaltspunkte bestehen, die die Notwendigkeit der Abwehr von Ansprüchen anzeigen; wenn also etwa ein Beratungsfehler tatsächlich gegeben ist. Aber auch dann sollte nicht pauschal ein Zeitraum von dreißig Jahren gewählt werden, sondern die Notwendigkeit der fortdauernden Speicherung **regelmäßig überprüft** werden.

C.1.1.1.5.1.2.1 Checkliste Löschkonzept

- Für welche konkreten IT-Systeme und Datenbestände soll das Löschkonzept gelten und ist dieser Anwendungsbereich ausreichend?
- Welche Datenarten werden im Regelungsbereich des Löschkonzepts verwendet?
- Für welche dieser Datenarten ist welche Löschregel anzuwenden?
- Durch welchen Prozess wird die Löschung durchgeführt? Resultieren aus dem Schutzbedarf der Daten Sicherheitsanforderungen an den Löschmechanismus?
- Soweit Löschmechanismen konfigurierbar sind: Welche Parameter sind mit welchen Werten zu verwenden, um die zu löschenden Daten zu bestimmen?
- Wer ist für Ausführung und Überwachung des Löschprozesses verantwortlich?
- Wem gegenüber sind Nachweise über die Löschung zu führen und wie ist die Durchführung von Löschmaßnahmen zu dokumentieren?

C.1.1.1.5.1.3 Auftragsverarbeitungsvertrag (AVV), Art. 28 Abs. 3 DS-GVO, § 30 DSG-EKD

Werden Daten automatisiert erfasst und verarbeitet, muss ein **Verarbeitungsverzeichnis**[237] geführt werden, das auf einen Blick Auskunft darüber gibt, welche Daten auf welcher (Rechts-)Grundlage verarbeitet werden. Ist es zutreffend erstellt, bietet dieses Verarbeitungsverzeichnis eine gute Grundlage und Voraussetzung für die Entscheidung, welche Tätigkeiten ggf. **an Dritte ausgelagert** werden.

Im Zusammenhang mit der Einbindung Dritter, die nicht selbst als Verantwortliche gelten,[238] allzumal in Bereichen, die der Verschwiegenheitspflicht im Sinne des § 203 StGB unterliegen, ist der Abschluss eines **Auftragsverarbeitungsvertrages** (AVV) von entscheidender Bedeutung. Die Gewähr dafür, dass die Auftragsverarbeiterin eine technisch und organisatorisch einwandfreie Verarbeitung personenbezogener Daten vornimmt, **obliegt der Auftraggeberin** (Art. 28 Abs. 1 DS-GVO, § 30 Abs. 1 S. 1 DSG-EKD). Für Fehler bei der Ausführung der Datenverarbeitung **haftet die Auftraggeberin direkt**.

Bei der **Auswahl der Auftragsverarbeiterin** hat die Auftraggeberin sicherzustellen, dass sie eine Auftragsverarbeiterin heranzieht, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – **hinreichende Garantien** dafür bietet, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen der DS-GVO und des DSG-EKD genügen. Zertifizierungen, etwa nach ISO/IEC 27001 können der Auswahl mit zugrunde gelegt werden.

Zur Dokumentation und Sicherung der Auswahlkriterien hat die Auftraggeberin mit der Auftragsverarbeiterin

[237] Vgl. zur Erstellung eines solchen die Hinweise des Datenschutzbeauftragten der EKD: https://datenschutz.ekd.de/infothek-items/verzeichnis-der-verarbeitungstaetigkeiten/ (zuletzt abgerufen am 11. September 2020).

[238] Zur Abgrenzung der (gemeinsam) Verantwortlichen von den Auftragsverarbeiterinnen siehe die Guidelines 07/2020 on the concepts of controller and processor in the GDPR (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf – zuletzt abgerufen am 25. September 2020).

einen Auftragsverarbeitungsvertrag abzuschließen, in dem ein ausreichendes Sicherheitsniveau der den Auftragsverarbeiterin auferlegten Pflichten ablesbar ist. Folgenden **Mindestinhalt** sollte ein AVV aufweisen:[239]

- Gegenstand und Dauer des Auftrags/der Verarbeitung;
- Umfang, Art und Zweck der Verarbeitung der erhobenen Daten;
- Kategorien der personenbezogenen Daten (vor allem, wenn besondere Kategorien erhoben werden, vergl. Art 9 DS-GVO), Kreis der Betroffenen;
- Pflichten und Rechte der Berufsgeheimnisträger*innen (als Verantwortliche);
- Weisungen (inkl. Weisungsrechten), wie die Auftragsverarbeiterin die Daten zu verarbeiten hat (Umfang der Auftragsverarbeitung, Pflichten der Auftragsverarbeiterin); ist die Auftragsverarbeiterin der Auffassung, dass eine Weisung rechtswidrig ist, hat sie die Verantwortliche unverzüglich zu informieren;
- Art und Weise der Umsetzung der Sicherheit der Datenverarbeitung durch die Auftragsverarbeiterin, dh. insbesondere die nach § 27 DSG-EKD zu treffenden technischen und organisatorischen Maßnahmen sowie ihre Kontrolle durch die Auftraggeberin;
- Verpflichtung, die Auftraggeberin mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;
- Verpflichtung, der Auftragsverarbeiterin alle erforderlichen Informationen, zum Nachweis der Einhaltung ihrer Pflichten zur Verfügung stellt;
- Nachweis, dass die Auftragsverarbeiterin alle mit der Verarbeitung betrauten (befugten) Beschäftigten zur Vertraulichkeit entsprechend der einschlägigen gesetzlichen Vorgaben verpflichtet;
- sofern die Auftragsverarbeiterin (eine) weitere Auftragsverarbeiterin(nen) im Unterauftragsverhältnis einbeziehen können soll: Nachweis, dass die mit der Hauptauftragsverarbeiterin festgelegten Bedingungen auch bei der/den Unterauftragsverarbeiterin(nen) Anwendung finden;
- Verpflichtung der Auftragsverarbeiterin, Verletzungen des Schutzes personenbezogener Daten unverzüglich anzuzeigen, sowohl gegenüber der betroffenen Person als auch gegenüber der Auftraggeberin, sowie zur evtl. Benachrichtigung der zuständigen Aufsichtsbehörde (Landesdatenschutzbeauftragte/r) durch den/die Auftraggeberin, wenn mit der Verletzung der Schutzrechte hohe Risiken für die Betroffenen und/oder die Auftraggeberin einhergehen;
- Ggf. Durchführung einer Datenschutz-Folgenabschätzung[240] durch die Auftragsverarbeiterin;
- Berichtigung, Löschung und Sperrung von Daten, inkl. der Festlegung, wie die Löschung bzw. Rückgabe der Datenträger bzw. der bei der Auftragsverarbeiterin gespeicherten Daten nach Beendigung des AV-Vertrages erfolgt, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
- Vereinbarung der Möglichkeit, die Einhaltung der Vereinbarung vor Ort (in den Räumen) der Auftragsverarbeiterin zu prüfen oder dies ggf. durch eine kundige Vertreterin der Auftraggeberin prüfen und bescheinigen zu lassen.

Die Dienststelle des Beauftragten für den Datenschutz der EKD hat auf ihrer Website einen Mustervertrag[241] hinterlegt, um den kirchlichen Stellen die datenschutzkonforme Vertragsausgestaltung zu erleichtern.

Gemäß § 30 Abs. 5 DSG-EKD besteht nunmehr die Möglichkeit, Verträge mit Auftragsverarbeiterinnen abzuschließen, auf die die kirchlichen Datenschutzbestimmungen keine Anwendung finden, wenn sich die Inhalte des AV-Vertrages an Artikel 28 DS-GVO orientieren. Voraussetzung ist, dass sich die Auftragsverarbeiterin der kirchlichen Datenschutzaufsicht unterwirft. Die Vertreter der Gliedkirchen der EKD und der Beauftragte für den Datenschutz der EKD haben daher ergänzend zu dem Mustervertrag eine Musterunterwerfungserklärung[242] erstellt.

Ferner legen wir zur Verdeutlichung ein Muster aus der Praxis bei (Anlage D.2.7), das von der Agaplesion gAG freundlicherweise zur Verfügung gestellt wurde.

Praxis-Hinweis:
Bei allen datenschutzrechtlich relevanten Planungen und Vertragsschlüssen ist die jeweils zuständige Datenschutzbeauftragte einzubeziehen.

C.1.1.1.6 Betroffenenrechte

TOM sind auch im Hinblick auf die Rechte der Betroffenen wesentlich, damit sie diese effektiv geltend machen können. Dies entspricht aber nicht nur den Interessen der Betroffenen, sondern auch denen der Verantwortlichen, die so **gleichzeitig ihre Compliance sichern und den Arbeitsaufwand gering halten**. Die Umsetzung der Betroffenenrechte ist **bereits bei der Planung** einer jeden Lösung zu berücksichtigen.

[239] Siehe zu Folgendem § 30 DSG-EKD sowie DS-GVO-Erwägungsgrund 81 und § 62 Abs. 5 BDSG.
[240] Siehe dazu C.1.1.1.8.
[241] https://datenschutz.ekd.de/wp-content/uploads/2018/09/AV-Vertrag_Version-2.1_2018.rtf (zuletzt abgerufen am 12. Juni 2020).
[242] https://datenschutz.ekd.de/wp-content/uploads/2018/05/AV-Annex_Version-1.0_2020.rtf (zuletzt abgerufen am 12. Juni 2020).

Zu den Betroffenenrechten nach Art. 13 – 22 DS-GVO bzw. §§ 16 – 25 DSG-EKD gehören das Recht auf Information,[243] Auskunft,[244] Berichtigung und Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit (dazu sogleich), das Widerspruchsrecht sowie das Recht, keiner Entscheidung aufgrund einer automatisierten Verarbeitung unterworfen zu sein.[245]

C.1.1.1.7 Datenportabilität

Ein Recht der Betroffenen soll aufgrund seiner Implikationen noch besonders hervorgehoben werden. Dieses ist das Recht auf Datenportabiliät (Art. 20 DS-GVO, § 24 DSG-EKD). Dabei handelt es sich um ein interessantes Rechtsinstitut. Dieses gründet nämlich nicht nur auf datenschutzspezifischen Erwägungen, sondern wird auch durch Aspekte des allgemeinen Verbraucherschutzes und sogar des Wettbewerbsrechts bestimmt. Mit seiner Hilfe sollen insbesondere Lock-In-Effekte reduziert; also der Wechsel von einer zu einer anderen Plattform erleichtert werden.

Mit dem Recht auf Datenübertragbarkeit geht die korrespondierende Verpflichtung der verantwortlichen Stelle einher, **die zur Erfüllung des Anspruchs notwendigen technischen Maßnahmen vorzusehen**. Daraus ergeben sich **konkrete technische Anforderungen**.

Die Daten müssen in einem **„strukturierten, gängigen und maschinenlesbaren Format“** übermittelt werden. Allerdings geht die Verpflichtung nicht so weit, dass sie die Gewährleistung der funktionalen Interoperabilität der Daten im Sinne echter Kompatibilität umfasst.[246] Solch eine Kompatibilität wäre im Sinne effektiver Nutzerrechte allerdings wünschenswert. Anbieterinnen der sozialen Wohlfahrt sollten daher bestenfalls darauf achten, dass sie ihren Nutzer*innen ein **Höchstmaß an funktionaler Interoperabilität** ihrer Daten gewähren, so dass die Daten auch im Falle des Wechsels des Dienstes unproblematisch genutzt werden können.

Die Pflicht zur Übermittlung der Daten an Dritte steht unter dem Vorbehalt der technischen Machbarkeit, Art. 20 Abs. 2 DS-GVO, § 24 Abs. 1 S. 2 DSG-EKD. Dabei ist zumindest dem Stand der Technik Rechnung zu tragen.

C.1.1.1.8 Datenschutz-Folgenabschätzung[247] (DSFA)

Wie gezeigt, fordern die Datenschutzgesetze an verschiedensten Stellen eine risikobasierte Herangehensweise. Bei voraussichtlich **hohem Risiko** einer Verarbeitung für die Rechte und Freiheiten natürlicher Personen ist vor **Aufnahme der Datenverarbeitung** eine **Datenschutz-Folgeabschätzung** vorzunehmen (gemäß Art. 35 Abs. 1 DS-GVO bzw. § 34 DSG-EKD und § 67 BDSG). Allerdings eröffnen die in den Vorschriften verwendeten Begriffe einen relativ großen Interpretationsspielraum.

Insbesondere die **Verarbeitung besonders schützenswerter Daten**, insg. Gesundheits- und Krankheitsdaten, kann in Verbindung mit weiteren risikoerhöhenden Faktoren die Durchführung einer Datenschutz-Folgenabschätzung indizieren, vor allem aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie bei **Verwendung neuer Technologien**. Ist eine Datenschutz-Folgenabschätzung durchzuführen, ist sie „vorab“ durchzuführen, bevor es also zu der fraglichen Verarbeitung von Daten kommt.

Ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss, kann mithilfe folgender Screening-Fragen[248] ermittelt werden:

Checkliste Vorprüfung

	Vorprüfung, ob eine DSFA durchzuführen ist	geprüft
1.	Liegt eine „Form der Verarbeitung“ im Sinne des § 34 Abs. 1 Satz 1 DSG-EKD vor?	
2.	Gibt es für die geplante Verarbeitung der personenbezogenen Daten eine Rechtsgrundlage?	
3.	Liegt eine Verarbeitung aus der Liste des BfD EKD nach § 34 Abs. 5 DSG-EKD vor?	
4.	Liegt eine Ausnahme nach § 34 Abs. 7 DSG-EKD vor? (Wurde bereits im Gesetzgebungsverfahren eine DSFA durchgeführt?)	
5.	Handelt es sich bei der Verarbeitung um einen Fall des § 34 Abs. 3 DSG-EKD?	
6.	Liegt nach einer Prognose ein „voraussichtlich hohes Risiko“ für die Rechte natürlicher Personen vor (vgl. § 34 Abs. 1 Satz 1 DSG-EKD)?	

Fig. C.3: Vorprüfung einer DSFA

[243] Auf die Arbeitshilfe zur Umsetzung der Informationspflichten des Beauftragten für Datenschutz der EKD wird hingewiesen: https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-umsetzung-von-informationspflichten/ (zuletzt abgerufen am 11. September 2020).

[244] Der Auskunftsanspruch ist in seinem Umfang durchaus begrenzt. Er ist nicht vergleichbar mit dem Recht auf Akteneinsicht oder Einsicht in die Patientenakte nach § 630g BGB, sondern soll den Berechtigten (nur) einen angemessenen Überblick über die verarbeiteten Daten geben.

[245] Zu den Inhalten der Rechte im Einzelnen siehe etwa Reich: Überblick über Betroffenenrechte nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (neu), VuR 2018, S. 293 ff.

[246] von Lewinsky, in: Wolff/Brink (Hrsg.), BeckOK Datenschutz, Rz. 69 zu Art. 20 DS-GVO; Spiecker gen. Döhmann, Digitale Mobilität: Plattform Governance, in: GRUR 2019, S. 341, 349.

[247] Siehe zu den Einzelheiten einer DSFA ergänzend das ausführliche Kurzpapier #04 des Datenschutzbeauftragten der EKD, https://datenschutz.ekd.de/wp-content/uploads/2018/04/04-Kurzpapier_Datenschutz-Folgenabschaetzung.pdf (zuletzt abgerufen am 18. Juni 2020).

[248] Aus der Handreichung des Datenschutzbeauftragten der EKD, https://datenschutz.ekd.de/wp-content/uploads/2020/04/Handreichung_Datenschutz-folgenabschaetzung.pdf (zuletzt abgerufen am 18. Juni 2020), S. 7. Auf die dortigen umfangreichen Erläuterungen zur Vorprüfung wird verwiesen.

Folgende Risikomatrix kann bei der Erhebung helfen:

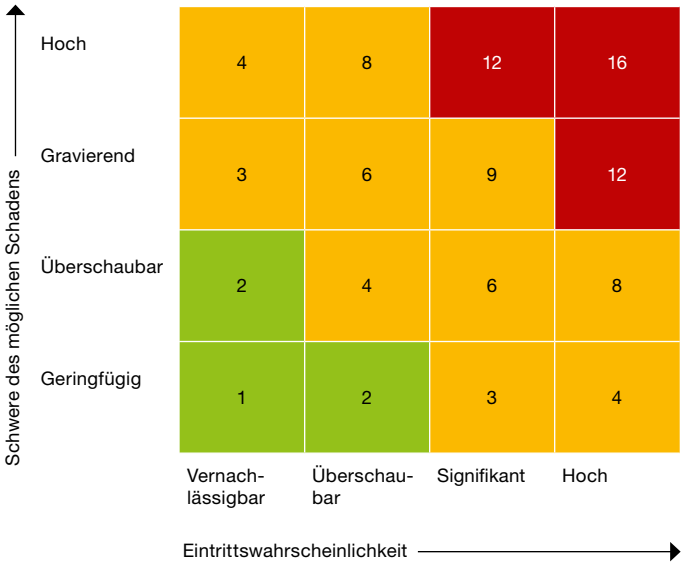


Fig. C.4. Risikomatrix zur DSFA

Ist etwa eine Verarbeitung von Gesundheitsdaten geplant, kann die Wahrscheinlichkeit der Notwendigkeit einer DSFA erhöht sein. Ferner kann zur weiteren Illustration auf die Liste von Verarbeitungsvorgängen, die die Notwendigkeit der Durchführung einer DSFA anzeigen, verwiesen werden.[249] Die Liste orientiert sich an den bereits von anderen Aufsichtsbehörden veröffentlichten Listen zur Datenschutz-Folgenabschätzung.

Der ordnungsgemäße Ablauf einer DSFA kann anhand folgender Checkliste[250] überprüft werden:

Checkliste „Ablauf“

	Ablauf, wie eine DSFA durchgeführt werden kann	erledigt
1.	**Beschreibungsphase:** Systematische Beschreibung der geplanten Verarbeitungsvorgänge sowie Besprechung des Verfahrens der DSFA mit dem Team (vgl. § 34 Abs. 4 Nr. 1 DSG-EKD)	
2.	**Bewertungsphase:** Gegenüberstellung und anschließende Bewertung der a. Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung für die verantwortliche Stelle (vgl. § 34 Abs. 4 Nr. 2 DSG-EKD) b. Risiken für die betroffenen Personen (vgl. § 34 Abs. 4 Nr. 3 DSG-EKD)	
3.	**Maßnahmenphasen:** Festlegung der Abhilfemaßnahmen um ggf. Risiken zu minimieren und deren Umsetzung (vgl. § 34 Abs. 4 Nr. 4 DSG-EKD)	
4.	**Dokumentation**	
5.	**Überprüfung und Fortschreibung**	

Fig. C.5. Verdeutlichung des typischen Ablaufs einer DSFA

Gemäß § 34 Abs. 2 DSG-EKD liegt die Zuständigkeit für die Durchführung der DSFA bei der verantwortlichen Stelle. Je nach konkretem Fall und Größe der Stelle sollte geprüft werden, ob die Bildung einer **Arbeitsgruppe** zur Durchführung der DSFA sinnvoll ist. Die Arbeitsgruppe sollte horizontal wie vertikal heterogen zusammengestellt sein, dh. sowohl die Leitungsebene und Fachebene wie auch Vertreter der IT-Abteilung umfassen. Die oder der örtlich Beauftragte für den Datenschutz hat beratende Funktion und muss einbezogen werden. Bei komplexen DSFA ist eine verantwortliche Person als Leiterin oder Leiter der Arbeitsgruppe zu benennen.

Um die Durchführung zu vereinfachen, empfiehlt sich die Anwendung des PIA-Tools[251], das von der französischen Aufsichtsbehörde entwickelt und veröffentlicht wurde und nunmehr auch in Deutsch zur Verfügung steht. Dieses nimmt einem zwar die Arbeit nicht ab, nimmt einen aber hilfreich an die Hand.

[249] https://datenschutz.ekd.de/infothek-items/liste-von-verarbeitungsvorgaengen-fuer-eine-datenschutz-folgeabschaetzung/ (zuletzt abgerufen am 11. September 2020).

[250] Aus der Handreichung des Datenschutzbeauftragten der EKD, https://datenschutz.ekd.de/wp-content/uploads/2020/04/Handreichung_Datenschutzfolgenabschaetzung.pdf (zuletzt abgerufen am 18. Juni 2020), S. 8. Auf die dortigen umfangreichen Erläuterungen zum Ablauf wird verwiesen.

[251] https://www.cnil.fr/en/privacy-impact-assessment-pia (zuletzt abgerufen am 06. Dezember 2020).

Ist eine DSFA notwendig, ist sie immer nur der Beginn eines permanenten Verbesserungsprozesses (PDCA-Zyklus).

Eine Überprüfung muss insbesondere erfolgen, wenn die die Verarbeitung begleitenden Risiken sich verändert haben. Das kann durch das Auftreten neuer Risiken begründet sein; aber auch schlicht dadurch, dass hinsichtlich der Risiken neue Erkenntnisse vorliegen. Ergibt die Durchführung einer DSFA, dass tatsächlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, muss die verantwortliche Stelle gemäß § 34 Abs. 9 DSG-EKD die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeit konsultieren.

C.1.1.1.9 Weitere relevante Aspekte

C.1.1.1.9.1 Übermittlung von Daten in ein Drittland

Sofern Daten nicht der DS-GVO unterfallende Jurisdiktionen übertragen werden sollen, zB. weil der zu nutzende Website-Host oder die Anbieterin des zu nutzenden Servers im außereuropäischen Ausland sitzen, in welchem die DS-GVO nicht greift, kann dies problematisch sein. Nach den Maßgaben der DS-GVO dürfen personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden, wenn dieses ein **angemessenes Schutzniveau** gewährleistet, was von der Europäischen Kommission festzustellen ist.

Liegt kein derartiger **Angemessenheitsbeschluss** vor, darf eine solche Übermittlung nur erfolgen, wenn die Übermittlerin der personenbezogenen Daten **geeignete Garantien** über die von der Kommission erarbeiteten **Standardvertragsklauseln** gewährleistet und wenn die betroffenen Personen über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügen.

Falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien über Standardvertragsklauseln bestehen, kann die Übermittlung in engen Fällen noch bei Bestehen geeigneter und gelebter **Binding Corporate Rules** erfolgen, was seitens des verantwortlichen Diensteanbieters sorgfältig abzuklären ist.

Hilfreich sind insofern auch die jüngsten Empfehlungen des Europäischen Datenschutzausschuss (EDSA) zu Datentransfers in Drittländer.[252] Zudem hat die Europäische Kommission zuletzt in Reaktion auf die Rechtsprechung des EuGH zum Privacy Shield (siehe nachfolgend) neue Standardvertragsklauseln zur Durchführung eines Konsultationsverfahrens veröffentlicht.[253]

C.1.1.1.9.1.1 Spezialfall USA

Bereits zum zweiten Mal hat der EuGH den Beschluss der EU-Kommission im Hinblick auf die Angemessenheit des US-amerikanischen Datenschutzniveaus für ungültig erachtet. Nachdem er 2015 bereits den Safe-Harbour-Beschluss kippte, hat er mit Entscheidung vom 16. Juli 2020 auch den **Privacy Shield-Beschluss 2016/1250** für ungültig erklärt, da die US-amerikanischen Bedingungen hinter den Forderungen europäischen Rechts zu weit zurückblieben und daher – entgegen dem Angemessenheitsbeschluss der Kommission – eben kein angemessenes Schutzniveau auf US-amerikanischer Seite angenommen werden könne.

Dies insbesondere, weil die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt seien und weil der im „Beschluss angeführte Ombudsmechanismus entgegen den darin von der Kommission getroffenen Feststellungen den betroffenen Personen keinen Rechtsweg zu einem Organ eröffnete, das Garantien böte, die den nach dem Unionsrecht erforderlichen Garantien der Sache nach gleichwertig wären, d.h. Garantien, die sowohl die Unabhängigkeit der durch diesen Mechanismus vorgesehenen Ombudsperson als auch das Bestehen von Normen gewährleisten, die die Ombudsperson dazu ermächtigen, gegenüber den amerikanischen Nachrichtendiensten verbindliche Entscheidungen zu erlassen“[254].

Die Datenübermittlung in die USA ist daher zunächst nur noch unter der Bedingung des Bestehens geeigneter **Standardvertragsklauseln bzw. von Binding Corporate Rules** möglich, die aber sehr selten sein dürften.[255/ 256] Eine „Gnadenfrist“ zur Umstellung existiert nicht. Eine Übermittlung von Daten in die USA (und andere Drittstaaten) kann nur dann über Standardvertragsklauseln hinreichend abgesichert werden, wenn über zusätzliche Maßnahmen das gleiche Datenschutzniveau wie in der EU gewährleistet ist, wobei die Problematik des Zugriffs amerikanischer Geheimdienste auf Server U.S.-amerikanischer Unternehmen fortbesteht. Dies erschwert derzeit die Nutzung und Einbindung von Diensten und Komponenten U.S.-amerikanischer IT-Unternehmen. Eine spezifische Beratung hierzu ist unumgänglich.

C.1.1.1.9.2 Gemeinsame Verantwortlichkeit

Wesentlich für im hier interessierenden Kontext häufig vorkommende **Kooperationen** ist zudem **die Regelung zur gemeinsamen Verantwortlichkeit**, Art. 26 DS-GVO,

[252] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en (zuletzt abgerufen am 07. Dezember 2020).

[253] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries (zuletzt abgerufen am 07. Dezember 2020).

[254] Pressemitteilung des EuGH vom 16. Juli 2020 zur Rechtssache C-311/18 („Schrems II“), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf (zuletzt abgerufen am 03. September 2020).

[255] Siehe im Einzelnen die klare Handreichung des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württembergs, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf (zuletzt abgerufen am 03. September 2020).

[256] Die Verschlüsselung von Daten schafft allein keine Abhilfe. Dadurch können Daten im Rechtssinne allenfalls pseudonymisiert, nicht aber anonymisiert werden.

§ 29 DSG-EKD.[257] Eine gemeinsame Verantwortlichkeit ist vertraglich zu regeln und muss **transparent** sein. Das heißt, dass die **Rollenverteilung** (insbesondere in Bezug auf die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den Betroffenen sowie in Bezug auf Informationspflichten und Betroffenenrechte) so klar erfolgt, dass den Aufsichtsbehörden eine leichte Ausübung ihrer Kontroll- und Überwachungspflichten möglich ist.

Die klare Pflichtenverteilung muss auch für die Betroffenen transparent sein. Entweder wird diesen die getroffene Vereinbarung zur Verfügung gestellt oder deren **wesentlicher Inhalt** in den Datenschutzhinweisen leicht verständlich widergespiegelt.[258] Wesentlich in diesem Sinne ist alles, was zur **effektiven Rechtegeltendmachung erforderlich** sein kann. Dazu muss den Betroffenen gegenüber dargestellt werden, **welche Phasen und Akteure** es im Prozess der Datenverarbeitung gibt, einschließlich der **verschiedenen Verantwortlichkeiten und Zuständigkeiten**. Dabei sind alle tatsächlichen **Verarbeitungsvorgänge** entsprechend abzubilden.

Die gemeinsam Verantwortlichen müssen also sämtliche Strukturen der internen Datenverarbeitung detailliert, wahrheitsgetreu und vollständig offenlegen. Inhaltlich sollte sich die **Vereinbarung zur gemeinsamen Verantwortlichkeit** zudem auch an den Inhalten des Art. 28 Abs. 3 DS-GVO/§ 30 DSG-EKD orientieren. Um den Betroffenen die Wahrnehmung ihrer Rechte zu ermöglichen, sollten folgende Informationen zusätzlich enthalten sein:

- die Beteiligten und deren Sitz bzw. Niederlassung, deren Funktion und Beziehung zu den Betroffenen;
- die von den Beteiligten jeweils verfolgten Zwecke und die jeweiligen Mittel, derer sie sich zur Datenverarbeitung bedienen;
- die verwalteten Datenbestände und deren Orte sowie die Angabe, worauf sich die gemeinsame Verantwortung erstreckt;
- zeitlicher und inhaltlicher Rahmen des Verhältnisses, dem die gemeinsame Verantwortlichkeit zugrunde liegt;
- Informationen darüber, welche der Beteiligten welche Informationspflichten erfüllen und welchen datenschutzrechtlichen Aufgaben nachkommen.

Im Anhang findet sich das Muster für eine Vereinbarung zur gemeinsamen Verantwortlichkeit unter D.2.8. Das Muster geht von einer weitestgehenden inhaltlichen Deckungsgleichheit der Verantwortlichkeit aus. In der Praxis wird häufig eine Anpassung im Sinne einer weiteren Spezifizierung nach den oben genannten Maßgaben erforderlich sein.

C.1.1.1.10 Konsequenzen bei Nichtbeachtung datenschutzrechtlicher Vorgaben

Die Beachtung der oben beschriebenen Aspekte gebietet sich nicht nur aufgrund der besonderen Bedeutung von personenbezogenen Daten in einer digitalisierten Welt. Zusätzliches Gewicht erhalten die Bestimmungen der DS-GVO (und des DSG-EKD) durch die Bußgeldbewährung. Es ist bei Nichtbeachtung mit „abschreckenden“ Geldbußen zu rechnen. Zur Orientierung ist ein Rahmen bis zu 20 Millionen Euro oder – wenn höher – bis zu 4% des Jahresumsatzes vorgegeben.

C.1.1.1.11 Datenschutzmuffel

Das Thema Datenschutz ist für viele nur ärgerlich, da es einen großen Mehraufwand verursacht, ohne dabei unmittelbar spürbare Vorteile zu generieren. Insoweit ist es ein bisschen wie mit den notwendigen Schritten zur Einschränkung der Klima-Krise. Da sie nur langfristig wirken und unmittelbar zunächst nur Nachteile zu begründen scheinen, haben sie bei vielen Bürgern keine Lobby. Den wenigsten Menschen ist langfristiges Planen ein Anliegen. Hinzu tritt, dass die Wirtschaft – durch eine immer stärkere Bindung an kurzfristige Renditen – langfristig orientiertes Denken abzustrafen scheint.

Wenn auch das Klima noch einige Jahre brauchen wird, um auch dem Letzten noch die Notwendigkeit des Umdenkens aufzuzeigen, kann es im Rahmen des Datenschutzes deutlich schneller gehen. Die Behörden sind dabei, die Überprüfungen der Verantwortlichen voranzutreiben. Empfindliche Bußgelder gehören mehr und mehr zur Tagesordnung. Auch im Bereich der Freien Wohlfahrt ist nicht damit zu rechnen, dass sich die Praxis der zurückhaltenden Überprüfung lange aufrechterhalten lässt.

Zu den datenschutzrechtlichen Bußgeldern tritt das Risiko der **persönlichen Haftung** der Verantwortlichen nach § 130 OWIG, „Inhaberhaftung“. Hat es die aufsichtspflichtige Person versäumt, notwendige Aufsichtsmaßnahmen zur Verhinderung der Zuwiderhandlung gegen betriebsbezogene Pflichten zum Datenschutz einzurichten, kann dies eine Ordnungswidrigkeit im Sinne des § 130 OWiG sein und zu einem empfindlichen Bußgeld führen. Neben den gesetzlichen Pönalisierungen ist aber auch der drohende Reputationsschaden umso relevanter, je stärker das Bewusstsein der Bürger den Schutz der eigenen Daten umfasst.

[257] Auf den Abschluss haben die gemeinsam Verantwortlichen einen wechselseitigen Anspruch, und zwar bereits aufgrund § 26 DS-GVO/§ 29 DSG-EKD, die als unmittelbare Anspruchsgrundlage gelesen werden können. Zur Abgrenzung der (gemeinsam) Verantwortlichen von den Auftragsverarbeiterinnen siehe die Guidelines 07/2020 on the concepts of controller and processor in the GDPR (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf – zuletzt abgerufen am 25. September 2020).

[258] Strittig ist, ob erst auf Aufforderung oder bereits unangefragt. Im Sinne des umfassenden Betroffenenschutzes sollte die Information bereits ohne Anfrage erfolgen.

Auch Datenschutzmuffel sollten sich daher die folgenden Fragen stellen:

- Welche Anforderungen aus der Datenschutz-Grundverordnung (DSGVO) wurden bislang nicht umgesetzt? Was wurde vernachlässigt?
- Welche Hinweise haben die Mitarbeitenden bislang nicht umgesetzt und welche Folgen kann das Ignorieren nach sich ziehen?
- Bei welchen Verarbeitungen besteht ein erhöhtes Risiko für einen Datenschutzverstoß?
- Wo wird sorglos mit personenbezogenen Daten umgegangen?
- Welches Image hat die Einrichtung in der Öffentlichkeit und was setzt sie mit einem zu gering ausgeprägten Datenschutz aufs Spiel?

C.1.1.2 Checkliste DS-GVO (allgemein)

- Wird die Umsetzung des Datenschutzes unabhängig (z.B. vom DSB) geprüft werden, also nicht vom Projektteam selbst?
- Ist die Datenschutzbeauftragte in die Planung eines Vorhabens/einer Lösung von Anfang an einbezogen?
- Ist ein an den Grundsätzen der Datenminimierung, Transparenz und an Betroffenenrechten ausgerichtetes angemessenes Datenschutzkonzept und –management vorhanden? Wird dieses innerhalb eines PDCA-Zyklus laufend aktualisiert?
- Besteht Klarheit über Art, Zweck und Umfang der zu erhebenden personenbezogenen Daten?
- Besteht Klarheit über den Schutzbedarf der zu erhebenden Daten, insbesondere Einwilligungserfordernissen, und ist das Schutzkonzept auf entsprechendem Niveau?
- Ist eine Datenschutz-Folgenabschätzung indiziert und ggf. durchgeführt?
- Ist ein transparentes Verzeichnis der Verarbeitungstätigkeiten erstellt worden, das sämtliche Vorgänge erfasst, bei denen personenbezogene Daten verarbeitet werden?
- Ist zu jeder Verarbeitungstätigkeit festgelegt, aus welchem Grund die Daten welcher Personen verarbeitet werden und zu welcher Kategorie die Daten gehören (zB. Gesundheitsdaten)?
- Ist ein Verzeichnis zu den möglichen Empfängern der Daten angelegt?
- Sind alle geeigneten und notwendigen technischen und organisatorischen Maßnahmen (TOM) zum Datenschutz getroffen und umgesetzt?
- Ist Privacy by Default und by Design sichergestellt?
- Ist die effektive Umsetzung der Rechte der Betroffenen gesichert?
- Ist insbesondere die Datenportabilität gesichert?
- Sind insbesondere Löschfristen festgelegt? Werden sie hinsichtlich ihrer Angemessenheit regelmäßig überprüft und werden sie auf ihre Einhaltung überwacht?
- Ist die Einholung der aktiven, informierten und freiwilligen Einwilligung in den angezeigten Fällen gesichert und für jeden Einzelfall hinreichend dokumentiert?
- Sind in Auftragsverarbeitungsverträgen die Haftung im Innenverhältnis geregelt und mit Freistellungsklauseln abgesichert)?
- Sind die Sicherstellung der Einhaltung des Datenschutzes in den Auftragsverarbeitungsverträgen garantiert und ein Weisungsrecht eingeräumt?
- Sind die Auftragsverarbeiterinnen zertifiziert (etwa nach ISO/IEC 27001)?
- Sind besondere Vorkehrungen getroffen worden, sofern personenbezogene Daten in ein Drittland übermittelt werden bzw. ist geprüft, ob die Übermittlung zulässig ist?
- Ist eine ggf. bestehende gemeinsame Verantwortlichkeit erkannt und transparent und angemessen zwischen den Verantwortlichen geregelt?
- Ist ein Zugriffskonzept erstellt und werden Zugriffe auf Daten dokumentiert?
- Besteht eine Handlungsanweisung/ein Prozess für den Fall eines Datenschutzvorfalls?
- Ist (bei Vorliegen der Voraussetzungen) eine Datenschutzbeauftragte benannt?
- Werden die Mitarbeiter*innen regelmäßig geschult und werden regelmäßig Audits durchgeführt?
- Sind die Mitarbeiter*innen insbesondere zur Verschwiegenheit hinsichtlich der aus der Verarbeitung personenbezogener Daten folgenden Kenntnisse informiert und – auch über das Dienstverhältnis hinaus – verpflichtet worden?

C.1.2 IT-SICHERHEIT

Die IT-Sicherheit geht mit Gefährdungen für die in Anspruch genommene technische Infrastruktur unter den Aspekten von Verlässlichkeit, Authentizität und Zugriffsmöglichkeiten um.

Anmerkung:
Zur Verdeutlichung sei angemerkt, dass es sich hier nicht etwa um eine Dopplung der bereits unter der Maßgabe des Datenschutzes diskutierten technischen Maßnahmen handelt. Vielmehr geht es der IT-Sicherheit darum, generell die Einrichtung an sich und deren – auch nicht personenbezogene – Daten sowie Infrastruktur zu schützen.

Als Kernanliegen sind die Herstellung von **Safety**, der immanenten Sicherstellung des Funktionierens und der Verfügbarkeit eines Systems sowie die Herstellung von **Security**, dem Schutz der IT-Systeme vor Angreifern oder vor Sabotage, zu benennen.

Das erst 2015 kodifizierte Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (IT-SichG)[259], im Wesentlichen also das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)[260] ist bisher weniger von

[259] BGBl. I 2015, 1324. Gesetz vom 17. Juli 2015, BGBl. I S. 1324 (Nr. 31); zuletzt geändert durch Art. 5 Abs. 8 des Gesetzes vom 18. Juli 2016, BGBl. I S. 1666

[260] Artikel 1 des Gesetzes vom 14. August 2009 BGBl. I S. 2821 (Nr. 54); zuletzt geändert durch Art. 73 der Verordnung vom 19. Juni 2020 BGBl. I S. 1328.

Bedeutung. Es findet lediglich auf sogenannte kritische Infrastrukturen Anwendung (siehe dazu den folgenden Exkurs). Sein risikobasierter Ansatz hat aber allgemeine Bedeutung. Er fließt auch ein in die nach § 1 Abs. 3 S. 1 ITSVO-EKD[261] zu beachtenden Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz[262], die nur durch vergleichbare Sicherheitsstandards ersetzt werden dürfen, § 1 Abs. 3 S. 2 ITSVO-EKD.

Die Evangelische Kirche in Deutschland stellt Muster-IT-Sicherheitskonzepte[263] nach dieser Maßgabe zur Verfügung.

Kürzlich hat das Bundesinnenministerium allerdings den – zwischenzeitlich dritten – **Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme** (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)[264] vorgelegt. Mit diesem soll das BSIG reformiert und über kritische Infrastrukturen von wichtiger öffentlicher Bedeutung hinaus auch auf viele Unternehmen der Privatwirtschaft und der Verbraucher*innenmärkte erweitert werden. Der Gesetzesentwurf plant zudem Änderungen des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) sowie des Zehnten Sozialgesetzbuches (SGB X). Hier bleibt zu beobachten, ob und inwieweit sich hieraus künftig neue Anforderungen ua. auch im Hinblick bisher nicht im Fokus des BSIG liegender Infrastrukturen ergeben.

Kürzlich hat das Bundesinnenministerium allerdings den – zwischenzeitlich dritten – Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) vorgelegt. Mit diesem soll das BSIG reformiert und über kritische Infrastrukturen von wichtiger öffentlicher Bedeutung hinaus auch auf viele Unternehmen der Privatwirtschaft und der Verbraucher*innenmärkte erweitert werden. Der Gesetzesentwurf plant zudem Änderungen des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) sowie des Zehnten Sozialgesetzbuches (SGB X). Hier bleibt zu beobachten, ob und inwieweit sich hieraus künftig neue Anforderungen ua. auch im Hinblick bisher nicht im Fokus des BSIG liegender Infrastrukturen ergeben.

C.1.2.1 Exkurs: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Wie bereits erwähnt, verfolgt der Gesetzgeber mit dem BSIG das Ziel, so genannte kritische Infrastrukturen sicher zu machen, in dem es sie zur Einhaltung geeigneter organisatorischer und technischer Anforderungen verpflichtet. Kritische Infrastrukturen im hier interessierenden Sinne des Gesetzes sind medizinische Leistungserbringer, die hervorgehoben und unmittelbar der Sicherung des Allgemeinwohls dienen.)[265] Dabei handelt es sich um Krankenhäuser, Hersteller von Medizinprodukten, Arzneimittelhersteller und Apotheken. Sie unterfallen aber dem Gesetz nur, sofern ihr Tätigkeitsumfang einen bestimmten Schwellenwert überschreitet, sie also innerhalb der jeweiligen Branche eine erhebliche Größe darstellen.)[266]

Für Krankenhäuser wird beispielsweise eine vollstationäre Fallzahl von 30.000 p.a. vorausgesetzt (wie nach § 21 Abs. 2 KHEntgG zu ermitteln).[267] Ist der jeweilige Schwellenwert überschritten, so sind die Vorgaben des BSIG und der BSI-Kritis-VO ohne weitere Verzögerung umzusetzen. Bei Überschreitung des Schwellenwerts gilt die Verpflichtung nach BSIG also vom Folgetag (!) ab, und zwar ohne Umsetzungsfrist. Daher ist jedenfalls auch bei nur knapper Unterschreitung eine Umsetzung vorzubereiten.

Inhaltlich heißt das gemäß §§ 8ff. BSIG insbesondere, dass die Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse bei umfassender Einhaltung des jeweiligen Stands der Technik sowie der Informationsaustausch zwischen der Betreiberin der Einrichtung und dem Bundesamt für Sicherheit in der Informationstechnik sicherzustellen sind.[268]

Damit dynamisiert das Gesetz seine Anforderungen, deren Einhaltung mindestens alle zwei gegenüber dem Bundesamt für Sicherheit in der Informationstechnik

[261] https://www.kirchenrecht-ekd.de/document/32147 (zuletzt abgerufen am 04. Juni 2020)
[262] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html (zuletzt abgerufen am 04. Juni 2020)
[263] https://datenschutz.ekd.de/infothek-items/rat-der-ekd-erlaesst-it-sicherheitsverordnung/ (zuletzt abgerufen am 04. Juni 2020)
[264] https://intrapol.org/2020/11/21/it-sig-2-0-dritter-referentenentwurf-mit-stand-vom-19-11-2020-veroeffentlicht/ (zuletzt abgerufen am 05. Dezember 2020); siehe auch https://www.bundesregierung.de/breg-de/aktuelles/it-sicherheit-1829080 (zuletzt abgerufen am 16. Dezember 2020).
[265] Daneben zählen auch bestimmte Anlagen aus den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen sowie Transport und Verkehr zur kritischen Infrastruktur.
[266] Siehe zu den Schwellenwerten den Anhang 5 (Teil 3) zur BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Art. 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903).
[267] Räumlich getrennte Standorte können als eine Anlage im Sinne des Gesetzes zu verstehen sein, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten als Einheit anzusehen sind (siehe Jorzig/Sarangi, Digitalisierung im Gesundheitswesen, Berlin 2020, S. 86). In ihrer Umsetzungsempfehlung aus dem Jahre 2017 geht die Deutsche Krankenhausgesellschaft davon aus, dass 5 – 10% der Krankenhäuser in Deutschland pflichtig sind (a.a.O, S. 85). Womöglich wird der Wert aber in naher Zukunft abgesenkt.
[268] Unmittelbar umzusetzen sind: Meldung der Einrichtung gegenüber dem Bundesamt für Sicherheit in der Informationstechnik; Einrichtung einer Kontaktstelle; unverzügliche Meldungen von erheblichen Störungen an das Bundesamt; sofortige Umsetzung von Maßnahmen zur Vermeidung von Störungen, der Verfügbarkeit, Integrität, Authentizität sowie der Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse; Bestandsaufnahme der bestehenden IT-Strukturen mitsamt einer entsprechenden Risikoeinschätzung; Bestimmung und Zuordnung von relevanten Zuständigkeiten und Verantwortlichkeiten; transparente Einrichtung von effektiven Informationswegen.

nachzuweisen sind. Außergewöhnliche Störungen sind zwingend sofort zu melden. Werden die Pflichten nach dem BSIG nicht eingehalten, können erhebliche Sanktionen drohen.

Die **IT-Grundschutz-Methodik** zeichnet sich durch einen **ganzheitlichen Ansatz** aus. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird ein Sicherheitsniveau erreicht, das für den **jeweiligen Schutzbedarf angemessen und ausreichend** ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Anforderungen **des IT-Grundschutz-Kompendiums** nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern erläutern an vielen Stellen, wie ein höheres Sicherheitslevel erreichbar ist.[269]

Wer sich mit dem BSI-Grundschutz beschäftigt, ist mitunter von der schieren Fülle von Informationen und Anforderungen überwältigt. War der Grundschutzkatalog ursprünglich sehr umfangreich (rd. 5000 Seiten), ist die Darstellung vor wenigen Jahren deutlich vereinfacht worden. Heute erlauben die sogenannten 200er-Dokumente (BSIS-Standard 200-1 bis 200-3) eine leichtere und schnelle Annäherung an die allgemeinen Anforderungen, die an ein Managementsystem für Informationssicherheit (ISMS) zu stellen sind. Nach dem Einstieg über die allgemeinen Anforderungen nach BSI-Standard 200-1 kann anhand des BSI-Standard 200-2 zur IT-Grundschutz-Methodik ein solides ISMS aufgebaut werden.[270] Dabei steht mit der Standard-Absicherung die **bewährte IT-Grundschutz-Vorgehensweise** zur Verfügung. Sie wird vorbereitet durch die Basis-Absicherung, die eine grundlegende Erst-Absicherung in der Breite ermöglicht, sowie durch die Kern-Absicherung, die sich dem Schutz der besonders schützenswerten Daten einer Institution widmet. Der BSI-Standard 200-3 zum Risikomanagement enthält alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.

Der Einstieg in das IT-Grundschutz-Kompendium, das seit 2018 jährlich in einer aktualisierten Edition erscheint, ist über das Inhaltsverzeichnis themenbezogen sehr gut möglich. Das Kompendium enthält die IT-Grundschutz-Bausteine, in denen jeweils Gefährdungen und Sicherheitsanforderungen für ein Thema der Informationssicherheit übersichtlich auf rund zehn Seiten erläutert werden. Mit den Bausteinen erhalten Anwender*innen konkrete Empfehlungen zur Umsetzung der IT-Grundschutz-Methodik. Die IT-Grundschutz-Bausteine sind in Prozess- und System-Bausteine aufgeteilt und in insgesamt zehn Schichten untergliedert.

Die einzelnen Kapitel des Kompendiums folgen dabei immer dem gleichen Prinzip. Die zentrale Rolle des IT-Grundschutz-Kompendiums spielen die einzelnen Bausteine, deren Aufbau jeweils gleich ist. Zunächst wird jeweils das betrachtete Zielobjekt allgemein beschrieben. Die folgende Zielsetzung formuliert, welcher Sicherheitsgewinn mit der Umsetzung des IT-Grundschutz-Bausteins erreicht werden soll. Danach folgt das Kapitel Abgrenzung und Modellierung. Hier erfolgt eine Abgrenzung der Aspekte, die nicht im jeweiligen Baustein behandelt werden, sowie Verweise auf andere Bausteine, die diese Aspekte aufgreifen. Neben der Abgrenzung werden in diesem Kapitel auch Modellierungshinweise für den konkreten Baustein aufgeführt. Im Anschluss werden spezifische Gefährdungen dargelegt. Sie erheben keinen Anspruch auf Vollständigkeit, liefern aber ein Bild über die Sicherheitsprobleme, die ohne Gegenmaßnahmen beim Einsatz der betrachteten Komponente, Vorgehensweise oder des IT-Systems entstehen können. Die Erläuterung der möglichen Risiken kann die Anwendenden noch stärker für das Thema sensibilisieren. Bei der Risikoanalyse, die jedem Baustein zugrunde liegt, wurden diese spezifischen Gefährdungen aus den elementaren Gefährdungen abgeleitet.

Auf die spezifischen Gefährdungen folgen in der Bausteinstruktur die Anforderungen. Diese sind in drei Kategorien gegliedert: Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen müssen vorrangig umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Gemeinsam mit den Basis-Anforderungen erfüllen die Standard-Anforderungen den Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu bieten die Bausteine des IT-Grundschutz-Kompendiums auch Vorschläge für Anforderungen bei erhöhtem Schutzbedarf.

Vertiefende Anmerkung zum Verhältnis des IT-Grundschutzes zum allgemeinen Datenschutz:

Die Umsetzung der durch den IT-Grundschutz implizierten Maßnahmen ist für den Datenschutz essenziell. Gleichwohl unterscheiden sich die Zielrichtungen beider ganz erheblich. Nimmt der IT-Grundschutz die Informationssicherheit in den Fokus und zielt also auf den Schutz der verarbeitenden Institution und deren Infrastruktur, nimmt der Datenschutz die Perspektive der Betroffenen und deren Grundrechtsausübung ein. Aus dieser Blickrichtung ist die Beeinträchtigung relevant, die den Betroffenen aufgrund der Datenverarbeitung der betreffenden Institution droht.

Die Gewährleistungsziele des Datenschutzes erfordern daher im Vergleich zu den Schutzzielen der IT-Sicherheit das erweiterte Verständnis für die Risiken, die durch die Aktivitäten der betreffenden Organisation – innerhalb wie auch außerhalb ihrer Geschäftsprozesse – für die Rechte und Freiheiten natürlicher Personen begründet werden. Die Umsetzung des IT-Grundschutzes ist daher aus datenschutzrechtlicher Sicht zwar unbedingte Voraussetzung eines effektiven Datenschutzmanagements, nicht aber bereits dessen vollständige Erfüllung.

[269] Der IT-Grundschutz kann insoweit als eine praxisorientierte Herangehensweise angesehen werden, die Anforderungen der ISO/IEC 27001 und deren Erweiterung nach ISO/IEC 27701 umzusetzen.

[270] Siehe dazu insbesondere den Leitfaden des BSI zur Basis-Absicherung nach IT-Grundschutz (https://wwn-bayern.de/fileadmin/user_upload/docs/pdf/Leitfaden_zur_IT-Basis-Absicherung.pdf - zuletzt abgerufen am 26. Juni 2020).

In geeigneten Fällen ist zudem die Technische Richtlinie des BSI für Digitale Gesundheitsanwendungen (TR-03161)[271] zu beachten, die sich unmittelbar an Hersteller von digitalen Gesundheitsanwendungen für mobile Endgeräte (vgl. § 33a SGB V) wendet. Damit erschöpft sich das mögliche Anwendungsfeld der Richtlinie aber nicht. Alle mobilen Anwendungen, die sensible Daten verarbeiten, wozu natürlich auch das bloße Speichern gehört, sollten die Vorgaben der Richtlinie als Mindestanforderungen erfüllen. Denn ein kompromittiertes Smartphone kann über das Leben eines Menschen ungewollt Erhebliches preisgeben. Während beispielsweise bei Datenabfluss im Bereich des Finanzwesens eine Kompensation grundsätzlich möglich ist, etwa durch Erstattung betrügerisch abgeflossener Beträge, ist die Vertraulichkeit von unwillentlich zugänglich gemachten Gesundheitsdaten auf immer verloren. Entwickler von Gesundheitsanwendungen sollten hierauf aus mehreren Gründen besonders Rücksicht nehmen. Aus ethischen Gründen, weil die Verletzung der Integrität der Gesundheitsdaten die Gesundheit der betroffenen Person beeinträchtigen kann. Aber auch aus eigenem wirtschaftlichen Interesse. Denn letztlich schadet ein schwaches Sicherheitsprofil einer App auch deren Akzeptanz und hindert damit ihre Marktdurchdringung.

Technische Systeme lassen sich grundsätzlich angemessen absichern. Dazu ist die Eintrittswahrscheinlichkeit der umfassend zu definierenden Risiken und das ihr entsprechende Reagieren mit technischen und organisatorischen Maßnahmen nach dem aktuellen Stand der Technik maßgeblich. Da meist der Mensch die wesentliche Schwachstelle ist, versucht ein effektives IT-Management, die Einflussmöglichkeiten des Menschen weitestgehend zu beschränken bzw. zu flankieren. So ist das beliebteste Passwort der Deutschen wohl immer noch 123456.[272]

Bei der Planung des Systems ist besonders zu beachten, dass vorgegebene Schnittstellen und Formate alle Beteiligten in Zukunft binden. **Pfadabhängigkeiten** sind dadurch womöglich im wahrsten Sinne des Wortes „vorprogrammiert“. Derlei Problemen kann immerhin teilweise durch eine strikte System-Hierarchie begegnet werden, indem das System in unterschiedliche Hierarchie-Ebenen unterteilt wird, um so modulartige Änderungen besser zu ermöglichen.

Immer wieder kommt es in der Praxis dazu, dass bestehende Systeme oder deren Komponenten den stattfindenden Veränderungen nicht angepasst werden, weil sie in bisherigen Versionen als sicher galten. Dieser Trugschluss kann ein System erheblich schwächen, da die laufenden Veränderungen mitunter Möglichkeiten eröffnen, mit denen zuzeiten der Vorversionen nicht gerechnet werden musste.

C.1.3 ERSTELLUNG/ BESTELLUNG EINER DIGITALEN LÖSUNG

C.1.3.1 Projektmanagement

Die Einführung einer neuen digitalen Anwendung stellt häufig eine besondere Herausforderung dar. Die Prozesse zur Unterstützung der Anwendung sind mitunter noch nicht oder nicht vollständig etabliert oder es müssen bereits etablierte Prozesse mit dem Einsatz der Software in Einklang gebracht werden. Sofern eine Prozessveränderung oder -Erweiterung nicht ohnehin geplant ist, empfiehlt es sich freilich, die Eigenschaften der Software und ihre Einführung möglichst nah an der bisherigen Praxis zu orientieren. Aber auch wenn das gelingt, ist die erfolgreiche Einführung umfassenderer digitaler Lösungen voraussetzungsreich. Insoweit empfiehlt es sich in vielen Fällen, sie **als Projekt zu organisieren**. Eine gewisse Orientierung kann dabei der Leitfaden kirchliches Projektmanagement bieten.[273]

C.1.3.2 Die Auswahl von Lösungen anhand der Testbarkeit der Sicherheit

Wie oben gesehen, muss die ausgewählte Lösung nicht nur **effektiv** und **ansprechend** sein, sondern auch **hinreichend sicher**. Diese Sicherheit kann unterschiedlich gewährleistet werden – abhängig von ihrer Quelle.

Am einfachsten ist dies bei einer **Eigenentwicklung**. Bei ihnen lässt sich die Sicherheit der Lösung bereits bei ihrer Entwicklung **genuin einplanen**. Sicherheitsspezifische Vorgaben bzgl. Konzeption, Umsetzung und Betrieb werden dabei teilweise mit der Ausschreibung veröffentlicht, teilweise aber auch erst im Rahmen des Projekts erarbeitet. Letzteres führt dazu, dass Webanwendungen und Apps immer wieder mit Schwachstellen behaftet sind, die für unterschiedliche Angriffe ausgenutzt werden. Vor diesem Hintergrund empfiehlt es sich, bei der Eigenprogrammierung vor allem **auf Zweierlei zu achten**:

Zum einen ist die genuine Einplanung hinreichender Sicherheit nur dann möglich, wenn auch die entscheidende **Sensibilität** auf Seiten der Entwickler vorhanden ist. Diese ist mitunter stark abhängig vom Anwendungsfeld, das für die Entwickler neu sein kann. Für den **anwendungsfachlichen Hintergrund** zu sorgen, kann insoweit eine wesentliche Aufgabe der auftraggebenden Stelle sein. Dies ist umso erforderlicher, je geringer die Erfahrung der Entwickler im betreffenden Anwendungsfeld ist.

[271] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161.html (zuletzt abgerufen am 04. Juni 2020)

[272] https://hpi.de/news/jahrgaenge/2019/die-beliebtesten-deutschen-passwoerter-2019.html (zuletzt abgerufen am 03. Juni 2020).

[273] https://www.kirchenfinanzen.de/download/Leitfaden_kirchliches_Projektmanagement.pdf

Zum anderen empfiehlt es sich, den **„Industriestandard" der sicheren Softwareentwicklung** zu wahren. Dabei helfen etwa die BSI-Leitfäden zur Entwicklung sicherer Webanwendungen[274], der Baustein „Software-Entwicklung"[275] aus dem BSI-Grundschutz-Kompendium, Kategorie „Konzeption und Vorgehensweisen". Hilfreiche kostenlose Dokumente stellen ferner die Anleitungen des Open Web Application Security Project® (OWASP) dar, darunter insbesondere:

- OWASP Application Security Verification Standard[276]
- OWASP Mobile Security Testing Guide[277]
- OWASP Mobile Top 10[278]
- OWASP Top Ten[279]
- OWASP Web Security Testing Guide[280]
- OWASP API Security Project[281]
- OWASP Automated Threats to Web Applications[282]

Sofern einschlägig sollte die Beachtung dieser Standards nach Möglichkeit **vertraglich vereinbart** werden. Unterstützend kann der Praxisleitfaden Softwareprüfung und -freigabe der EKD[283] herangezogen werden, der mit guten Checklisten aufwartet.

Über die Einhaltung der beschriebenen Standards hinausgehend, empfehlen sich abschließende **Sicherheits-Audits und Penetrationstests**, die ggf. bei darauf spezialisierten Unternehmen in Auftrag gegeben werden können.

Sofern Open-Source-Software eingesetzt werden soll, empfiehlt sich ebenfalls der Einsatz von **Sicherheits-Audits und Penetrationstests**. Dies gilt genauso auch bei quellcode-geschützter Dritt-Software, die aber deutlich schwieriger zu prüfen ist.

C.1.3.3 Weitere wesentliche Aspekte bei Planung/Einkauf

Die Entscheidung, Software **inhouse** zu entwickeln, führt nicht unbedingt zu einer Kosten- und Aufwandsersparnis. Das Gegenteil kann der Fall sein, da die erfolgreiche Entwicklung von Software ihre effektive Organisation voraussetzt. Sofern die Entscheidung auf einen externen Dienstleister fällt, sollte dieser bestenfalls umfassende Kenntnisse im einschlägigen Bereich nachweisen können.[284] Der Auftragserteilung sollte eine möglichst **präzise Beschreibung** der an das Arbeitsergebnis zu stellenden Anforderungen zugrunde liegen.

Wie oben gezeigt, ist dabei insbesondere der durch Art. 25 DS-GVO bzw. § 28 DSG-EKD eingeforderte Datenschutz durch Technikgestaltung („by design") und datenschutzfreundliche Voreinstellungen („by default") sicherzustellen, und zwar von Anfang an, da **nachträgliche Änderungen** häufig aufwendig und teuer sind.

Wird ein Dritter mit der Programmierung einer Anwendung beauftragt, handelt es sich um einen Software-Erstellungsvertrag. Der Vertrag muss sicherstellen, dass die Programmierung ggf. auch die eventuellen **Vorgaben** der Store-Betreiberin einhält und für ggf. eingebundene Inhalte Dritter (insbesondere Texte, Audio, Video) die **erforderlichen Rechte** zum Vertrieb über die App vorliegen, sofern der Anbieter diese Inhalte nicht selbst bereitstellt. Geschieht dies nicht, ist der Vertrieb der App gefährdet. Ferner können im Einzelfall Vorgaben des Vergaberechts zu beachten sein.

Auch der Einsatz **von Open-Source-Software** kann **weitreichende rechtliche Konsequenzen** haben. So verpflichten einige Lizenzen die Lizenznehmerin bei veröffentlichten Veränderungen dazu, den Quellcode der Veränderungen oder Ergänzungen unter der ursprünglichen Lizenz zugänglich zu machen („**Copyleft**"). Dann muss also die Anbieterin zwingend den Programmcode der proprietären App **offenlegen**. Problematisch kann dies insbesondere dann sein, wenn zusätzlich zu OSS-Komponenten proprietäre Komponenten von Drittanbietern verwendet werden und deren Bedingungen eine Offenlegung nicht zulassen. Der Vorteil von Open-Source-Lizenzen liegt gleichwohl häufig in der Kostenreduktion.

C.1.3.4 Vergaberechtliches

In vergaberechtlicher Hinsicht ist festzuhalten, dass sich aufgrund der Komplexität von Software-Projekten die **Verhandlungsvergabe** (Verhandlungsverfahren ohne Teilnahmewettbewerb) häufig anbieten wird. Gegenüber der öffentlichen und der beschränkten Ausschreibung bietet die Verhandlungsvergabe den Vorteil einer geringeren formellen Strenge und einer erhöhten (Nach)Steuerbarkeit des Vergabeprozesses. Gemäß § 8 Abs. 4 Ziff. 3 UVgO bietet sich die Verhandlungsvergabe in den Fällen an, in denen die Leistung aus objektiven Gründen nicht eindeutig und erschöpfend beschreibbar ist,[285] insbesondere, wenn zu ihrer Festlegung ein enger und fortlaufender Austausch zwischen Auftraggeberin und Auftragnehmerin erforderlich ist. Gemäß § 8 Abs.

[274] https://www.bsi.bund.de/DE/Publikationen/Studien/Webanwendungen/index_htm.html (zuletzt abgerufen am 26. Juni 2020).
[275] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/CON/CON_8_Software-Entwicklung.html (zuletzt abgerufen am 26. Juni 2020).
[276] https://owasp.org/www-project-application-security-verification-standard/ (zuletzt abgerufen am 26. Juni 2020).
[277] https://owasp.org/www-project-mobile-security-testing-guide/ (zuletzt abgerufen am 26. Juni 2020).
[278] https://owasp.org/www-project-mobile-top-10/ (zuletzt abgerufen am 26. Juni 2020).
[279] https://owasp.org/www-project-top-ten/ (zuletzt abgerufen am 26. Juni 2020).
[280] https://owasp.org/www-project-web-security-testing-guide/ (zuletzt abgerufen am 26. Juni 2020).
[281] https://owasp.org/www-project-api-security/ (zuletzt abgerufen am 26. Juni 2020).
[282] https://owasp.org/www-project-automated-threats-to-web-applications/ (zuletzt abgerufen am 26. Juni 2020).
[283] https://datenschutz.ekd.de/2017/08/23/praxisleitfaden-softwarepruefung-und-freigabe-ist-online/ (zuletzt abgerufen am 28. Juli 2020).
[284] Ergänzend sei zur Auswahl hingewiesen auf den Praxisleitfaden Softwareprüfung und -freigabe der EKD, der ein allgemeines und standardisiertes Verfahren zur Prüfung und zur Freigabe von Software beschreibt: https://datenschutz.ekd.de/2017/08/23/praxisleitfaden-softwarepruefung-und-freigabe-ist-online/ (zuletzt abgerufen am 10. September 2020).
[285] Wenn also „die Leistung nach Art und Umfang, insbesondere ihre technischen Anforderungen, vor der Vergabe nicht so eindeutig und erschöpfend beschrieben werden kann, dass hinreichend vergleichbare Angebote erwartet werden können".

4 Ziff. 10 UVgO kann die Verhandlungsvergabe auch dann das richtige Verfahren sein, wenn nur ein Unternehmen zur Leistungserbringung in Betracht kommt, etwa deshalb, weil es als einziges über das notwendige Sonderwissen verfügt. Die Leistung muss dazu mit außergewöhnlichen Schwierigkeiten oder Eigenarten verbunden sein. Eine entsprechende Behauptung genügt nicht. Die Umstände sind vielmehr aufgrund angemessener Markterkundung zu ermitteln und zu dokumentieren.

Die Entscheidung über die Vergabeart ist jedenfalls – und ganz besonders im Rahmen der Verhandlungsvergabe – **vollständig, ausführlich, nachvollziehbar und einzelfallbezogen** zu begründen.

C.1.3.5 IT-Vertragsgestaltung

C.1.3.5.1 EVB-IT

Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT) sind ergänzende Vertragsbedingungen für die Beschaffung von Leistungen im Bereich der Informationstechnik. Sie wurden ursprünglich vom Kooperationsausschuss Automatisierte Datenverarbeitung Bund/ Länder/ Kommunaler Bereich (mittlerweile aufgegangen im IT-Planungsrat) in Abstimmung mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) entworfen. Sie bieten eine gute Grundlage für Beschaffungsverträge. Die Vorlagen[286] sind sehr umfangreich und umfassen auch komplexe Systemverträge. Die EVB-IT haben die BVB (Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen) im Wesentlichen abgelöst. Es existieren nur noch zwei[287] BVB (zu Miete und Planung).

Die EVB-IT sind ergänzende Vertragsbedingungen (im Sinne von § 9 Abs. 1 S. 3 VOL/A) und haben **keinen Gesetzescharakter**. Sie gelten nur, wenn sie **vereinbart** sind und können zwingende gesetzliche Regeln – beispielsweise des BGB – **nicht verdrängen**. Insbesondere unterliegen sie der Angemessenheitsprüfung nach §§ 307 ff. BGB. In einem Individualvertrag wäre die Gestaltungsmöglichkeit also größer – die EVB-IT können aber individualvertraglich entsprechend angepasst werden. Weder in der VGV noch in der UVgO werden sie erwähnt. Sie gehören insoweit zu den **Vertragsunterlagen**. Die EVB-IT können durch Vereinbarung Vorrang vor der VOL/B haben.

Das typische Vertragskonvolut bei Einbeziehung der EVB-IT umfasst daher das Vertragsformular, die Leistungsbeschreibung sowie die EVB-IT AGB und die VOL/B.

C.1.3.5.1.1 Übersicht EVB-IT

Vertragstyp	Charakter/Inhalt
EVB-IT Überlassung Typ A	Kaufvertrag über Standardsoftware
EVB-IT Überlassung Typ B	Mietähnlicher Vertrag über Standardsoftware
EVB-IT Kauf	Kaufvertrag über Hardware
EVB-IT Instandhaltung	Werkvertrag über Hardwareinstandhaltung
EVB-IT Pflege S	Werk- bzw. Kaufvertrag über Standardsoftwarepflege
EVB-IT Dienstleistung	Dienstvertrag über Leistungen im Zusammenhang mit IT
EVB-IT System	Werkvertrag über komplexes IT-System-
EVB-IT Systemlieferung	Kauf mit Montageverpflichtung über ein IT-System
EVB-IT Erstellung	Werkvertrag über Softwareerstellung bzw. -anpassung
EVB-IT Service	Gemischter Vertrag über Systemservice und weitere Leistungen

Fig. C.6: Übersicht über die Vertragsarten EVB-IT

Überarbeitete EVB sollen kommen; noch steht ein Zeitpunkt aber nicht fest. Sie werden die wesentlichen Teile der Bereiche abdecken, die von der Vorlagensammlung bislang noch nicht umfasst sind, insbesondere zu Cloud-Leistungen; der agilen Erstellung von Software (zB. Scrum), Rahmenverträgen und Planungsleistungen.

C.1.3.5.1.2 Anwendungsverpflichtung

Eine Anwendungsverpflichtung kann sich für Einrichtungen der Freien Wohlfahrt insbesondere aus den zuwendungsspezifischen Auflagen ergeben. Aber auch wenn eine Anwen-

[286] https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html (zuletzt abgerufen am 16. Juni 2020)

[287] https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Noch_geltende_BVB/noch_geltende_bvb_node.html (zuletzt abgerufen am 16. Juni 2020).

dungsverpflichtung besteht, ist sie **nicht bieterschützend**. Neben dem zuwendungsrechtlichen Problem kann sich die Nichtanwendung auch als Verstoß gegen das **interne Haushaltsrecht** darstellen. Ein Verstoß gegen Vergaberecht ist sie aber jedenfalls **nicht**.

C.1.3.5.1.3 Besonderheit: Haftungsbegrenzung

Die EVB-IT sehen zugunsten der Anbieterinnen **Haftungsbeschränkungen** vor. Dies ist auch für die Auftraggeberinnen ein Vorteil, da viele Anbieterinnen anderenfalls aufgrund der **Unkalkulierbarkeit der Haftung** kein Angebot abgeben können. Dabei ist die Einbeziehung der EVB-IT auch für die Auftraggeberin insoweit ein Vorteil, als die Haftungsbeschränkung **intern vertreten** werden kann; sie gälte sonst leicht als unberechtigte Bevorteilung der Anbieterin.

C.1.3.5.1.4 Rahmenvertragliche Regelungen

Da die EVB-IT sind überwiegend für Einzelvorhaben entworfen worden. Sie bieten nur in begrenztem Maße über einzelne IT-Leistungen („Basisverträge“) hinausgehende, auf mehrere verbundene IT-Leistungen bezogene sog. „Systemverträge“. Es fehlen ihnen **rahmenvertragliche Regelungen**, die beispielsweise bei agilen Verfahren (dazu sogleich) wichtig werden. Diese müssen ggf. nachgetragen werden. So ist die Notwendigkeit des Abschlusses von **Einzelverträgen** im Hinblick auf ihre Granularität[288] zu regeln. Ferner sind Regelungen notwendig zur **Laufzeit** des Vertrages. Diese muss grundsätzlich **befristet** sein.[289] Zu regeln ist auch das Schicksal der Einzelverträge im Falle der **Kündigung** des Rahmenvertrages.[290] Auch Regelungen zu einer eventuellen **Mindestabnahme** und **Exklusivität** sind zu treffen.[291]

C.1.3.5.1.5 Checkliste EVB-IT

- Ist die Einbeziehung der EVB-IT geprüft worden?
- Ist die Vereinbarung von Haftungsbeschränkungen zugunsten der Auftragnehmerin geprüft worden?
- Sind ggf. rahmenvertragliche Regelungen (Laufzeit, Kündigung, Mindestabnahme, Exklusivität etc.) ergänzend bestimmt worden?

C.1.3.5.2 Mögliche Probleme bei Verträgen über Software

Der Einkauf von Software kann eine Reihe von Problemen begründen. Ein häufig relevantes **vertragsrechtliches Problem** besteht bereits in der Frage der Natur des Vertrages. So hat die Frage, ob es sich um einen **Werk- oder Dienstvertrag** handelt, etwa weitreichende Auswirkungen auf Fragen der Gewährleistung. Die Frage ist nach dem **Inhalt** des Vertrages zu beantworten. Die bloße Überlassung kann, je nachdem ob eine einmalige oder laufende Gegenleistung vereinbart wird, Kauf oder Miete bzw. Pacht sein. Kommen andere Leistungsversprechen hinzu, etwa die Erstellung, Installation, Wartung oder Schulung, können werk- und dienstvertragliche Elemente in den Vordergrund treten.

Achtung: Dies zeigt bereits, dass es auch wesentlich darauf ankommen kann, welches **territoriale Recht** Anwendung findet, unterscheiden sich Gewährleistungs- und Haftungsregelungen in unterschiedlichen Jurisdiktionen doch erheblich.

Von den genannten Vertragstypen bietet nur der **Dienstvertrag kein „echtes“ Gewährleistungsmodell**. Hier besteht der Anspruch auf Nachbesserung nur im **Falle der verschuldeten Schlechtleistung**. Die anderen Vertragstypen bieten dagegen verschuldensunabhängige Gewährleistungsansprüche.[292]

Schwerpunkt Abnahme: In vielen Fällen ist es für die Auftraggeberin erstrebenswert, das Institut der werkvertraglichen Abnahme nutzen zu können. So gelten besondere (insbesondere vom Dienstvertrag sich unterscheidende) Gewährleistungs- und Zahlungsregeln. Die Abnahme kann und sollte zudem spezifisch ausgestaltet werden. Abnahmeregelungen passen jedoch nur in Verträge, die die Herbeiführung eines bestimmten Erfolgs zum Inhalt haben; sie passen hingegen nicht in rein leistungsbezogene Verträge wie Dienstverträge.

Die zentrale Bedeutung der Abnahme liegt in ihren rechtlichen Auswirkungen:

- dem Erlöschen des originären Erfüllungsanspruches;
- dem Beginn der Gewährleistungsfristen;
- der Einhaltung der versprochenen Liefertermine,
- der Auslösung des Vergütungsanspruches der Anbieterin, und
- dem Gefahrübergang.

Im Regelfall bietet die werkvertragliche Ausgestaltung vor dem Hintergrund dieser Rechtsfolgen **dezidierte Vorteile** für die Auftraggeberin. Sie strebt einen möglichst hohen Grad an Sicherheit an, dass die Arbeitsergebnisse den vereinbar-

[288] ZB. im Hinblick auf einzelne Schritte oder (nur) auf Abschnitte bezogen.
[289] Ohne besondere vergaberechtliche Begründung grundsätzlich vier Jahre nach § 21 Abs. 6 VgV bzw. sechs Jahre nach § 15 Abs. 4 UVgO.
[290] Automatisches Erlöschen, unabhängiges Weiterlaufen oder (abhängige) Kündbarkeit kommen in Betracht. Insbesondere für den Fall, dass eine zielführende Fortsetzung des Vertragsverhältnisses nicht mehr zu erwarten ist, sollte die Kündbarkeit eingeräumt werden. AGB-rechtliche Bindungen sind ggf. zu beachten. Danach könnte nicht gleichzeitig grund- und entschädigungslos gekündigt werden.
[291] Auf die Regelung von Obergrenzen sollte hingegen verzichtet werden, sofern sie nicht (ausnahmsweise) etwa aus Billigkeitsgründen zu fordern sind.
[292] Verschuldensabhängig sind aber auch hier grundsätzlich die Ansprüche auf Schadensersatz.

ten Spezifikationen entsprechen und die vereinbarte Vergütung erst dann zu zahlen ist, wenn das Arbeitsergebnis der vertraglichen Vereinbarung entspricht.[293] Zu diesem Zweck sollten die zugesagten Leistungen, Arbeitspakete und Erstellungsfristen und die jeweils nach Abnahme zu leistenden (Teil-)Vergütungen möglichst genau spezifiziert werden.

Empfehlenswert ist eine Abnahme möglichst „unter Einsatzbedingungen", dh. möglichst nah an der geplanten Umgebung der Verwendung (zB. auf dem System der Auftraggeberin). Um Streitigkeiten zu vermeiden, sollte die Abnahme an die Erfüllung **möglichst eindeutiger Kriterien** geknüpft werden. Ein regelmäßiger Fall widersprüchlicher Interessen betrifft die Frage, wer die Einordnung von gefundenen Mängeln in die jeweiligen Mängelkategorien vornimmt. Ein Kompromiss kann hier oft über eine ausführliche und objektive **Definition der Mängelkategorien**[294] und ein eventuelles Eskalationsverfahren im Falle der Uneinigkeit erzielt werden. Die Mängelkategorien sollten aber nicht dazu führen, dass die an einen Mangel grundsätzlich anzulegenden Kriterien zu eng ausfallen und so verhindern, dass die Gewährleistung ein möglichst **breites Spektrum potenzieller Fehler und Probleme** abdeckt.

Möglichst sollte im Interesse der Auftraggeberin dabei darauf geachtet werden, dass sich die Gewährleistung auch auf Fehler erstreckt, die sich **aus der Kombination** der vertraglichen Leistung mit der Leistung anderer sowie mit bereits vorhandenen Komponenten ergeben können; dies zumal dann, wenn eine solche Integration Teil der vertraglich vereinbarten Leistung ist.

Es ist ferner empfehlenswert, die Abnahme in ein **übergeordnetes Testkonzept** zu integrieren, um Redundanzen und Lücken zu vermeiden. Zudem kann die Hinzuziehung sachverständiger Dritter (insbesondere bei kleiner IT-Abteilung) angezeigt sein.

Achtung: „Freigaben" oder „Bestätigungen" in „**agilen**"[295] Softwareentwicklungsprojekten stellen regelmäßig keine Abnahme im zivilrechtlichen Sinne dar, da die jeweiligen Ergebnisse von beiden Parteien gemeinschaftlich erarbeitet werden, so dass es an der vorauszusetzenden Kontrolle und Verantwortlichkeit der Anbieterin fehlt. Außerdem fehlt es in diesen Kontexten regelmäßig auch an einer vorab definierten Sollbeschaffenheit, die eine Abnahmeprüfung inhaltlich überhaupt erst möglich macht.

Im Hinblick auf eine **effektive Gewährleistung** sind sowohl bei **Werk- wie auch bei Kaufverträgen** insbesondere folgende Punkte regelungsbedürftig:[296]

- Beginn und Dauer der Gewährleistung (im Interesse der Anbieterin möglichst langfristig und im Hinblick auf Rechtsmängel angemessen länger, da sie häufig erst später erkennbar werden);[297]
- Hemmung und Neubeginn der Verjährung sollten nicht entgegen dem Interesse der Auftraggeberin stark eingeschränkt werden;
- Gegenstand der Gewährleistung, insbesondere bei Kombination von Leistungen (zB. Konflikt zwischen Gewährleistung und Pflege im Falle von Software);
- die Ersatzvornahme sollte bestenfalls nicht oder nur unter sehr engen Bedingungen ausgeschlossen werden;
- Beweislast für Werkerstellung, korrekte Umsetzung und Fehlerfreiheit (Auftragnehmerin);
- Reaktionszeiten und Zeiten für die Behebung der Mängel[298]; und
- Fristen und Zusammenarbeit zwischen Leistungsempfängerin und Leistungserbringerin (ua. dem Betrieb der Leistungsempfängerin);
- Über die Gewährleistung hinausgehende Garantieabsprachen zu Eigenschaften und Funktionen von Software- und IT-Systemen sollten ggf. erwogen werden.

Im Hinblick auf die Beweislast bei der Geltendmachung von Gewährleistungsansprüchen ist insbesondere sicherzustellen, dass **immer eine unveränderte Kopie der von der Anbieterin übergebenen Originalfassung einer Software aufbewahrt wird**. So kann nachgewiesen werden, dass der Mangel nicht auf eine spätere Veränderung des übergebenen Arbeitsergebnisses zurückzuführen ist.

Sofern Mitarbeitende der Auftraggeberin an der Erstellung der Software mitwirken sollen oder umgekehrt, ist die **Abgrenzung zur Arbeitnehmerüberlassung** zu beachten. Diese bedarf grundsätzlich einer **behördlichen Erlaubnis** und kann **weitreichende Konsequenzen** nach sich ziehen. Daher ist vertraglich etwa zu regeln, dass kein Übergang der Weisungsbefugnisse gegeben ist, die Steuerung der Mitarbeitenden über eine dedizierte Ansprechpartnerin der die Mitarbeitenden stellenden Vertragspartei erfolgen soll und keine Eingliederung der Mitarbeitenden in die betriebliche Organisation der anderen Partei gegeben ist.

Die **Verletzung von Schutzrechten** Dritter ist bei Softwareprojekten oft möglich und daher regelungsbedürftig.

[293] Gewährleistungsansprüche bleiben zwar grundsätzlich auch nach der Abnahme erhalten; die Abnahme trotz (gravierender) Mängel kann aber zu Einschränkungen führen, § 640 Abs. 3 BGB. Bezüglich unwesentlicher Mängel ist die Abnahme zur Vermeidung des Ausschlusses explizit unter dem Vorbehalt der Behebung zu erklären.

[294] Möglich ist beispielsweise eine Unterscheidung in – je nach Kritikalität im Hinblick auf die angestrebte Nutzung der Software – „gravierende", „wesentliche" und „unwesentliche" Mängel.

[295] Agile Softwareentwicklung zeichnet sich durch selbstorganisierende Teams sowie eine iterative und inkrementelle Vorgehensweise aus, was Transparenz und Flexibilität erhöhen soll. Bürokratischer Aufwand und der Einsatz von Regeln und Hierarchien soll weitestgehend begrenzt werden, so dass eine schnelle Anpassung an sich ergebende Veränderungen möglich wird, ohne dabei das Fehlerrisiko substanziell zu erhöhen.

[296] Mutatis mutandis, also in einem angepassten Sinne sind die Punkte weitgehend auch auf Verträge über Software as a Service (SAAS) zu übertragen, bei denen es sich regelmäßig um Miet- bzw. Pachtverträge handelt.

[297] Vor diesem Hintergrund empfiehlt sich der Ausschluss der Anwendung der Fiktion des § 377 HGB auf Rechtsmängel.

[298] Es empfiehlt sich, die Mängeldefinition im Rahmen der Sachmängelgewährleistung mit derjenigen im Rahmen der Abnahme zu synchronisieren, und zwar sowohl im Hinblick auf die relevanten Spezifikationen wie auch auf die Kategorien. Sind in Wartungs- und Pflegeverträgen bestimmte Service Level (Reaktionszeiten) vereinbart, können diese hier ebenfalls Anwendung finden.

Es sollten Zusicherungs- und Freistellungsvereinbarungen getroffen werden, die typischerweise folgende Punkte regeln:

- Zusicherung, dass die zu erstellende und die schließlich fertiggestellte Software einschließlich aller Komponenten, Schnittstellen und User Interfaces keine Schutzrechte Dritter verletzt, und die Auftragnehmerin berechtigt ist, über alle vereinbarten und notwendigen Rechte frei von Rechten Dritter zu verfügen;
- Umfang der Freistellung (insbesondere bezüglich welcher Lieferungen und Leistungen aber auch welcher Schutzrechte und deren Status [Ausschlüsse sollten auch bei Drittleistungen von der Auftraggeberin weitestmöglich vermieden werden]);
- territoriale und zeitliche Abgrenzung (im Interesse der Auftraggeberin möglichst weit und umfassend);
- Umfang der in den Schutz einbezogenen Rechtssubjekte (Mitarbeiter, [persönlich haftende] Geschäftsführung, verbundene Unternehmen);
- Abgrenzung von Eigenschäden/Beschränkung auf die Ansprüche der Dritten;
- Voraussetzungen der Freistellung;
- Verhalten im Verteidigungsprozess und dessen Kontrolle,
- Unterstützung durch Auftraggeberin und dafür ggf. anfallende Vergütung;
- ggf. Verbot der abstimmungslosen Anerkennung von Ansprüchen Dritter.

Ein weiteres besonderes Problem in Verträgen sind regelmäßig **Haftungsklauseln**. Für die Auftraggeberin ist eine möglichst umfassende Haftung der Auftragnehmerin freilich erstrebenswert. Allerdings steigt damit bei seriösen Angeboten regelmäßig auch der Preis. Insofern sollte ein sachgerechter Ausgleich gefunden werden. Das empfiehlt sich auch deshalb, weil zu einseitige Haftungsklauseln insbesondere nach AGB-rechtlicher Wertung rechtliche Schwierigkeiten bereiten können.[299]

Das eigene **Haftungsrisiko** Auftraggeberin sollte sich betragsmäßig sowie inhaltlich auf den Bruch der Geheimhaltungspflichten, Sorgfaltspflichtverletzungen im Umgang mit der Vertragsleistung und ggf. auf die Verletzung von Mitwirkungspflichten beschränken.

Veränderte Rahmenbedingungen begründen oft die Notwendigkeit der Vertragsanpassung (**Change Request**). Daher sollte Möglichkeit bestehen, den zugrundeliegenden Vertrag in einem geordneten und vordefinierten Verfahren zu ändern, wobei alle Vertragspartnerinnen Veränderungen vorschlagen können. Dies dient der Effizienzsteigerung und vermeidet Komplikationen und daraus resultierende Verzögerungen. Eine **klare Dokumentation** von Vertragsänderungen stärkt die Rechtssicherheit. Es kann sich empfehlen, „Mandatory changes“ (zB. bei sich verändernder Rechtslage) festzulegen, dh. solche Änderungen der Umstände, die eine Partei berechtigen, einseitig eine Vertragsänderung zu verlangen. Auf eine **möglichst kurzfristige Prüfungs- und Angebotserstellungsfrist** kann im Interesse der Auftraggeberin hingewirkt werden. Auf eine praktische Vertretungsregel auf Seiten der Auftragnehmerin sollte zur Beschleunigung des Verfahrens geachtet werden.

Zwar ergibt sich die Pflicht zur **vertraulichen Behandlung von geschäftlichen Informationen**[300] der Vertragspartnerin regelmäßig schon als vertragliche Nebenpflicht, womit die eventuelle Verletzung dieser Nebenpflicht bereits gesetzlich sanktioniert ist. Gleichwohl ist die Aufnahme einer Vertraulichkeitsklausel in den Vertrag zu empfehlen; da so Umfang und Inhalt des gesetzlichen Schutzes der Vertraulichkeit konkretisiert werden kann.[301]

Davon abgesehen können **Ideen für neue Apps, Plattformen, Geschäftsmodelle etc. sowie Entdeckungen, neue Erkenntnisse, Know-how etc. und sonstige geschäftliche Informationen** durch das – in Umsetzung der Richtlinie (EU) 2016/943 erlassene – **Gesetz zum Schutz von Geschäftsgeheimnissen** vor unerlaubter Offenlegung, Nutzung oder unerlaubtem Erwerb geschützt werden. Voraussetzung ist das Bestehen bzw. Ergreifen angemessener Geheimhaltungsmaßnahmen, die jeweils an Art, Verwendung und Bedeutung der konkret zu schützenden Informationen auszurichten sind. Insbesondere bei Einbeziehung Dritter unter Offenlegung von Geschäftsgeheimnissen besteht der gesetzliche Schutz als Geschäftsgeheimnis dabei nur fort, wenn dieser durch Vertraulichkeitsvereinbarungen – möglichst mit Vertragsstrafenversprechen – mit allen einbezogenen Dritten abgesichert ist.

Achtung: Eine Vertraulichkeitsklausel greift erst mit Vertragsschluss. Soll im Vorfeld des eigentlichen Vertragsschlusses bereits der Schutz von Informationen vereinbart werden, etwa deshalb, weil diese den Vertragsschluss vorbereitend ausgetauscht werden sollen, so ist ein besonderes **Non Disclosure Agreement (NDA)** abzuschließen.

[299] Nach der Rechtsprechung ist eine Haftungsbegrenzung der Höhe nach auf bei Vertragsschluss vorhersehbare und vertragstypische Schäden sogar in AGB durchaus zulässig (BGH, Urteil vom 18.7.2012 – VIII ZR 337/11). Die Haftung für entgangenen Gewinn und Folgeschäden wird in der Praxis häufig ebenfalls ausgeschlossen, um das Haftungsrisiko im Sinne der Auftragnehmerin gering zu halten. Für leichte Fahrlässigkeit wird anbieterseitig häufig eine Haftungsbegrenzung auf den Auftragswert verlangt. Die Haftung für Personenschäden, für Vorsatz und die Produkthaftung können nicht ausgeschlossen werden.

[300] Abzugrenzen ist die Vertraulichkeit vom Datenschutz und der Datensicherheit. Belange des Datenschutzes und der Datensicherheit, also beispielsweise Berechtigung zur Datenspeicherung, Abwehr unberechtigter Datenzugriffe und Verpflichtung zur Datenlöschung, werden in einer Vertraulichkeitsvereinbarung nicht oder jedenfalls nicht hinreichend abgedeckt und bedürfen eigener vertraglicher Regelungen, und zwar insbesondere eines Auftragsverarbeitungsvertrages (AVV). Siehe hierzu oben C.1.1.1.5.1.3.

[301] Es kann sich nämlich durchaus ein Interesse an der Weiterverwertung von Informationen (etwa im Rahmen der Eigenbewerbung) ergeben, so dass berechtigte Offenlegungszwecke geregelt werden sollten. Eine Vertraulichkeitsklausel umfasst regelmäßig nur solche Informationen, die nicht das Produkt (Output) der Zusammenarbeit sind, also unabhängig der Vertragsdurchführung existieren.

C.1.3.5.3 Checkliste Vertrag Softwareerstellung (allgemein)[302]

- Sind die Anforderungskriterien im Hinblick auf die Auftragnehmerin geklärt?
- Ist ein Non Disclosure Agreement (NDA) abgeschlossen, um schützenswerte Informationen auch vor Vertragsschluss hinreichend zu schützen?
- Nach dem Recht welchen zivilrechtlichen Vertragstyps soll sich die Gewährleistung richten? Ist nach der Gesamtanlage des Vertrages damit zu rechnen, dass ein ggf. entscheidendes Gericht zu derselben Einordnung gelangt?
- Steht das anzuwendende (nationale) Recht fest und trägt es die gewollten rechtlichen Konsequenzen? Soll das anwendbare Recht und/oder ein Gerichtsstand für Rechtsstreitigkeiten vertraglich festgelegt werden?
- Ist eine präzise Beschreibung der Anforderungen an das/die Arbeitsergebnis/se, Workpackages/Milestones, die jeweiligen Erstellungsfristen und zur notwendigen Abnahme vor den (Teil-)Vergütungen zur Vertragsgrundlage gemacht worden?
- Bestehen generelle Absprachen über das Verhältnis von möglichen Nachbesserungen/Anpassungen/Neuspezifizierungen während des Erstellungsprozesses im Verhältnis zu Vertrags-/Leistungserweiterungen sowie den Grundsätzen hierfür anfallender bzw. zu vereinbarender Vergütungen?
- Sieht der Vertrag angemessene Regeln zur Geheimhaltung vor? Ist die Vertraulichkeit der Vertragsparteien hinreichend umfassend und sachgerecht geregelt und ihre Verletzung ggf. auch sanktioniert? Sind sachgerechte Ausnahmen definiert worden?
- Steht ggf. die Einschaltung von Subunternehmen auf verlässlicher Grundlage (Zuverlässigkeit und Verschwiegenheitsverpflichtungen, insbesondere im Zusammenhang mit dem Zugriff auf besonders schützenswerte Daten)? Eine Unterscheidung nach Kernbereich und Hilfstätigkeiten kann sich insoweit anbieten.
- Ist die Vertraulichkeit der Vertragsparteien und des von diesen eingesetzten Personals/Subunternehmen hinreichend umfassend und sachgerecht geregelt und ihre Verletzung ggf. auch sanktioniert? Sind sachgerechte Ausnahmen definiert worden?
- Gehen die Haftungsbeschränkungen der Auftragnehmerin nicht über den sachgemäßen Rahmen hinaus?
- Sieht der Vertrag angemessene Regeln zum Datenschutz (insbesondere einen AV-Vertrag) vor? Gelten die Datenschutzregeln auf für die konkret mit der Umsetzung befassten Subunternehmen/Personen?
- Sind Mitwirkungspflichten (und sonstige Obliegenheiten) der Auftraggeberin eindeutig und angemessen geregelt und ist ggf. ein Prozess der Mitwirkung geregelt?
- Besteht ein besonderes Interesse an der Höchstpersönlichkeit der Leistungserbringung bzw. der Teamgröße? Ist der Einfluss der Auftraggeberin auf die Projektbesetzung auf Seite der Ausführenden hinreichend („Staffing“)? Ist die Tragung in diesem Zusammenhang ggf. anfallender Kosten geregelt?
- Verhindert die Vertragsgestaltung ggf. ausreichend die Annahme der Arbeitnehmerüberlassung, und zwar beiderseitig, also auch im Hinblick auf das von der Auftragnehmerin bei der Auftraggeberin eingesetzte Personal?
- Sind die BSI- und OWASP-Standards zur Softwareentwicklung soweit einschlägig vereinbart?
- Sieht der Vertrag angemessene Regeln zum Schutz und zur Verwertung von Urheberrechten und sonstiger geistiger Eigentumsrechte aller vertraglich einbezogenen Parteien vor?
- Sind die eingeräumten Nutzungsrechte für alle beabsichtigten Nutzungsarten weit und detailliert genug formuliert? Hat die Auftragsnehmerin zugesichert, dass sie in der Lage ist, die Nutzungsrechte frei von Rechten Dritter zu übertragen?
- Ist eine (territorial und inhaltlich) angemessene Regelung zur Freistellung der Auftraggeberin von Ansprüchen Dritter bei Verletzung von deren Schutzrechten gegeben und bezieht diese eine Absprache über die Vorgehensweise bei Vergleichsverhandlungen mit den Dritten mit ein?
- Trifft der Vertrag Regelungen, die eine sichere Grundlage für die Erstellung und Weiterverwertung auf Basis von OSS gewährleisten (falls gewünscht)? Stehen ggf. Bedingungen zur Nutzung vorbestehender Komponenten einer OSS-Verwertung entgegen?
- Sind die ggf. zu leistenden Beiträge der Auftraggeberin bei (gemeinsamer oder getrennter) Weiterverwertung durch die Auftragnehmerin hinreichend geschützt?
- Sind die wesentlichen Punkte zur Gewährleistung geregelt worden? Ist die Anwendung der Fiktion des § 377 HGB auf Rechtsmängel vorsorglich ausgeschlossen worden?
- Sollen über eine Gewährleistung hinausgehende Garantien vereinbart werden?
- In welchem Umfang und zu welchen Bedingungen soll die Auftragnehmerin nach Projektabschluss für Fragen zur Funktionalität und Umsetzung des IT-Systems zur Verfügung stehen?
- Ist das Haftungsrisiko der Auftraggeberin in angemessener Weise beschränkt worden?
- Ist die Behandlung und Ausführung eines Change Request möglichst praktisch geregelt?
- Sind Sicherheits- und Penetrationstests vorgesehen?

[302] Auf die Praxishilfe Ausgewogene Vertragskonzepte der Bitkom (https://www.bitkom.org/sites/default/files/file/import/Praxishilfe-Ausgewogene-Vertragskonzepte-final.pdf – zuletzt abgerufen am 10. Juli 2020) wird ergänzend verwiesen. Darin finden sich für eine Reihe der dargestellten Probleme auch Formulierungsvorschläge für Vertragsklauseln. Diese sind zu unterscheiden von AGB, da sie nicht einseitig verwendet werden, sondern als Grundlage für Vertragsverhandlungen dienen sollen.

C.1.3.5.4 Exkurs: Open-Source-Software (OSS/Freie Software)[303]

„Freie Software ist Software, die die Freiheit und Gemeinschaft der Nutzer respektiert.“
https://www.gnu.org/philosophy/

Freie Software[304] darf[305] für **jeden Zweck** genutzt werden und ist grundsätzlich **frei von Einschränkungen** wie dem Ablauf einer Lizenz oder willkürlichen geografischen Beschränkungen. Sie darf ohne Vertraulichkeitsvereinbarungen oder ähnliche Einschränkungen von allen untersucht werden, darf kostenfrei kopiert und weitergegeben werden und darf beliebig modifiziert und angepasst werden. Verbesserungen dürfen weitergegeben werden. Charakteristisch ist daher, dass der **Quelltext offengelegt** wird.

Die Nutzung der Freien Software bietet häufig **Vorteile**. Sie kann beispielsweise maßgeschneiderte Lösungen ermöglichen, ermöglicht ohne zusätzliche Kosten eine unbegrenzte Anzahl von Lizenzen und stärkt die Unabhängigkeit von einzelnen Anbietern, vermeidet also insoweit den Lock-in-Effekt. Mit Freier Software können Anwendungen erzeugt werden, die von den Erfahrungen und Ressourcen unterschiedlicher Akteure profitieren.

Bei aller Freiheit sind gleichwohl **gesetzliche Bestimmungen** zu beachten. Auch wenn der Nutzerin pauschale und umfassende Nutzungsrechte eingeräumt werden, verbleiben den Schöpfer*innen des Codes dennoch die **Urheberrechte**, die eine vollkommen freie Verfügung über die Arbeit beschränken können. Insoweit unterscheidet sich die Situation nicht elementar von der proprietärer Software. Es kommt allerdings wesentlich auf den **konkreten Inhalt der freien Lizenz** an. Derer gibt es viele unterschiedliche, die die Weitergabe und Verwertung unterschiedlich anspruchsvoll ausgestalten.[306]

Unterschieden werden kann prinzipiell danach, **wie stark der „Copyleft-Effekt“** ist. Copyleft ist ein – quasi als Antonym – von Copyright abgeleiteter Begriff, der die relative Freiheit von urheberrechtlichen Beschränkungen signalisieren soll. Ein „starkes“ oder „strenges“ Copyleft verpflichtet Lizenznehmerinnen, die Software oder jede Bearbeitung im Sinne eines viralen Effekts ebenfalls unter denselben Lizenzbedingungen wie die Originalsoftware als Open Source Software auszugeben.[307]

In diese Klasse fallen beispielsweise die klassische **GNU General Public License (GPL)** oder die **Deutsche Freie Softwarelizenz** (dfsl). Lizenzen mit beschränktem Copyleft-Effekt nehmen dagegen bestimmte Formen der Weiterverwertung aus.[308] Beispiele hierfür sind etwa die GNU Lesser General Public License (LGPL) oder die Mozilla Public License (MPL). Daneben gibt es die europäischen „interoperablen“ Copyleft-Lizenzen, die als rechtlich vereinheitliche Lizenz insbesondere für die Nutzung durch öffentliche Verwaltungen Europas und europäischer Staaten konzipiert sind; ferner die Lizenzen ohne Copyleft-Effekt, die im Hinblick auf die Weiterverbreitung zu keinem bestimmten Lizenztyp verpflichten, und vielzählige Mischformen, die Wahlmöglichkeiten und Sonderrechte einräumen können.

Die Frage ist also immer, auf welchen Lizenzen das Vorhaben aufbauen soll, ob das Produkt veröffentlicht und ob und ggf. wie es weiterverwertet[309] werden soll, welche besonderen Lizenzbedingungen für das Vorhaben also insgesamt passend bzw. notwendig sind. Die Entscheidung für ein bestimmtes Lizenzmodell ist sehr wesentlich. Hier ist **im Einzelfall Beratung** einzuholen.[310] Die im einschlägigen Bereich tätigen Agenturen können solche Beratung im Regelfall leisten und haben für eine **Fehlberatung zu haften**. Die **rechtsanwaltliche Begleitung** kann aber namentlich bei größeren und komplexeren Vorhaben zusätzlich empfohlen werden. Entscheidend ist jedenfalls, dass potentielle

[303] Teilweise wird zwischen den beiden Begriffen unterschieden. Für den vorliegenden Zusammenhang ist diese Unterscheidung nicht von tragender Bedeutung.

[304] Das Prinzip Open Source unterscheidet sich von Freeware und Public-Domain-Software. Bei Freeware handelt es sich lediglich um kostenlose Software; die Befugnis zur Änderung der Software besteht nicht notwendiger Weise und der Quellcode ist auch häufig nicht bekannt. Bei Public-Domain-Software verzichtet der Autor ganz auf sein Urheberrecht. Anders als in den USA ist dies in Deutschland aber aus rechtlichen Gründen nicht möglich. Das Urheberrecht an einer persönlichen geistigen Schöpfung verbleibt beim Schöpfer. Lediglich die Verwertungsrechte sind übertragbar. Auf dieser Basis steht Public-Domain-Software zur allgemeinen Verfügung.

[305] Nach den Standards der Open Source Initiative (OSI).

[306] Einen Überblick über die unterschiedlichen Lizenzarten verschafft die Seite https://ifross.github.io/ifrOSS/Lizenzcenter (zuletzt abgerufen am 10. Juli 2020).

[307] Das ist nicht immer gewollt. Zur Lösung daraus womöglich entstehender lizenzrechtlicher Probleme bieten sich etwa Kompatibilitätsklauseln, das Dual Licensing und auch die Trennung von Programmkomponenten an. Zudem ist die Verwendung von Bibliotheken (Libraries) privilegiert.

[308] Die Nutzungsrechte werden also von vornherein nur unter der Bedingung eingeräumt, dass die Verwenderin die Pflichten aus der Lizenz erfüllt. Damit wirkt die GPL wie eine auflösende Bedingung (§ 158 Abs. 2 BGB). Soll die Modifikation einer OSS als eigene Distribution unter eigenen Bedingungen vertrieben werden, so verstößt dies gegen die erworbene Lizenz mit der Folge, dass weder die Befugnis zur Verbreitung der ursprünglichen noch der geänderten Software fortbesteht. Relevant wird das insbesondere dadurch, dass Dritte von der Verletzenden dann keinerlei Nutzungsrechte erwerben können und auch sie die Software somit unrechtmäßig nutzen und den Ansprüchen des Urhebers und damit einem erheblichen Risiko ausgesetzt sind. Das kann allein dadurch geheilt werden, dass die Lizenznehmerin bzw. die nutzenden Dritten die Software wieder unter die ursprüngliche Lizenz stellen.

[309] Sollen etwa Dritte zur Weiterentwicklung und Integration der Software ermutigt werden, kann sich empfehlen, ihnen möglichst keine Beschränkungen in Hinblick auf die spätere Lizenzierung ihrer Produkte in den Weg zu legen. Denn ein strenges Copyleft könnte sich insoweit kontraproduktiv auswirken. Insoweit bietet sich die Verwendung von Permissive-Lizenzen an, die eine Lizenzierung abgeleiteter Werke unter beliebigen Bedingungen zu lassen. Im Übrigen ist die Ermöglichung von Interoperabilität durch Veröffentlichung von Schnittstellen- oder Formatdokumentation lizenzrechtlich unproblematisch. Die Entwicklung von Software unter Verwendung solcher Informationen begründet für sich genommen

[310] Insbesondere auch zur Kommerzialisierung (durch Dritte), Rechtswahl (die allerdings nur beschränkt möglich und von Einfluss ist) und Haftung und Gewährleistung. OSS/Freie Software sollte möglichst von Anbietern bezogen werden, deren Sitz sich mit hinreichender Sicherheit feststellen lässt.

lizenzrechtliche Schwierigkeiten frühzeitig erkannt und ggf. schon bei der Entwicklung der Software berücksichtigt werden.

Wird Freie Software eingesetzt, sollte von Beginn an strategisch vorgegangen werden:

- die stetige **Weiterentwicklung** des Projekts sollte von Anfang an mitgedacht und eingeplant werden;
- die Community und einzelne Entwicklergruppen, die relevante Erfahrungen haben, sollten nach Möglichkeit von Anfang an **einbezogen** werden;
- die Kooperation mit weiteren Stakeholdern, die ebenfalls von der Software profitieren könnten, sollte von Anfang an gesucht werden;
- der Code sollte von Beginn an grundsätzlich einsehbar sein, wenn es gewünscht wird, dass andere sich beteiligen können.

„Release early, release often!“

Eric S. Raymond in seinem Essay Die Kathedrale und der Basar, 1997

C.1.3.5.4.1 Haftungsfragen

Software ist zwar kein materielles Produkt, kann aber wie ein solches Schäden verursachen. Evident wird dies etwa bei Steuerungssoftware von gefahrbegründenden Anlagen, gilt aber auch im Hinblick auf die von der Software im Einzelfall angesteuerte private Hardware (zB. CPU und Speicher). Insbesondere die (verschuldensabhängige) **Produkthaftung** kommt daher auch bei Software in Betracht. Die Haftung wird insbesondere auch nicht dadurch ausgeschlossen, dass der Zurverfügungstellung ggf. eine Schenkung zugrunde liegt. Auch unentgeltlich abgegebene Software muss den zu erwartenden Mindestanforderungen an die (Produkt-) Sicherheit genügen.

Aber nicht nur im Hinblick auf den Verwender, sondern auch im Hinblick auf die Weiterverwendung der erstellten Software kommt eine Haftung in Betracht. Im typischen Rahmen der Weitergabe von OSS (Copyleft) ist der Haftungsmaßstab aufgrund der schenkungsrechtlichen **Haftungsprivilegierungen** aber deutlich günstiger als im Rahmen der regulären Haftung bei proprietären Verträgen.

Schließlich besteht ein nicht unerhebliches Risiko bei der Verwendung von OSS/Freier Software durch eine möglicherweise gemäß §§ 97ff. UrhG und §§ 812 ff. BGB begründete Haftung.[311] Denn eine solche kann aufgrund der Besonderheiten des Urheberrechts nicht aufgrund gutgläubigen Erwerbs, welcher im Bereich von geistigen Eigentumsrechten generell nicht möglich ist, ausgeschlossen werden. Ist die **Urheberschaft ungesichert** oder deren Konsequenzen aufgrund komplexer internationaler Rechtslage **undurchsichtig**, kann im Einzelfall ein erhebliches Haftungsrisiko bestehen. Eine gute Beratung wie auch Vertragsgestaltung kann auch hier absichern.

C.1.3.5.4.2 Checkliste OSS/ Freie Software

- Soll der Quellcode aus strategischen oder gemeinnützigen Gründen veröffentlicht werden oder sprechen steuerrechtliche Gesichtspunkte (Gemeinnützigkeit) für eine Offenlegung des Quellcodes?
- Ist die Weiterverwertung des Produkts oder dessen Teile geplant? Soll ein Entgelt für die Weitergabe erhoben werden (in diesen Fällen ist eine Vereinbarkeit mit den verwendeten Lizenzen intensiv zu prüfen, da sich eine entgeltliche Verwertung im Sinne entgeltpflichtiger Lizenzen in der Regel mit den Vorgaben von OSS-Lizenzen beißt)?
- Ist klar definiert, welche Lizenzbedingungen dem Vorhaben entsprechen und passen OSS-Lizenzen? Welche?
- Ist der mit der Agentur/der Entwicklerin zu schließende Vertrag auf den Einsatz von OSS/Freier Software abgestimmt (Rechtswahl, Lizenzierung, Anpassung der Lizenz, Nutzungsrechte, Gewährleistung, Haftung etc.)?
- Ist insbesondere die Haftung gegenüber Dritten nach §§ 97ff UrhG etc. durch hinreichende Beratung und Haftungsfreistellung ausgeräumt?

[311] Bei Verletzungen von geistigen Eigentumsansprüchen kommt auch ein Anspruch aus §§ 812 Abs. 1 2. Alt, 818 III BGB als verschuldensunabhängiger Bereicherungsanspruch in Betracht. Das „Erlangte“ besteht in den ersparten Lizenzkosten. Im Rahmen des Wertersatzes kann daher u.a. die „fiktive“, sprich übliche Lizenzgebühr verlangt werden (sog. Lizenzanalogie). Auch § 667 BGB analog (GoA) kann evtl. als verschuldensunabhängiger Anspruch auf das Erlangte in Betracht gezogen werden. Auch § 823 BGB kann eine eigene Relevanz haben, da hierüber bei Verletzungen der immateriellen Urheberpersönlichkeitsrechte über § 253 BGB auch ein „Schmerzensgeld“ denkbar ist. Dies wäre aber nur dann relevant, wenn man § 97 Abs. 2 S. 1 UrhG als rein materiellen Schadensersatzanspruch verstünde. Ein immaterieller Schadensersatz spielt – anders als bei Persönlichkeitsrechten – bei Urheberrechtsverletzungen in der Praxis aber nur eine untergeordnete Rolle.

C.1.3.5.5 Vertiefung: Agile Softwareprojekte

Agile Projektmethoden[312] finden immer mehr Verbreitung. Sie sind aufgrund ihrer naturgemäßen Flexibilität oft **krisenfester** als herkömmliche Softwareprojekte. Allerdings lässt sich auch bei ihnen ein Scheitern nicht ganz ausschließen. Umso wichtiger ist eine **gute Vorbereitung und sorgfältige Vertragsgestaltung**. Letzterer sind die Besonderheiten der agilen Methode zugrunde zu legen.

C.1.3.5.5.1 Vertragstyp

Eine grundsätzliche Frage wirft das agile Verfahren von vornherein auf: Welches Gesetzesrecht beansprucht Geltung? Handelt es sich bei agil gestalteten Softwareerstellungs-Verträgen um **Werk- oder Dienstvertragsrecht**?[313] Die Antwort auf diese Fragen ist nicht nur aufgrund **gewährleistungsrechtlicher Aspekte** entscheidend. Auch **AGB-rechtlich** können sich erhebliche Abweichungen ergeben. So kann etwa der im Rahmen von § 307 Abs. 2 Ziff. 1 BGB anzulegende Maßstab der „gesetzlichen Regelung“ überhaupt nur vermittels einer typologischen Einordnung des in Frage stehenden Vertrages bestimmt werden.

Die Auftragnehmerin hat im Regelfall ein Interesse daran, die Vertragsbeziehung dem Dienstvertragsrecht zuzuordnen, da die starke Einbindung der Auftraggeberin, die gewisse Abhängigkeit von dieser also, die Übernahme der werkvertraglichen Verantwortung als zu risikoreich erscheinen lässt. Dagegen dürfte die Auftraggeberin grundsätzliches Interesse an der Geltung des **Werkvertragsrechts** haben. Es empfiehlt sich daher, die **Geltung des Werkvertragsrechts vertraglich ausdrücklich zu vereinbaren und die vertraglichen Pflichten möglichst detailliert und in erfolgsbezogener Form auszugestalten**.

Zwar ist den Parteien keine grundsätzliche Disposition über das anzuwendende Recht gegeben, da sich dieses nun einmal aus dem Recht selbst ergeben muss. Sofern aber der Vertrag sich nicht grundsätzlich als anderer Vertragstypus darstellt, da sich – wie regelmäßig anzunehmen ist – die Hauptleistungspflichten werkvertraglich abbilden lassen,[314] sollte die Einordnung auch vor Gericht Bestand haben. Sollte allerdings das Entwicklungsteam zum Teil aus dem Hause der Auftraggeberin stammen und daher die Auftraggeberin immerhin eine Mitverantwortung für den Leistungserfolg treffen, sollte vertraglich klar geregelt werden, wer die **Hauptverantwortung für den Erfolg** trägt. Nur wenn dies die Auftragnehmerin ist und sich dies auch tatsächlich entsprechend auswirkt, etwa deshalb, weil die Mitarbeitenden der Auftraggeberin nur beraten oder in der deutlichen Minderzahl sind, die Entwicklungs- und Implementierungsarbeiten also nicht selbst vornehmen und die Auftragnehmerin die Bereitstellung eines funktionstüchtigen Systems versprochen hat, wird die Vereinbarung von Werkvertragsrecht erfolgreich sein.

C.1.3.5.5.2 Wesentliche Vertragsinhalte

Mit der Sicherstellung der richtigen vertragstypologischen Einordnung ist es aber noch nicht getan. Ist die inhaltliche Lückenhaftigkeit des Vertragstextes schon bei herkömmlichen Softwareprojekten problematisch, erweist sie sich im Rahmen agiler Projekte als mitunter besonders schädlich; insbesondere dann, wenn der Vertragsinhalt keine ausreichende **Rücksicht auf die anzuwendende Methode** liefert. Aber nicht nur die anzuwendende **Methodik sollte klar vereinbart** werden, sondern auch Inhalt und Umfang der aus ihr jeweils folgenden Pflichten, namentlich der **Mitwirkungspflichten**.[315]

Der bloße Hinweis auf die Methodik, zB. Scrum, ist insofern nicht ausreichend, da die bleibenden Spielräume ausgefüllt werden müssen – beispielsweise welche Partei welche Rollen besetzt (Product Owner, Scrum Master etc.), wobei auch die **Aufgaben der Rolleninhaberinnen** konkret beschrieben werden müssen (wie etwa die Erstellung und Verwaltung des Product Backlog beim Product Owner). Die sachgemäße Erstellung eines funktionierenden Product Backlogs ist allerdings

[312] Zu agilen Projektmethoden im Allgemeinen siehe Hoeren/Pinelli, MMR 2018, S. 199 ff. sowie Fuchs/Meierhöfer/Morsbach/Pahlow, MMR 2012, S. 427ff.

[313] Eine höchstrichterliche Klärung der Frage steht zum Zeitpunkt des Redaktionsschlusses noch aus. Die bisherige Rechtsprechung zu IT-Verträgen lässt sich nicht unabhängig des Einzelfalls übertragen. Auf das Urteil des OLG Frankfurt/M. vom 17. August 2017 (6 U 250/16), MMR 2018, S. 100, wird verwiesen. Das OLG hat die Frage allerdings offengelassen, da es den Fall unabhängig der Einschlägigkeit dienstvertraglicher Regelungen lösen konnte. Die Vorinstanz hatte hingegen noch das Werkvertragsrecht ausdrücklich als einschlägig erkannt.

[314] So erfolgt die Einordnung von (klassischen) Projektverträgen über die Erstellung von Individualsoftware nach ständiger Rechtsprechung des BGH und hM. in der Literatur regelmäßig als Werkvertrag (siehe die Nachweise bei Heydn, Agile Softwareprojekte: Probleme und Vertragsgestaltung, MMR 5/2020, S. 284 (286).

[315] In der Praxis kommt es beispielsweise nicht selten vor, dass sich die Anbieterin nach dem Scheitern des Projekts auf das agile Vorgehen beruft. Sofern dies als bloße Schutzbehauptung gemeint ist, kann sie ein konkreter Vertrag und eine gute Dokumentation des Vorgehens leicht abwenden. Es bietet sich an, die jeweiligen Elemente der zugrunde gelegten Methode vertraglich zu fixieren. Bei Scrum zB. die fünf Scrum-Ereignisse (Sprint und die dazugehörigen Events des Planning, Daily Scrum, Sprint Review und Sprint Retrospective). Auf den Daily Scrum kann allerdings verzichtet werden, wenn das Entwicklungsteam vollständig auftragnehmerseitig gestellt wird. Die Vereinbarung sollte aber jedenfalls die Phase der initialen Erstellung des Product Backlogs abbilden, das die Vorgaben aus dem vorausgegangenen Vergabeverfahren aufnimmt.

nur möglich, wenn zuvor die Produktvision umfassend erarbeitet wurde.[316] Einzelanforderungen können in Form von **User Stories** fomuliert werden. Dabei wird beschrieben, wie die Bedarfe der Nutzer*innen konkret durch die Software beantwortet werden.

Im Hinblick auf die Abarbeitung des Backlogs empfiehlt sich die folgende Klausel im Vertrag:

> Die in Anlage X niedergelegte Produktvision bestimmt die Leistungserbringung nach diesem Vertrag. Die Leistungsbeschreibung wird im Product Backlog im Rahmen von Sprint Backlogs fortlaufend präzisiert. Sofern sich Sprint Backlogs widersprechen, gehen jüngere älteren vor.

Typischerweise entsteht im Rahmen von IT-Projekten auch immer wieder Streit darüber, ob eine bestimmte Funktionalität oder Eigenschaft der Software schon aufgrund des ursprünglichen Vertrages geschuldet ist oder „out of scope“ liegt, also vom bisherigen Leistungsversprechen nicht umfasst wird. Über den Vertragsinhalt hinausgehende Leistungen müssen im Change-Request-Verfahren zusätzlich beauftragt und vergütet werden, wogegen das Fehlen bereits versprochener Leistungsinhalte eine Abweichung der vertraglichen Soll- von der Ist-Beschaffenheit darstellen. Ohne eine zusätzliche Vergütung zu schulden, stehen der Auftraggeberin insoweit Erfüllungs- und Gewährleistungsansprüche zu.

Die **Vermeidung solcher Diskussionen ist ein wesentlicher Ansatzpunkt des agilen Verfahrens**. In einem solchen sind **Änderungswünsche grundsätzlich willkommen**, auch wenn sie erst vergleichsweise spät geäußert werden. Hierdurch wird quasi eine **Umkehrung des Regel-Ausnahme-Verhältnisses** bewirkt:

In der Regel bedürfen Änderungen des Kundenwunsches **keiner** Vertragsänderung. Das kann ein wesentlicher Vorteil agiler Verfahren sein, denn die Change-Request-Verfahren im herkömmlichen Sinne können so entfallen. Das heißt aber nicht, dass die Auftraggeberin alle Änderungen und Erweiterungen kostenfrei verlangen kann. Sollten sich die Änderungen auf die Zeit-, Aufwands- und Kostenschätzung auswirken, hat dies die Auftragnehmerin klarzustellen. Eine Klausel könnte folgendermaßen lauten:

> Mit Ausnahme derjenigen Product Backlog Items, die im jeweils aktuell laufenden Sprint abgearbeitet werden, können die Product Backlog Items geändert, durch neue ersetzt oder in ihrer Priorisierung verändert werden. Sollten die Änderungen Auswirkungen auf Zeit-, Aufwands- und/oder Kostenschätzung haben, wird die Auftragnehmerin die Auftraggeberin hierauf unverzüglich in Textform spezifiziert hinweisen. Durch Mitteilung in Textform kann die Auftraggeberin die Änderungen freigeben. Erst nach Freigabe ist die Auftragnehmerin berechtigt und verpflichtet, die Änderungen umzusetzen.

Bei größeren und längerfristigen Vorhaben kann es sich allerdings anbieten, daneben auch die Change-Request-Regel der Ziff. 16 EVB-IT Erstellung AGB für grundsätzliche Änderungen offen zu halten. Dies insbesondere, wenn ein **(„agiler“) Festpreis**[317] vereinbart werden soll. Im Vertrag sollte daher eine **möglichst konkrete Abgrenzung** vorgenommen werden, für welche besonderen Fälle die Change-Request-Regelung aus den AGB anwendbar bleiben soll.

C.1.3.5.5.3 Abnahme

Streit um die im Sinne des Vertragserfolgs wichtige Abnahme kann bereits dadurch vermieden werden, dass die Kriterien der Abnahme möglichst konkret vereinbart werden. Es ist insoweit sinnvoll, **Mängelklassen zu vereinbaren**. Die Mängelklassen des EVB-IT Erstellung-AGB werden der Praxis nicht immer gerecht.[318] Zu achten ist jedenfalls darauf, dass die Testfreiheit der Auftraggeberin nicht beschränkt wird. In Ziff. 13 sehen die AGB der EVB-IT Erstellung zusätzlich zu den Inhalten der Ziffer 11 die Möglichkeit zur individuellen Anpassung der Abnahmeregeln vor, wovon im Hinblick auf das konkrete Projekt – im Rahmen der aufgrund der Agilität naturgemäß beschränkten Möglichkeiten – auch Gebrauch gemacht werden sollte. Beispielsweise kann sich die Vereinbarung einer verlängerten Funktionsprüfungsdauer empfehlen.

Im Hinblick auf die Abnahme kann zugunsten der Auftragnehmerin eine **Teilabnahme** der jeweils ausgelieferten Softwareteile vereinbart werden.[319] Folgendes kann dazu vereinbart werden:[320]

> **(1)** Nach jedem Sprint Review Meeting prüft die Auftraggeberin unverzüglich die Funktionalität des

[316] Im Prinzip entspricht der Product Backlog dem herkömmlichen Lastenheft (das auftragnehmerseits noch in ein Pflichtenheft zu übersetzen wäre). Die in ihm aufgeführten Einzelanforderungen werden nach festgelegter Priorität einzeln zunächst im Sprint Backlog präzisiert und dann im Sprint abgearbeitet. Im Unterschied zu der herkömmlichen Herangehensweise, die bei veränderten Anforderungen grundsätzlich einen change request voraussetzt, kann der Product Backlog jederzeit einseitig von der Auftraggeberin geändert werden. Eine Ausnahme besteht nur für die Teile, die sich gerade im Sprint, also der Abarbeitung befinden.

[317] Beim agilen Festpreis wird eine Überschreitung auch dann zugelassen, wenn diese nicht auf eine Leistungsänderung zurückzuführen ist. Es soll aber nur ein bestimmter Prozentsatz der Aufwände vergütet werden, während die Auftragnehmerin den Rest selbst trägt. Das Risiko wird also geteilt.

[318] Siehe zu Einzelheiten etwa Koch/Kunzmann/Müller, EVB-IT Erstellung, Gestaltungshinweise für agile Softwareentwicklungsverträge, MM§ 01/2020, S. 8 ff. (10).

[319] Soll mit der Teilabnahme eine Abschlagszahlung ermöglicht werden, ist das – wie auch die Höhe der Zahlung – ausdrücklich zu vereinbaren.

[320] Die Abnahme von Sprint-Leistungen ist allerdings nicht immer sinnvoll. Ggf. sollten stattdessen eher größere Projekteinheiten, zB. ein ganzes Softwaremodul, abgenommen werden.

Product Increments anhand des Product Backlog und der entsprechenden Definitions of Done, was sie in einem Teilabnahmeprotokoll mitsamt einer Liste eventueller Mängel dokumentiert.

(2) Meldet die Auftraggeberin nicht innerhalb von [X][321] Tagen nach textförmlicher Aufforderung durch die Auftragnehmerin aufgetretene Mängel, gilt das Increment als abgenommen. Die Teilabnahme tritt auch dann ein, wenn das Increment nach Entscheidung des Product Owner als funktionstüchtig in den laufenden Betrieb übernommen wird.

Da die einzelnen Softwareteile nicht nur für sich, sondern auch im Zusammenspiel funktionieren sollen, ist eine Endabnahme ebenfalls erforderlich:

(1) Ist das letzte Product Increment abgenommen, prüft und protokolliert die Auftraggeberin die Abnahmefähigkeit des gesamten Produkts unverzüglich in seinem Zusammenspiel.
(2) Unwesentliche Mängel behindern die Abnahmefähigkeit nicht, sofern sie durch die Auftragnehmerin unverzüglich beseitigt werden. Auch sie sind einzeln zu protokollieren.

Da die Definitions of Done sich sowohl aus den Anforderungen aus der Leistungsbeschreibung, den weiteren Vergabeunterlagen, dem bezuschlagten Angebot wie auch aus den weiteren Änderungen ergeben, die die Anforderungen bzw. deren Umsetzung im Zuge des Projekts erfahren haben, ist die genaue Dokumentation aller Änderungen anzuraten.

C.1.3.5.5.4 Pflege

Bei der agilen Erstellung stellen sich Fragen der Pflege anders als bei herkömmlichen Softwareprojekten. Der Beginn der Pflege wird häufig an Teilabnahmen geknüpft; und die Vergütung der Pflege muss berücksichtigen, dass nur ein Teil der Gesamtsoftware gepflegt wird. Dies ergibt sich (nur) dann automatisch, wenn die Vergütung der Pflege mit einem Prozentsatz des Gesamtentwicklungspreises berechnet wird und dieser jeweils auf das Teilabgenommene heruntergebrochen wird.

Zur Vereinfachung des Aufwands, der durch häufig wechselnde Vergütungen entsteht, kann auch vereinbart werden, dass die Pflegevergütung erst mit der Endabnahme überhaupt einsetzt. Ein Argument gegenüber der Auftragnehmerin kann darin liegen, dass die Pflege insbesondere anfänglich häufig ohnehin in der Beseitigung von Störungen besteht, die der Mängelbeseitigung unterfallen.

C.1.3.5.5.5 Dokumentation

Obwohl im Rahmen der agilen Denke der Schwerpunkt eher auf das Produkt denn auf die Dokumentation gelegt wird, ist die **Dokumentation dennoch von entscheidender Bedeutung**, da sie die Lauffähigkeit und Veränderbarkeit der Software (insbesondere bei Anbieterwechsel) **langfristig sichern** kann. Zwar sehen die EVB-IT Erstellung in Ziffern 5 und 17 umfassende Dokumentationspflichten für die Software und den Quellcode vor. Es finden sich dort allerdings keine Vorgaben dazu, **wann** der Auftragnehmer die Dokumentation **erstellt**, sondern nur, wann diese fertig zu übergeben ist, nämlich spätestens zur Bereitstellung zur Funktionsprüfung. Da im Rahmen der agilen Entwicklung die Auftragnehmerin aber nicht isoliert für sich arbeitet, sollte **ausreichend Raum für eine gute Dokumentation** geplant werden. Die Regelungen aus den EVB-IT Erstellung sind **entsprechend anzupassen und zu ergänzen**.[322]

C.1.3.5.5.6 Vergütung

Die Gestaltung der Zahlungsflüsse ist in agilen Projekten auf mehrere Arten denkbar. Die Vereinbarung eines **Festpreises ist regelmäßig unangemessen**, denn der Aufwand wird durch die Auftragnehmerin **nicht selten unterschätzt**. Die Vereinbarung einer **Vergütung nach Aufwand ist dagegen** – auch in Ansehung der Vereinbarung der Geltung des Werkvertragsrechts – **gut möglich**, trägt aber immer auch die Gefahr ausufernder Erstellungskosten in sich. Zumindest sollte **ausdrücklich im Vertrag bestimmt** werden, dass hierdurch die **Kostenfreiheit der Mängelbeseitigung unberührt** bleibt. Die Aufwände zur Beseitigung von Mängeln sind separat zu erfassen und vorzulegen und dürfen nicht abgerechnet werden. Allerdings wird die **Kombination von aufwands- und erfolgsabhängiger Vergütung** im Regelfall dem agilen Geschehen am ehesten gerecht.

Folgendes könnte vereinbart werden:

(1) Für jeden Sprint zahlt die Auftraggeberin unabhängig einer Teilabnahme[323] eine Pauschalvergütung in Höhe von € X.[324]

[321] Beispielsweise: 10.
[322] So kann fortlaufend während und innerhalb der Sprints aber auch in intermettierenden Konsolidierungsphasen dokumentiert werden. Auch sollte vor Projektabschluss die Finalisierung der Dokumentation erfolgen können.
[323] Die Unabhängigkeit hat zugunsten der Auftragnehmerin zur Folge, dass die Auftraggeberin keinen Anreiz hat, die Teilabnahme zu verweigern. Dies zumal sie die Nachbesserung ohnehin kostenfrei verlangen kann.
[324] Diese Klausel passt insbesondere zum Scrum-Verfahren, da hier jeder Sprint grundsätzlich die gleiche Dauer haben soll.

(2) Mit erfolgter Endabnahme wird eine weitere Vergütung in Höhe von € X fällig.

Alternativ ist auch eine Vergütung nach Meilensteinen möglich, wenn die dafür zu erbringenden Leistungspakete bei Vertragsschluss bereits feststehen – was aber eher die Ausnahme sein dürfte. Von der **Abhängigkeit der Vergütung von der Abnahme sollte im Interesse der Auftraggeberin keinesfalls abgewichen werden**. Kalenderabhängige Zahlungen für Leistungen der Erstellung sind zu vermeiden. Solche widersprechen dem Werkvertragscharakter und machten die daraus für die Auftraggeberin resultierenden Vorteile weitgehend zunichte. Sofern **Abschläge** vereinbart werden, sollte für die Gesamtabnahme noch ein signifikanter **Restbetrag** verbleiben, um der Auftraggeberin genügend Druckmittel zu belassen. Abschläge sollten insgesamt 80% der Gesamtvergütung nicht überschreiten.

Im Falle der aufwandsbezogenen Vergütung sind neben dem Stunden- oder Tagessatz vor allem auch Regelungen zu Materialkosten, Nebenkosten, Reisekosten und Reisezeiten zu treffen. Material- und Nebenkosten können regelmäßig ausgeschlossen werden. Hinsichtlich Reisekosten und -zeiten kann sich eine All-inclusive-Regelung anbieten, die eine gesonderte Abrechnung von vornherein ausschließt.

Bei Vergütungen nach Aufwand kann aber naturgemäß die **Gefahr des Ausuferns** bestehen. Dem kann dadurch entgegengewirkt werden, dass sich die Auftraggeberin im Vergabeverfahren Aufwände und damit feste Preise für fiktive oder nicht fiktive Referenz-User-Stories anbieten lässt. Dies ermöglicht ihr nicht nur, verschiedene Anbieter hinsichtlich ihrer potenziellen Entwicklungsgeschwindigkeit zu **vergleichen**. Sind repräsentative User Stories zur Grundlage gemacht, können die später geltend gemachten Aufwände mit denen verglichen werden, die die Auftragnehmerin im Vergabeverfahren angegeben hat. Für den Fall der größeren Überschreitung kann die Auftraggeberin durch eine entsprechende Vertragsgestaltung sicherstellen, dass sie **ggf. eine Herabsetzung der Vergütung verlangen** kann.

C.1.3.5.5.7 Vorzeitige Beendigung

Auch dann, wenn hinsichtlich der Produktvision möglichst sorgfältig gearbeitet wurde, kann sich im Laufe des Projekts dessen Undurchführbarkeit herausstellen. Die Gefahr ist im Rahmen von agilen Projekten deutlich größer als bei herkömmlichen. Je unpräziser im Rahmen der Produktvision (und der Vertragsgestaltung) gearbeitet wurde, desto größer ist die Gefahr. Es sollte daher für alle Parteien die Möglichkeit eines für alle Seiten akzeptablen Ausstiegs vereinbart werden. Hierzu kann etwa die das Kündigungsrecht der Auftraggeberin nach § 648 BGB modifiziert werden:

> Der Vertrag kann durch die Auftraggeberin jederzeit ohne Angabe von Gründen mit sofortiger Wirkung beendet werden. In diesem Fall gilt abweichend von § 648 S. 2 und 3 BGB das Folgende: Es sind nur die bis zum Projektausstieg vertragsgemäß erbrachten Leistungen zu vergüten. Erfolgt der Ausstieg binnen dreier Monate seit Projektbeginn, wird zusätzlich ein Betrag in Höhe von € X fällig. Darüber hinaus bestehen keine weiteren Ansprüche auf Vergütung oder Kompensation.

Da durch die vorstehende Klausel im Wesentlichen nur die Auftraggeberin geschützt ist, kann es sich im Hinblick auf eine möglicherweise notwendige vorzeitige Beendigung anbieten, eine gemeinsame Evaluierung des Projektes als mögliche „Sollbruchstelle“ zu vereinbaren:

(1) Nach den ersten drei Sprints evaluieren die Parteien das Projekt und seinen bisherigen Verlauf gemeinsam.[325] Es steht jeder Partei frei, aufgrund der Evaluierung das Projekt abzubrechen. Entscheiden sich beide Parteien oder nur die Auftraggeberin für den Abbruch, sind nur die bisher vertragsgemäß erbrachten Leistungen zu vergüten. Entscheidet sich allein die Auftragnehmerin für den Abbruch, ist dieser Anspruch um 20% zu kürzen. § 648 findet keine Anwendung.

(2) Aufgrund der Projektevaluation kann jede Partei die Fortführung des Projekts zu veränderten vertraglichen Bedingungen verlangen. Ist das Verlangen nicht unbillig und kommt dennoch keine Einigung binnen zweier Wochen zustande, gilt das Projekt als abgebrochen. Abs. 1 S. 3 bis 5 gelten entsprechend.

C.1.3.5.5.8 Urheberschaft

Gerade im Rahmen agiler Projekte kann es aufgrund der Zusammenarbeit im Einzelfall zu urheberrechtlichen Schwierigkeiten kommen. Das Institut der Miturheberschaft (§ 8 UrhG) kann insoweit Abhilfe schaffen.[326] Die Rechtsbeziehungen aller beteiligten Miturheber- bzw. Mitrechtsinhaber zueinander und im Verhältnis zur Software sollten insoweit in **möglichst klarer und eindeutiger Form geregelt sein**, die eine Nutzung und Verwertung der Projektergebnisse zu den beabsichtigten Zwecken, einschließlich späterer Ak-

[325] In geeigneten Fällen können weitere Evaluierungen vereinbart werden.

[326] Vgl. hierzu im Einzelnen Hoeren/Pinelli, Miturheberschaft in der agilen Softwareentwicklung?, MMR 12, 2019, S. 779 ff.

tualisierungen der Software, gestatten. Dies kann und sollte ggf. auch die Pflicht zur Einräumung sämtlicher ausschließlicher Rechte zur Nutzung und Bearbeitung der Software an die Auftraggeberin beinhalten, was ggf. durch eine detaillierte Ausformulierung der vertraglichen Nutzungsrechts- bzw. Lizenzklauseln abzusichern ist. Um eine spätere Verwertung und Aktualisierung nicht zu gefährden, sollte hierfür ein möglichst fachkundiger Rechtsrat eingeholt werden.

C.1.3.5.5.9 Checkliste Agiles Softwareprojekt

- Die Geltung des Werkvertragsrechts ist ausdrücklich im Vertrag vereinbart worden.
- Es besteht eine eindeutige vertragliche Regelung von Methode, Rollen und den geschuldeten (Mitwirkungs-)Pflichten.
- Product Owner gehört dem Hause der Auftraggeberin an.
- Product Owner ist im erforderlichen Umfang für die Arbeit im Projekt freigestellt.
- Definitions of Done und die Entscheidung der Abnahmefähigkeit der Leistung sind dem Product Owner vorbehalten.
- Gemeinsame Erarbeitung einer Produktvision (statt eines umfangreichen Lastenhefts [und des darauf basierenden Pflichtenhefts]): Die übergeordneten Zwecke und Ziele sind umfassend dargestellt.
- Beschreibung der Produktvision ist Bestandteil des Vertrages.
- Regelung zum zeitlichen Primat der Sprint Backlogs ist getroffen.
- Regelungen zur Abnahme und Teilabnahme sind getroffen worden.
- Zahlungen für die Erstellung sind nicht an Daten geknüpft.
- Eine konsistente Regelung zur Vergütung ist getroffen worden. Die Vergütung ist abhängig von der Abnahme. Kalendermäßige Zahlungen sind nicht vereinbart.
- Im Falle der Vergütung nach Aufwand hat sich die Auftraggeberin Aufwände und damit feste Preise für fiktive oder nicht fiktive Referenz-User-Stories anbieten lassen, so dass bei Ausufern der geltend gemachten Vergütung eine auf einem entsprechenden Vergleich beruhende Herabsetzung verlangt werden kann.
- Sofern Abschläge vereinbart werden, verbleibt ein signifikanter Restbetrag im Hinblick auf die Gesamtabnahme.
- Im Falle der aufwandsbezogenen Vergütung sind neben dem Stunden- oder Tagessatz auch Regelungen zu Materialkosten, Nebenkosten, Reisekosten und Reisezeiten getroffen worden. Die Vergütung von Material- und Nebenkosten ist bestenfalls ausgeschlossen.
- Für den Fall der vorzeitigen Notwendigkeit der Beendigung des Projekts ist vertraglich angemessen vorgesorgt worden. Eine Regelung zur Projektevaluierung ist insoweit vereinbart worden.
- Durch entsprechende Nutzungs- bzw. Lizenzklauseln ist sichergestellt, dass die Projektergebnisse für alle beabsichtigen Zwecke, einschließlich von Aktualisierungen, nutzbar sind.

C.1.4 SONDERPROBLEM: ARBEITGEBERIN UND TKG, TMG

Zu beachten ist, dass die Arbeitgeberin unter bestimmten Bedingungen als Diensteanbieterin im Sinne des Telekommunikationsgesetzes (TKG) bzw. des Telemediengesetzes (TMG) gelten kann. Die genannten Gesetze sichern u.a. das Fernmeldegeheimnis ab und unterwerfen die Diensteanbieter bestimmten **Vertraulichkeitsvorgaben**. Dies kann dann der Fall sein, wenn der Arbeitgeber **auch** die **private** Nutzung der betrieblichen Internet- Kommunikationsdienste erlaubt.[327] Die Pflichten und Vorgaben erstrecken sich dann (auch) auf die Kommunikation von Dritten (also Externen, die zB. den Beschäftigen private E-Mails zurückschicken). Insbesondere hat eine fehlende Trennung bzw. Unterscheidungsmöglichkeit von dienstlichen und privaten E-Mails zur Folge, dass der Arbeitgeberin der Zugriff auf die dienstliche Kommunikation der Beschäftigten **versagt** ist. Verstöße hiergegen können strafrechtliche Konsequenzen haben (u.a. nach § 206 StGB).

[327] § 11 Abs. 1 Ziff. 1 TMG macht eine Ausnahme nur im Hinblick auf die rein dienstliche Nutzung.

C.2 GoBD-FÄHIGKEIT DER ANWENDUNG[328]

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) sollen eine **reibungslose Betriebsprüfung durch Steuerprüfer und Finanzamt** gewährleisten, indem die steuerlich relevanten Geschäftsunterlagen ordnungsgemäß geführt und aufbewahrt werden.

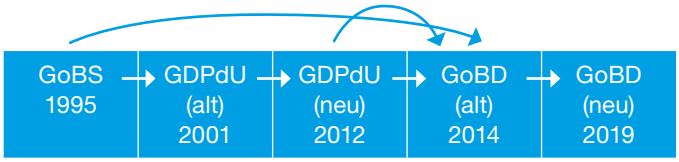


Fig. C.7: Entwicklung der GoBD über ihre Vorstufen (die gebogenen Pfeile heben besondere Einflüsse hervor)

Bei Planung einer digitalen Lösung sind auch Fragen der ordnungsgemäßen Buchführung von Beginn an **mitzudenken**. Nach § 140 AO sind die außersteuerlichen Buchführungs- und Aufzeichnungspflichten, die auch steuerlich relevant sind, auch für das Steuerrecht zu erfüllen. Außersteuerliche Buchführungs- und Aufzeichnungspflichten ergeben sich insbesondere aus den Vorschriften der **§§ 238 ff. HGB** und aus den dort bezeichneten handelsrechtlichen Grundsätzen ordnungsmäßiger Buchführung (GoB).

Für einzelne Rechtsformen ergeben sich **flankierende Aufzeichnungspflichten** z. B. aus §§ 91 ff. Aktiengesetz, §§ 41 ff. GmbH-Gesetz oder § 33 Genossenschaftsgesetz. Des Weiteren sind zahlreiche **gewerberechtliche oder branchenspezifische Aufzeichnungsvorschriften** vorhanden, die gem. § 140 AO im konkreten Einzelfall für die Besteuerung von Bedeutung sind.

Daneben sind alle Unterlagen aufzubewahren, die **zum Verständnis und zur Überprüfung** der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind.[329] Dazu zählen neben Unterlagen in Papierform auch alle Unterlagen in Form von Daten, Datensätzen und elektronischen Dokumenten, die dokumentieren, dass die Ordnungsvorschriften umgesetzt und deren Einhaltung überwacht wurde.

Bei der Führung von Büchern sind im digitalen wie analogen Bereich die folgenden allgemeinen Grundsätze zu beachten:

- der Grundsatz der **Nachvollziehbarkeit und Nachprüfbarkeit** sowie die
- Grundsätze der **Wahrheit, Klarheit und fortlaufenden Aufzeichnung**, dh. insbesondere der **Vollständigkeit** unter Beachtung der **Einzelaufzeichnungspflicht**, der **Richtigkeit**, der **Zeitnähe** von Buchungen und Aufzeichnungen, der **Ordnung** und der **Unveränderbarkeit**.

Alle genannten Grundsätze müssen während der Dauer der Aufbewahrungsfrist **nachweisbar** erfüllt werden.

Daher müssen auch die Verarbeitung der einzelnen Geschäftsvorfälle[330] sowie das dabei angewandte Buchführungs- oder Aufzeichnungsverfahren nachvollziehbar sein. Die Buchungen und die sonst erforderlichen Aufzeichnungen müssen durch einen Beleg nachgewiesen sein oder nachgewiesen werden können (**Belegprinzip**). Und die einzelnen Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung **lückenlos verfolgen** lassen (**progressive und retrograde Prüfbarkeit**). Sie sind vollzählig und lückenlos aufzuzeichnen (Grundsatz der **Einzelaufzeichnungspflicht**; vgl. AEAO zu § 146 AO Nr. 2.1), wobei die Aufzeichnung jedes einzelnen Geschäftsvorfalls nur dann nicht zumutbar ist, wenn es technisch, betriebswirtschaftlich und **praktisch unmöglich** ist, die einzelnen Geschäftsvorfälle aufzuzeichnen.[331] Das Vorliegen dieser Voraussetzungen ist ggf. von den Steuerpflichtigen nachzuweisen.

Vor diesem Hintergrund ist es ein **entscheidendes Merkmal einer guten digitalen Lösung**, dass sie es ermöglicht, jeden in ihrem Rahmen erfolgenden und erheblichen Geschäftsvorfall im genannten Sinne nachvollziehbar aufzeichnen und belegen zu können. Sofern einschlägig, sollte beispielsweise der **gesamte Prozess einer Vertragsabwicklung** von dem sie begründenden Klick der Nutzerin/des Nutzers ggf. über die Leistungsabwicklung bis hin zur Zahlung durch die Anwendung selbst dokumentiert sein. Hierzu kann es erforderlich und oder sachgemäß sein, dass die Anwendung (beispielsweise als Vor- oder Nebensystem) in der Lage ist, **zweckentsprechend mit einer anderen Software zu kommunizieren**. Das eingesetzte System ist schließlich angemessen zu sichern und gegen unberechtigte Eingaben und Veränderung zu schützen. Es muss ferner die Gewähr dafür bieten, dass alle relevanten Informationen (Beleg, Grundaufzeichnung, Buchung) nicht unterdrückt oder ohne Kenntlichmachung (Protokollierung) überschrieben, gelöscht, geändert oder verfälscht oder durch neue ersetzt werden. Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben.

Je nach Einsatz der Anwendung kann sich empfehlen, ihre GoBD-Fähigkeit **unabhängig testieren** zu lassen.

[328] Vgl. zu den zu beachtenden Grundsätzen das BMF-Schreiben vom 29. November 2019 zu den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) (https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf?__blob=publicationFile&v=12 – zuletzt abgerufen am 14. Juli 2020). Mit dem BMF-Schreiben werden die GoBD neugefasst. Es tritt an die Stelle des BMF-Schreibens vom 14. November 2014, BStBl I S. 1450.

[329] vgl. BFH-Urteil vom 24. Juni 2009, BStBl II 2010 S. 452.

[330] Geschäftsvorfälle sind alle rechtlichen und wirtschaftlichen Vorgänge, die innerhalb eines bestimmten Zeitabschnitts den Gewinn bzw. Verlust oder die Vermögenszusammensetzung in einem Unternehmen dokumentieren oder beeinflussen bzw. verändern (z. B. zu einer Veränderung des Anlage- und Umlaufvermögens sowie des Eigen- und Fremdkapitals führen).

[331] BFH-Urteil vom 12. Mai 1966, IV 472/60, BStBl III S. 371.

C.2.1 CHECKLISTE GoBD

- Sind sämtliche einschlägige Aufzeichnungspflichten (allgemein HGB, nach Rechtsform und branchenspezifisch) beachtet worden?
- Wird dem Belegprinzip, der progressiven und retrograden Prüfbarkeit wie auch der Einzelaufzeichnungspflicht Rechnung getragen?
- Wird dabei den Prinzipien der Wahrheit, Klarheit, Vollständigkeit, Richtigkeit, Zeitnähe, Ordnung und Unveränderbarkeit Rechnung getragen?
- Ist die Kompatibilität der Lösung sichergestellt?

C.3 EINBEZIEHUNG DER MITARBEITENDEN-VERTRETUNG (MAV)

Aufgabe der MAV ist es, die Rechte der Mitarbeitenden zu wahren. Bei Ausführung dieser Tätigkeit hat natürlich auch die MAV die Einhaltung der Regeln des Datenschutzes sicherzustellen. Darum geht es an dieser Stelle aber nicht.[332] Es geht vielmehr darum, dass der MAV bei Einführung digitaler Lösungen Mitbestimmungsrechte zustehen können. Beim Einsatz digitaler Lösungen geht es insoweit darum, den Einsatz der Technik so mitzugestalten, dass den Arbeitnehmer*innen keine Nachteile entstehen. Es sollte daher bei der Einführung einer jeden technischen Lösung, die sich auf den Arbeitsablauf der Beschäftigten auswirkt, die **MAV in die Planung** einbezogen werden. Deren Ablehnung der Einführung einer Neuerung aufgrund mangelnder Information kann durch die frühzeitige und kooperative Einbeziehung häufig vermieden werden. Dies ist im Hinblick auf Fragen des Datenschutzes hilfreich, betrifft aber natürlich auch weitere Bereiche. So kann etwa auch die Freigabe von im Internet zu platzierenden Inhalten problematisch sein, wenn aufgrund einer hierarchischen Struktur ein besonderes Protokoll einzuhalten ist.

Im Hinblick auf die Digitalisierung kann sich insbesondere im Hinblick auf § 40 lit. h, i und j Mitarbeitervertretungsgesetz der EKD die **Notwendigkeit der Mitbestimmung** ergeben. Das Mitbestimmungserfordernis nach lit. j kann ggf. dadurch ausgeschlossen werden, dass eine **Überwachung der Mitarbeitenden** ohne wesentliche technische Veränderung der eingesetzten Software nicht stattfinden kann. Dies ist der Vertretung in geeigneter Form nachzuweisen.[333]

Ggf. ist hinsichtlich der Nutzung einer bestimmten Anwendung auch eine Dienstvereinbarung abzuschließen, die durch eine Rahmendienstvereinbarung/Betriebsvereinbarung vorbereitet werden kann. **Ziele und Modi des Einsatzes**, das **Verfahren zur Beteiligung und Mitbestimmung** sowie der **Datenschutz** sind darin im Wesentlichen zu beschreiben. Auch Empfehlungen zu Arbeitszeiten und psychischen Belastungen, die mitunter aus Leistungsverdichtungen und -erweiterungen resultieren, aber sich auch aus Veränderungen der Arbeitsgestaltung wie im Rahmen des Agilen Arbeitens ergeben können, können angebracht sein. Sowohl in diesen Vereinbarungen als auch in den Nutzungsbestimmungen/-bedingungen einer dienstlich einzusetzenden Software sollte immer ausdrücklich klargestellt und zugesichert werden, dass die Software **nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeitenden verwendet** wird.

[332] Siehe hierzu etwa den Flyer des Beauftragten für Datenschutzes des EKD (https://datenschutz.ekd.de/wp-content/uploads/2019/10/Flyer-MAV-und-Datenschutz_Druck.pdf - zuletzt abgerufen am 13. Juli 2020).

[333] Um die eigene Kompetenz zu vertiefen, wird der MAV in geeigneten Fällen die Kooperation mit der Datenschutzbeauftragten suchen.

Problem: informelle Einführung neuer Anwendungen
Ein besonderes Problem stellt die informelle Einführung neuer Software dar. Zwar haben viele Organisationen die Installation von Software auf betriebseigenen Geräten sperren lassen, so dass sie nur über die IT-Abteilung erfolgen kann. Allerdings betrifft dieser Vorbehalt zum einen nur dienstliche Geräte und erstreckt sich zum anderen nicht auf Web-basierte Anwendungen. Das kann dazu führen, dass einzelne Mitarbeitende aus eigenem Antrieb neue Lösungen ausprobieren und anwenden. Dadurch kann auch für andere Mitarbeitende der Druck entstehen, die betreffende Anwendung ebenfalls zu nutzen. Spätestens an dieser Stelle ist an eine Beteiligung der MAV zu denken.[334]

C.3.1 CHECKLISTE EINBEZIEHUNG DER MITARBEITENDEN-VERTRETUNG (MAV)

- Ist die MAV frühzeitig über die Einführung der Lösung informiert und ggf. in die Planung einbezogen worden?
- Ist geprüft worden, ob ein Mitbestimmungserfordernis besteht?
- Kann ein Mitbestimmungserfordernis ggf. durch technische Veränderungen ausgeschlossen werden?

C.4 RECHTS- UND ORGANISATIONS-FORMEN

Für die Umsetzung der Anwendung muss eine angemessene Form gefunden werden. In einigen Fällen ist es zwar möglich und angezeigt, die Anwendung im Rahmen der bestehenden Organisation ohne weitere erhebliche Veränderungen etwa als „Projekt“ aufzusetzen. Der für einen erfolgreichen und **nachhaltigen Betrieb einer digitalen Anwendung** vorauszusetzende Aufwand darf aber **weder in finanzieller noch in personeller Hinsicht unterschätzt** werden. Schon das Aufsetzen einer Lösung kann so anspruchsvoll sein, dass es die Möglichkeiten der bestehenden Struktur überfordert. Darüber hinaus ist immer zu bedenken, dass der **langfristige Erfolg** einer Anwendung auch dadurch bestimmt wird, wie gut sie **technisch und inhaltlich gepflegt**, also insbesondere an die sich **verändernden Bedingungen** und Ansprüche angepasst wird. Im Ergebnis wird daher die Einbettung der Anwendung in die Regelstrukturen nicht immer sinnvoller Weise möglich sein. Eine gute Bestandsaufnahme, Zielbestimmung und Planung sind elementar und können zu der Entscheidung führen, eine Anpassung der Struktur vorzunehmen.

Es kann sich in diesem Zusammenhang anbieten, Erstellung und/oder Betrieb der Anwendung in **eine eigene Organisation** auszugliedern. Dabei stellen sich Fragen der Form, insbesondere zur Rechtsform der Organisation. Die in der Sozialwirtschaft anzutreffenden Rechts- und Organisationsformen sind vielfältig und auch einem stetigen Wandel unterzogen.[335]

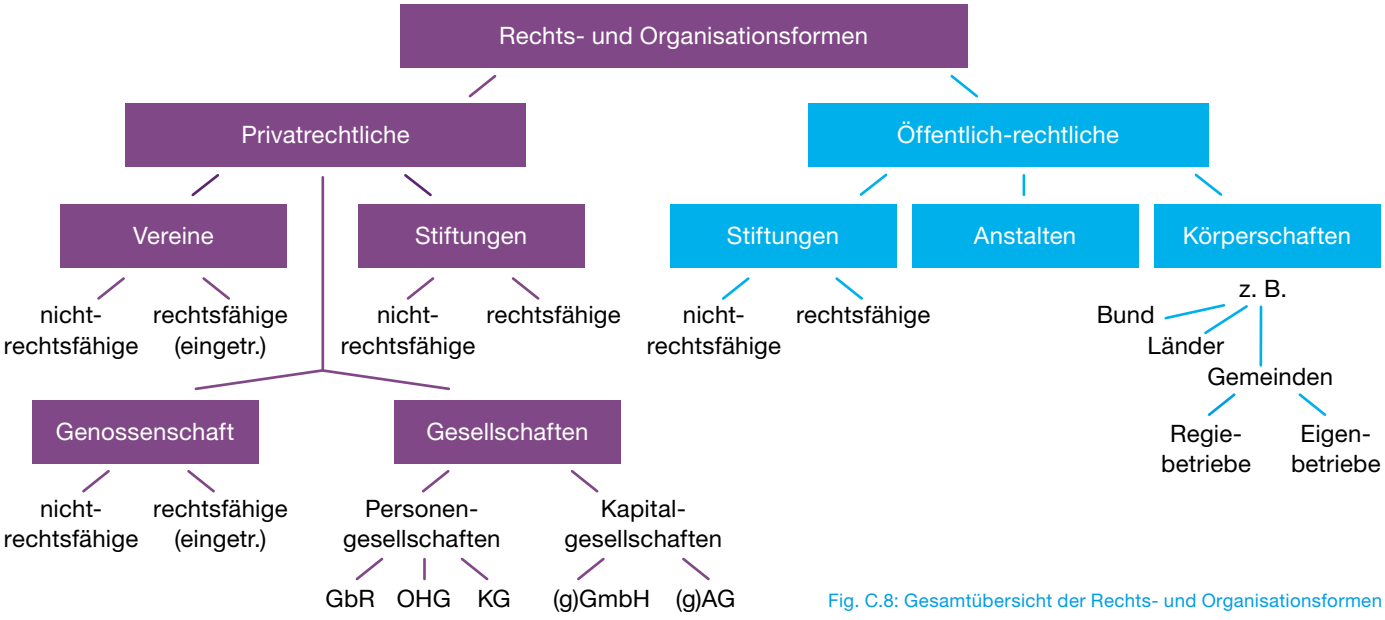


Fig. C.8: Gesamtübersicht der Rechts- und Organisationsformen

[334] Sofern personenbezogene Daten verarbeitet werden, ist die Datenschutzbeauftragte an sich bereits im Vorfeld zu konsultieren, was aber regelmäßig nicht der Fall sein wird. Problematisch kann es ferner sein, wenn Mitarbeitende sich ein Nutzerkonto bei einem Online-Dienst einrichten sollen, der – wie beispielsweise Google bei der Nutzung von Google-Docs – anlässlich dessen auch Informationen über private Konten und Geräte verarbeiten kann.

[335] Zwar entzieht sich die Wertbestimmung gemeinnütziger Organisationen weitgehend den im kaufmännischen Bereich üblichen Bewertungskriterien. Auch ist durch die enge Bindung des Vermögens an den steuerbegünstigten Zweck eine Kapitalisierung der Ertragskraft für die Unternehmensbewertung nur beschränkt tauglich. Gleichwohl kommt gemeinnützigen Organisationen eine erhebliche gesamtwirtschaftliche Bedeutung zu.

C.4.1 ORGANISATIONS-, FINANZ- UND HAFTUNGS-VERFASSUNG

Die **wesentlichen Fragestellungen**, die im Hinblick auf die Wahl der „richtigen“ Rechts- und Organisationsform zu stellen sind, lassen sich nach den Bereichen des **Aufbaus** (Organisationsverfassung), der **Finanzierung** (Finanzverfassung) und der **Haftung** (Haftungsverfassung) unterscheiden.

Die Vorgaben zur Entscheidungs- und Handlungsfähigkeit begründen die Organisationsform. Organe, Zuständigkeiten und Willensbildung sind insoweit zu bestimmen. Die Satzung bzw. der Gesellschaftsvertrag treffen hierzu Bestimmungen, die Kompetenzen und Verantwortlichkeiten definieren. Gemeinhin gilt dabei der Grundsatz, dass die Kompetenz die Verantwortlichkeit mit sich bringt. Die so getroffene Ausgestaltung der Geschäftsführungsorgane bilden den Ausgangspunkt für die Organisation des Aufbaus der gesamten Organisation.

Im Hinblick auf **Organzuständigkeiten** sind die Eigentümer-/Trägerfunktionen von denen der Geschäftsführungs- und Aufsichtsfunktion zu unterscheiden. Erstere bestimmen grundlegende Existenz- und Strukturfragen der Organisation, Letztere die Durchführung[336] und Überwachung der laufenden Geschäfte und sonstigen Aktivitäten der Organisation. Die praktische Aufsicht obliegt dabei entweder den Eigentümerinnen/Trägerinnen (insbesondere der Gesellschafter- oder Mitgliederversammlung) selbst oder wird auf ein weiteres Organ übertragen, etwa einem Bei-, Verwaltungs-, Aufsichtsrat oder Ausschuss.

Fragen der **Finanzierung und Finanzverfassung** betreffen insbesondere das zur Gründung vorauszusetzende Kapital. Dieses hängt wesentlich zunächst von der konkret gewählten Rechtsform ab, worauf (C.4.8) noch näher einzugehen ist, aber ganz entscheidend auch von dem verfolgten geschäftlichen Zweck. Bei Kapitalgesellschaften gilt ein strenger **Kapitalerhaltungsgrundsatz**. Im Sinne des Gläubigerschutzes verbietet dieser, das erforderliche Mindestkapital auszukehren.

Die **Haftung** der Geschäftsleistung ist **grundsätzlich verschuldensabhängig**. Im Rahmen einer Gesamtgeschäftsführungsbefugnis, wenn also mehrere Personen zur Geschäftsleitung bestimmt sind, haften grundsätzlich[337] alle der Geschäftsleitung angehörigen Personen (i.e. Geschäftsführer und Vorstände) gemeinsam gesamtschuldnerisch.[338] Eine Haftungserschwerung gibt es dagegen beim **nichtrechtsfähigen Verein**, bei dem die den Verein rechtsgeschäftlich vertretene Person generell und **ohne Rücksicht auf Verschulden** für sämtliche Verbindlichkeiten des Vereins – neben diesem –[339] haftet. Ebenso **haften dessen Mitglieder persönlich akzessorisch**, also automatisch neben dem Verein, sofern es sich um einen nichtrechtsfähigen (Wirtschafts-)Verein handelt, der ein kaufmännisches Handelsgewerbe betreibt.

C.4.2 RECHTSFÄHIGKEIT

Der Begriff der Rechtsfähigkeit bezeichnet die Möglichkeit einer Organisation, Trägerin von Rechten und Pflichten zu sein. Diese Fähigkeit kommt nicht nur natürlichen Personen zu, sondern originär auch juristischen Personen und – nach der Rechtsprechung – sogar der Gesellschaft bürgerlichen Rechts (GbR) und (daher) auch dem nichtrechtsfähigen Verein die wie Personenhandelsgesellschaften (OHG, KG, GmbH & Co. KG) klagen und verklagt werden können. Alle letztgenannten gelten aber nur als **teilrechtsfähig**.[340]

C.4.3 GESELLSCHAFTEN, VEREIN, STIFTUNG UND GENOSSENSCHAFTEN

Wie bereits gesehen, lassen sich die privatrechtlichen Organisationsformen in Personen- und Kapitalgesellschaften, rechtsfähige (dh. eingetragene) und nichtrechtsfähige Vereine, Stiftungen sowie Genossenschaften unterteilen.

Sowohl im Rahmen von **Personen- (GbR, [OHG, KG][341]) wie auch Kapitalgesellschaften (GmbH, AG, [KGaA][342]**) schließen sich mehrere (natürliche und/oder juristische) Personen zur Verfolgung eines gemeinsamen Zwecks, dem Gesellschaftszweck, zusammen. Im Rahmen dieses Zusammenschlusses halten alle Gesellschafterinnen Gesellschaftsanteile, die grundsätzlich übertragbar, insbesondere vererbbar, sind.

Auch im **Verein** schließen sich (natürliche und/oder juristische) Personen zusammen. Sie verfügen aber im Gegensatz zur Gesellschaft nicht über Anteilsrechte. Ihnen kommen allerdings Mitgliedschaftsrechte zu, die aber grundsätzlich nicht übertragbar sind.

Gänzlich anders ist wiederum die Rechtsform der **Stiftung** geraten. Diese kennt weder Gesellschafter noch Mitglieder. Die Stiftung gehört sich als selbständiges Vermögen gewissermaßen selbst. Die Kombination von Zweck und einem

[336] Der Geschäftsführung bzw. dem Vorstand obliegt sowohl die Führung der Geschäfte nach innen (Geschäftsführung im engeren Sinne) wie auch nach außen ([rechtliche] Vertretung).
[337] Ausnahmen können sich gegenüber den Eigentümern/der Trägerschaft dann ergeben, wenn ein Geschäftsverteilungsplan konkrete Zuständigkeiten vorsieht.
[338] Eine wichtige Haftungserleichterung existiert im ehrenamtlichen Bereich. Ehrenamtliche Vorstände haften nur für Vorsatz und grobe Fahrlässigkeit.
[339] Nach der Gesamthandlehre ist der nichtrechtsfähige Verein als Rechtssubjekt selbst Vertragspartner und Schuldner.
[340] Vgl. zu einer derzeit diskutierten Reform des Gesellschaftsrechts – auch zum Vereinsrecht – den Mauracher Entwurf..
[341] OHG und KG spielen wohl selten eine Rolle im gemeinnützigen Bereich.
[342] Die KGaA spielt wohl selten eine Rolle im gemeinnützigen Bereich.

zur Zweckerreichung ausreichendem Vermögen sind ihre Wesensmerkmale.

Die **Genossenschaft** ist eine Gesellschaft mit nicht geschlossener (dh. freier und wechselnder) Mitgliederzahl, deren Zweck darauf gerichtet ist, den Erwerb oder die Wirtschaft ihrer Mitglieder oder deren soziale oder kulturelle Belange durch einen gemeinschaftlichen Geschäftsbetrieb zu fördern, § 1 Abs. 1 GenG.

C.4.4 PERSONEN (HANDELS-) GESELLSCHAFTEN

Personengesellschaften umfassen neben der Grundform der Personengesellschaft der Gesellschaft bürgerlichen Rechts (GbR) oder BGB-Gesellschaft auch die Personenhandelsgesellschaften, zu denen die OHG und die KG gehören.

Auch die **GmbH & Co. KG** ist (nur) eine KG, also keine Kapitalgesellschaft, obwohl ihre Komplementärin eine GmbH ist. Ihr Konstrukt ist ursprünglich Ausdruck der **Kombination** von Elementen der Haftungsbeschränkung (GmbH als persönlich haftende Geschäftsführerin/Gesellschafterin) und Steueroptimierung (Personengesellschaft).

C.4.4.1 Insbesondere GbR

Für die **Sozialwirtschaft** ist die GbR von **wesentlicher Bedeutung**. Aufgrund der geringen konstitutiven Anforderungen – sie kann beispielsweise ganz formlos entstehen und benötigt kein Mindestkapital – kommt sie häufig auch ganz unerkannt zustande, obwohl sie erhebliche rechtliche, insbesondere auch steuerrechtliche Auswirkungen haben kann. So kann sie Umsatzsteuersubjekt sein und sogar für ihre steuerbegünstigten Gesellschafterinnen die Gefahr begründen, einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb zu führen.

Der Vorteil, dass für die Gründung einer GbR **kein Mindestkapital** vorauszusetzen ist, wird mit dem Nachteil erkauft, dass jede Gesellschafterin grundsätzlich **persönlich mit ihrem gesamten Vermögen für Verbindlichkeiten der GbR haftet**. Die den Gesellschafterinnen obliegende Treupflicht verpflichtet auf ein Verhalten, das sich – unter Berücksichtigung schutzwürdiger Eigeninteressen – am Gesellschaftsinteresse messen lassen muss.

Im Gesellschaftsvertrag werden regelmäßig Regelungen zur Auflösung der Gesellschaft festgehalten. Dabei ist das Recht auf außerordentliche Kündigung nicht abdingbar.

Gemeinnützigkeitsrechtlich weist die GbR verschiedene Beschränkungen auf, auf die im näher interessierenden Zusammenhang unter C.4.8.6.3 noch näher eingegangen wird.

C.4.5 KAPITALGESELLSCHAFTEN

Kapitalgesellschaften sind vornehmlich die GmbH, die AG sowie die KGaA. Im Zuge der europäischen Integration ist noch die Societas Europaea (SE), die Europäische Gesellschaft hinzugekommen,[343] die im hier interessierenden Zusammenhang bislang keine besondere Bedeutung erlangt hat.

C.4.5.1 GmbH

Die Organisation einer GmbH ist im Vergleich zu anderen Kapitalgesellschaften **flexibler**. Von gesetzlichen Vorgaben kann in einem gewissen Rahmen abgewichen werden, etwa indem neben den gesetzlich vorgeschriebenen Organen **weitere Organe** wie Beirat und Aufsichtsrat zur Seite gestellt werden können. Darüber hinaus liegt ein wesentlicher Vorteil der GmbH gegenüber der AG darin, dass den Gesellschafterinnen eine **Steuerung der Geschäftsführung durch Weisungen unproblematisch** möglich ist. Die Befugnisse der Gesellschafterversammlung sind dabei wie auch im Übrigen **allumfassend**.[344] Nur die Außenvertretung kann ihr nicht übertragen werden. Gleichwohl kann aber Gesellschafterinnen Vertretungsmacht eingeräumt werden, so dass sie jeweils oder gemeinsam im Namen der GmbH handeln können.

Das **Stimmrecht** der einzelnen Gesellschafterinnen bestimmt sich im Regelfall nach der **relativen Höhe der Beteiligung**, was im Gesellschaftsvertrag allerdings auch abweichend geregelt werden kann. Beschlüsse kommen **grundsätzlich durch einfache Stimmenmehrheit** zustande; sehr wesentliche Beschlüsse (zB. Änderungen des Gesellschaftsvertrages oder die Auflösung der Gesellschaft) setzen allerdings eine **qualifizierte Mehrheit** (idR. drei Viertel der Stimmen) voraus.

Das **Stammkapital** einer GmbH beträgt idealiter mindestens € 25.000,--. Es kann in Form einer Bar- oder Sacheinlage erbracht werden. Die Anmeldung zur Eintragung der Gesellschaft kann erst erfolgen, wenn die Sacheinlagen vollständig und die Bareinlagen zumindest zu einem Viertel erbracht sind. Dabei darf zudem ein Gesamtbetrag von € 12.500,-- nicht unterschritten werden.

Die GmbH kann als sogenannte **Unternehmergesellschaft (UG)** auch mit einer geringeren Erstausstattung gegründet werden.[345] Dann muss aber ein Viertel des Jahresüberschusses, gemindert um den Verlustvortrag, in eine gesetzliche

[343] Die dem britischen Recht entstammende Limited (Ltd.) hat in den letzten Jahren – seit Modifikation des deutschen GmbH-Rechts – erheblich an Bedeutung verloren. Der Austritt des Vereinigten Königreichs aus der Europäischen Union wird ihr in Zukunft weiter an Bedeutung nehmen.

[344] Gleichwohl wird in der Praxis häufig der Geschäftsführung ein maximales Maß an Befugnissen eingeräumt.

[345] Durch diese Modifikation des GmbH-Rechts, die auf das Vordringen der britischen Ltd. zurückgeht, ist Letzterer im Wesentlichen wieder der Rang abgelaufen worden.

Rücklage eingestellt werden. Zudem muss die Gesellschaft zum Schutz des Rechtsverkehrs die Tatsache ihrer verminderten Kapitalausstattung in ihrer Firma erkennen lassen, und zwar durch den Zusatz „Unternehmergesellschaft (haftungsbeschränkt)“ oder „UG (haftungsbeschränkt)“.

C.4.5.1.1 Gemeinnützige GmbH (gGmbH)

Die gemeinnützige GmbH ist – wie auch die der gemeinnützigen AG – **keine eigene Rechtsform**. Sie ist eine GmbH, die **zusätzlich** gemeinnützigkeitsrechtliche Anforderungen erfüllt. So ist ihr Vermögen im Wesentlichen an einen gemeinnützigen Zweck gebunden und scheidet eine Ausschüttung der Gewinne an die Gesellschafterinnen grundsätzlich aus. Bei Ausgestaltung der Satzung der gGmbH sollten die **Maßgaben der Mustersatzung** (Anlage 1 zu § 60 AO) Beachtung finden.

C.4.5.1.2 Praxis-Hinweis: Gründung der GmbH

Die GmbH kann zu jedem, nicht verbotenen Zweck gegründet werden. Ihr Gesellschaftsvertrag bedarf der notariellen Beurkundung und muss mindestens enthalten:

- Firma (als Personenfirma [vom Namen der Gesellschafterinnen abgeleitet]; Sachfirma [vom Zweck abgeleitet]; Fantasiefirma oder hybride Gestaltung),
- Gegenstand des Unternehmens (Zweck – jeder gesetzlich zulässige ist Zweck möglich),
- Sitz der Gesellschaft,
- Höhe des Stammkapitals (grundsätzlich mindestens € 25.000,--; mindestens ein Viertel der Stammeinlage, wobei € 12.500 nicht unterschritten werden dürfen; eine Sonderregelung besteht allerdings für Unternehmergesellschaft UG (s.o.); die Einlagen müssen der Geschäftsführung zur freien Verfügung stehen),
- Höhe der von jeder Gesellschafterin auf das Stammkapital zu leistenden Einlage (als Bar- und Sacheinlage möglich; letztere ist angemessen zu bewerten; der Nennbetrag der Stammeinlage beträgt mindestens € 1,--).

Bei Verwendung des gesetzlich definierten Gesellschaftsvertragsmusters kann die GmbH auch im **vereinfachten Verfahren** gegründet werden.

Vor der notariellen Beurkundung besteht nur eine sogenannte **Vorgründungsgesellschaft**, die als bloße GbR anzusehen ist. Mit Beurkundung tritt die **Vorgesellschaft** ins Leben, die GmbH i.Gr. (in Gründung), die bereits Züge rechtlicher Eigenständigkeit aufweist. Während dieser Zeit bestehen Risiken für die für die Gesellschaft Handelnden, insbesondere also den Geschäftsführer, die bis zur Eintragung nach § 11 Abs. 2 GmbHG persönlich in Haftung genommen werden können. Die Gesellschafter müssen zudem Gewähr dafür leisten, dass ihre Einlage zum Zeitpunkt der Eintragung noch vorhanden ist, haften also für eine sich zwischenzeitlich etwaig ergebende Differenz.

Erst mit der Eintragung ins Handelsregister ist die GmbH vollexistent. Die Rechte und Pflichten der Vorgesellschaft gehen automatisch auf sie über.

Im Gegensatz zur Rechtslage bei Verein und Stiftung und Personengesellschaften können bei der GmbH zur **Geschäftsführung nur natürliche Personen** bestellt werden.

Praxis-Tipp:
Bei der Gründung einer **GmbH für gemeinnützige Zwecke sind in Betracht kommende Zuwendungsbedingungen zu beachten**. Einige Zuwendungsgeber verlangen beispielsweise, dass die Geschäftsführung der GmbH weder generell von den sonst üblichen **Beschränkungen des Selbstkontrahierungsverbots (§ 181 BGB)** befreit ist noch gesellschaftsvertraglich zu der Befreiung die Möglichkeit besteht.

C.4.5.2 AG

Von der GmbH unterscheidet sich die AG vornehmlich durch die **Strukturstarre**, die ihr gesetzgeberisch auferlegt ist. So sieht das Aktienrecht die Bildung eines Aufsichtsrates zwingend vor. Die gesetzlichen Bindungen erklären sich vor dem Hintergrund des offeneren Kreises von Investoren, die, anders als bei der GmbH, nur schwer auf die Geschäftsführung einer AG einwirken können. Der Vorstand ist sogar von Weisungen des Aufsichtsrates unabhängig und hat so eine **vergleichsweise stärkere Stellung** als die Geschäftsführung einer GmbH.

Die Gründung einer AG bietet sich klassischer Weise vor allem dann an, wenn **Kapital am Markt aufgenommen** werden soll.

C.4.5.2.1 Gemeinnützige AG

Im **gemeinnützigen Bereich** kann die Gründung aber auch für solche Projekte interessant sein, bei denen Mitarbeitende oder Nutznießer (zB. die Bewohner einer Pflegeeinrichtung) in die Trägerschaft eingebunden werden sollen, **ohne dass sie Mitwirkungs- oder Weisungsrechte** gegenüber der Geschäftsführung haben.[346] Insoweit **unterscheidet sich die AG auch**

[346] Sich aufgrund des Gebots der Selbstlosigkeit möglicher Weise ergebende Beschränkungen sind aber unbedingt zu beachten, soll der Gemeinnützigkeitsstatus nicht gefährdet werden.

erheblich von der Genossenschaft (zu dieser sogleich unter C.4.6.2), die vom Prinzip der Selbstverwaltung durchwirkt ist.

In geeigneten Fällen sollte also auch die Gründung einer gemeinnützigen AG in Betracht gezogen werden. Wie auch bei der GmbH ist die gemeinnützige AG keine gesellschaftsrechtliche Sonderform der Aktiengesellschaft, sondern eine Aktiengesellschaft mit **steuerrechtlichem Sonderstatus**. Um diesen steuerrechtlichen Sonderstatus einer gAG zu begründen, hat die Satzungsgestaltung erhebliche Bedeutung. Sie ist der primäre Maßstab für die Erfüllung des Tatbestandsmerkmals der Gemeinnützigkeit. Bei ihrer Gestaltung sollten die Maßgaben der Mustersatzung (Anlage 1 zu § 60 AO) Beachtung finden.

C.4.6 VEREIN UND GENOSSENSCHAFT

Die Bedingungen für Verein und Genossenschaft haben zwar mitunter Ähnlichkeiten zu denen der Personengesellschaften einerseits und Kapitalgesellschaften andererseits, unterscheiden sich aber im Gesamtbild erheblich.

C.4.6.1 Verein

Der Verein ist ein auf eine gewisse Dauer angelegter und körperschaftlich organisierter Zusammenschluss einer Anzahl von Personen, die ein gemeinschaftliches Ziel verfolgen. Der Hinweis auf die körperschaftliche Struktur macht beim Verein deutlich, dass er **von Ein- und Austritt seiner Mitglieder unabhängig** sein soll, solange die **Mindestanzahl** an Mitgliedern (nach § 56 BGB sind es 7) nicht unterschritten wird.

Bei Vereinen wird der **Idealverein** (§ 21 BGB) und der **wirtschaftliche Verein** (§ 22 BGB) unterschieden. Letzterer ist dadurch gekennzeichnet, dass sein Zweck auf einen wirtschaftlichen Geschäftsbetrieb ausgerichtet ist. Die für die Praxis wichtige **Rechtsfähigkeit** erlangt der Idealverein einfach durch **Eintragung**, wogegen der wirtschaftliche Verein sie nur durch **Verleihung** erhalten kann, die allerdings **selten** erfolgt.[347]

Diese Vereinsklassenabgrenzung hat aber im Zuge der sogenannten **Kita-Rechtsprechung**[348] des BGH immerhin **im nicht am Gewinn orientierten Bereich** erheblich an Bedeutung verloren. Fortan kommt es im Hinblick auf die Eintragungsfähigkeit primär auf den **Vereinszweck** an; dieser heiligt nun quasi die Mittel. Einem ideellen Verein ist damit auch die wirtschaftliche Betätigung **durchaus möglich**. Ob eine solche vorliegt, verliert damit im Ergebnis an Bedeutung. Letztlich ist damit auch die Gemeinnützigkeit des Vereins im Sinne der Vorschriften der AO **keine zwingende Bedingung** (auch wenn ihre eine wesentliche Indizwirkung zukommen kann), da es dem BGH **lediglich auf das Gewinnausschüttungsverbot** ankam.

Vertiefende Anmerkung:
Der BGH-Rechtsprechung gingen mehrere Judikate des Kammergerichts voraus, nach denen einem Verein die Eintragungsfähigkeit abzusprechen war, wenn dieser seinen Vereinszweck entgeltlich verfolgte – wie etwa Kindertagesstätten, die Kinder gegen Entgelt betreuen. Unabhängig vom Vorliegen einer Gewinnerzielungsabsicht sei aufgrund der wesensmäßigen Entgeltlichkeit bereits auf einen wirtschaftlichen Geschäftsbetrieb zu erkennen. Insoweit wurde der steuerrechtlich gegebenen Gemeinnützigkeit die vereinsrechtliche Relevanz abgesprochen.[349]

Der BGH[350] verwies dagegen darauf, dass es sich beim Idealverein nach der Vorstellung des Gesetzgebers vordergründig um das Gegenstück zu den Kapitalgesellschaften handele, deren Zweck gerade auf „Geschäftsgewinn und den wirtschaftlichen Vorteil des Einzelnen abzielt". Dann komme dem steuerrechtlichen Gemeinnützigkeitsstatus immerhin eine **besondere Indizwirkung** zu, die eine Eintragungsfähigkeit anzeigen kann, auch wenn die Gemeinnützigkeit mit der Nichtwirtschaftlichkeit des § 21 BGB nicht zwingend gleichgesetzt werden könne.

Insbesondere verwies der BGH insoweit auf das Merkmal der **Selbstlosigkeit** in § 55 AO sowie das damit verknüpfte **Gewinnausschüttungsverbot** und das Gebot der zeitnahen Mittelverwendung. Auch sei der Umfang des Geschäftsbetriebes unerheblich. Sei die wirtschaftliche Betätigung zur Mittelbeschaffung zulässig, wie es die Entstehungsgeschichte des BGB beweise, könne dem Verein „auch nicht verwehrt werden, den ideellen Zweck unmittelbar mit seinen wirtschaftlichen Aktivitäten zu erfüllen".[351]

Der BGH hat damit im Kern das der Vereinsklassenabgrenzung immanente Verbot der übermäßigen wirtschaftlichen Betätigung **durch ein Gewinnausschüttungsverbot** ersetzt. Das ist im Vereinsrecht ein echter **Paradigmenwechsel**.

[347] Die Unterscheidung der Vereinsklassen rechtfertigt sich grundsätzlich durch das Argument des Gläubigerschutzes. Es besteht nämlich keine Haftung der Vereinsmitglieder für Schulden des Vereins. Wirtschaftliche Tätigkeiten sollen daher grundsätzlich den Personen- und Kapitalgesellschaften vorbehalten werden, die in ihrer Ausgestaltung den Schutz der Gläubiger berücksichtigen. So versteht sich, dass nach der Rechtsprechung des Bundesverwaltungsgerichts einem wirtschaftlichen Verein nur dann die Rechtsfähigkeit zu verleihen ist, wenn er seinen Zweck nicht in zumutbarer Weise auch in der Rechtsform einer Kapitalgesellschaft oder Genossenschaft verfolgen kann.

[348] Beschlüsse vom 16. Mai 2017 – II ZB 7/16 (NJW 2017, S. 1943), II ZB 6/16 und II ZB 9/16.

[349] Eine ausführliche Darstellung der Rechtsprechung des KG durch den zuständigen Berichterstatter Sdorra: npoR 2017, S. 45 ff.

[350] S.o. Fn. 344.

[351] Wenn auch das Ergebnis erfreut, die juristische Überzeugungskraft des Urteils ist vielfach bezweifelt worden, vgl. hierzu die Nachweise bei Leuschner, in MüKo BGB, 8. Aufl. 2018, Rz. 28.

Der Ein- und Austritt der Vereinsmitglieder ist gesetzlich nicht grundlegend geregelt. § 58 BGB sieht in seiner Ziff. 1 vor, dass die Satzung eine entsprechende Regelung treffen soll. In der Praxis sind Regelungen eines schriftlichen Aufnahmeantrags mit nachfolgender Entscheidung durch Vorstand oder Mitgliederversammlung üblich. Da Antragstellende grundsätzlich keinen Anspruch auf Aufnahme in einen Verein haben, kann die Satzung diese noch von weiteren Voraussetzungen abhängig machen. Dazu kann etwa die **Konfessionszugehörigkeit** gehören.

Der **Austritt** kann nach § 39 Abs. 2 BGB dergestalt beschränkt werden, dass er erst zum Ende eines Geschäftsjahres oder unter Einhaltung einer Kündigungsfrist von maximal zwei Jahren möglich ist. Der Austritt aufgrund wichtigen Grundes kann dadurch indes nicht beschränkt werden. Ob ein solcher gegeben ist, entscheidet sich danach, ob dem Mitglied ein Verbleib im Verein bis zum Ablauf der vorgesehenen Kündigungsfrist nach Abwägung aller Umstände des Einzelfalls zumutbar ist. Umgekehrt können Mitglieder bei Vorliegen eines wichtigen Grundes ausgeschlossen werden.

Zur Rechnungslegung bei Vereinen kann auf die Empfehlungen des Instituts der Wirtschaftsprüfer (IDW) verwiesen werden.[352]

C.4.6.1.1 Hauptpflichten und –Rechte der Mitglieder

Hauptpflichten der Mitglieder sind:

- die Erbringung der in der Satzung festgeschriebenen **Beiträge** sowie
- die Pflicht zu loyalem Verhalten.

Die Hauptpflichten der Mitglieder sind:

- das **Stimmrecht** in der Mitgliederversammlung,
- das Recht auf **Einberufung einer außerordentlichen Mitgliederversammlung** (nach § 37 BGB bei mindestens 10% der Stimmen oder abweichend nach Satzung) sowie
- das Recht auf Gleichbehandlung (Gleiches ist nicht ohne Sachgrund ungleich und Ungleiches nicht ohne Sachgrund gleich zu behandeln).

C.4.6.1.2 Aufbauorganisation eines Vereins

Zwingend vorgesehen sind für den Verein lediglich

- **Vorstand**, der den Verein nach außen vertritt, und die
- **Mitgliederversammlung**, die das Vereinsgeschehen grundlegend bestimmt.

Anders als bei der Genossenschaft (zu dieser sogleich unter C.4.6.2) kann beim Verein auch ein **Nichtmitglied** zum Vorstand bestellt werden. Die Satzung kann hiervon aber abweichende Bestimmungen treffen. Die Vorstandsmitglieder werden regelmäßig durch die **Mitgliederversammlung gewählt** (Bestellung durch **Beschluss**). Eine Abberufung ist grundsätzlich **jederzeit** möglich. Unter der Maßgabe des Vorbehalts der Abberufung aus wichtigem Grund (§ 27 Abs. 2 S. 2 2. HS. BGB) ist die Abbedingung der jederzeitigen Abberufung möglich. Es empfiehlt sich, die Beziehungen zum Vorstand durch **einen Arbeits-/Dienstvertrag** zu regeln, was § 27 Abs. 3 BGB möglich macht. Anderenfalls gelten die Bestimmungen des Auftragsrechts. Die Entgeltzahlung an den Vorstand ist nur bei **entsprechender Satzungsvorschrift** zulässig, sonst stellt sie eine Pflichtverletzung dar.

Die **Vertretungsmacht** des Vorstands kann so gestaltet werden, dass bestimmte Verträge die Zustimmung der Mitgliederversammlung oder eines anderen Vereinsorgans (zB. eines von der Satzung bestimmten Aufsichtsrats) voraussetzen. Neben dem Vorstand können nach § 30 BGB aber auch **andere (besondere) Vertreter** bestellt werden (so zB. die hauptberuflichen Geschäftsführenden der Wohlfahrtsverbände). Soll die Vertretungsbefugnis dieser besonderen Vertreter beschränkt werden, ist dies in der Satzung zu bestimmen.

Eine **Auflösung** des Vereins setzt einen entsprechenden **Beschluss** der Mitgliederversammlung voraus.[353] Daneben ist die Mitgliederversammlung umfassend zur Regelung der Angelegenheiten des Vereins berufen, soweit deren Besorgung nicht dem Vorstand oder einem anderen Organ des Vereins übertragen wurde, § 32 Abs. 1 S. 1 BGB. Die **Vorab-Übertragung durch die Satzung ist weitgehend möglich**. Zwingend zuständig bleibt die Mitgliederversammlung neben dem Auflösungsbeschluss auch für **Satzungsänderungen**. Beschlüsse der Mitgliederversammlung können auch im **schriftlichen Verfahren** getroffen werden, § 32 Abs. 2 BGB.

Hinweis:
In der Praxis werden neben Vorstand und Mitgliederversammlung häufig weitere Organe des Vereins begründet, zB. „Beirat“, „Ausschuss“, „Verwaltungsrat“, „Aufsichtsrat“ etc. Dies ist möglich; es muss aber bedacht werden, dass die Vertretungsbefugnis des Vorstands nicht beschnitten wird und dass die Mitgliederversammlung die Kompetenzen auch wieder einziehen kann.

Da sowohl rechtsfähige (eingetragene) und nicht rechtsfähige Vereine anders als Stiftungen und Kapitalgesellschaften **keinerlei Mindestkapital** benötigen, können sie ihren Zweck

[352] Und zwar auf die IDW RS HFA 14 sowie – zu Besonderheiten bei Spenden sammelnden Organisationen – auf die IDW RS HFA 21.

[353] Durch den Auflösungsbeschluss (der auch durch Zeitablauf vermittels eines in der Satzung bestimmten Zeitpunkts ersetzt werden kann) wird der Verein zum Liquidationsverein. Er besteht also zwar fort, sein Zweck ist aber von nun an auf die Auflösung, dh. die Abwicklung von Verträgen, Bereinigung von Schulden und Verwertung der Aktiva beschränkt. Während der Liquidation wird der Verein durch Liquidatoren vertreten. Dabei sind die Mitglieder des Vorstands „geborene“ Liquidatoren, § 48 BGB. Bei gemeinnützigen Vereinen ist insbesondere der Grundsatz der Vermögensbindung zu beachten. Durch öffentliche Bekanntmachung und besondere Mitteilung an bekannte Gläubiger ist die Aufforderung zur Geltendmachung von Forderungen zu publizieren, § 50 BGB. Erst nach Ablauf des Sperrjahres (berechnet nach Bekanntmachung der Auflösung) darf das Vereinsvermögen an den Anfallberechtigten ausgekehrt werden, § 51 BGB.

durch laufende Einnahmen verwirklichen. Ihre **Hauptfinanzierungsquellen** sind

- Mitgliedsbeiträge (auch als Sachleistung möglich) und Umlagen (beide sind in der Satzung zu regeln),
- Spenden und Zuschüsse,
- Entgelte aus wirtschaftlichen Geschäftsbetrieben (zu denen auch die Zweckbetriebe gehören).

Anmerkung:
Auch steuerpflichtige wirtschaftliche Geschäftsbetriebe sind durchaus zulässig, sofern der Zweck des rechtsfähigen Vereins nicht auf diese ausgerichtet ist (sogenanntes Nebenzweckprivileg). Dem Verein kann allerdings die Rechtsfähigkeit wieder entzogen werden, wenn der Zweck zwar nicht auf einen wirtschaftlichen Geschäftsbetrieb gerichtet ist, der Verein diesen aber nicht nur nebenzwecklich verfolgt. Die Ausrichtung auf einen Zweckbetrieb ist aber unproblematisch (zur Abgrenzung siehe genauer unter C.4.8.2.5.5).

Zum Zeitpunkt seiner Gründung muss der Verein **mindestens sieben Mitglieder** haben (§ 56 BGB), und von ebenso vielen ist die Satzung zu **unterschreiben** (§ 59 BGB). Bis zu seiner Eintragung, durch die er die Rechtsfähigkeit erlangt, ist der Idealverein ein sogenannter **Vorverein**. Die Rechtsfähigkeit ist bei weniger als drei Mitgliedern zu entziehen, § 73 BGB. Sofern der Verein keine Mitglieder mehr hat, erlischt er ohne Weiteres.

Die Eintragung ist vom Vorstand in vertretungsberechtigter Zahl durch schriftliche Erklärung vor einer Notarin anzumelden.

Praxis-Tipp:
Die Eintragung des Vereins erfolgt in der Praxis regelmäßig nur unter der Voraussetzung, dass neben den Angaben nach § 57 BGB (Zweck, Name, Sitz des Vereins und Eintragungsbestimmung) auch die Sollangaben nach § 58 BGB gemacht werden (Regelung zu Eintritt und Austritt, zu Beiträgen, zur Bildung des Vorstands und zur Mitgliederversammlung). Um Schwierigkeiten zu vermeiden, sollte die Satzung also mindestens in diesem Sinne umfassend sein.

C.4.6.1.3 Besonderheiten beim nicht rechtsfähigen Verein

Abweichend von § 54 BGB richtet sich die Haftungsverfassung des nicht rechtsfähigen Vereins nicht nach dem Recht der GbR, was eine persönliche Haftung der Mitglieder mit sich brächte, sondern – wie eben auch beim rechtsfähigen Verein – **nach Vereinsrecht**. Die Haftung der Mitglieder ist daher auch bei einem nicht rechtsfähigen Verein, sofern es sich nicht um einen wirtschaftlichen Verein handelt, auf das Vereinsvermögen beschränkt. Allerdings gilt dieses Privileg nicht gleichermaßen auch für den handelnden Vorstand. Dessen Haftung ist **verschuldensunabhängig** gegeben, § 54 S. 2 BGB. Diese **Handelndenhaftung**[354] ist eine gesetzliche Haftung. Daher kann sie nur für den Einzelfall und dann auch (ganz grundsätzlich) nur durch ausdrückliche Vereinbarung mit der Haftungsgegnerin ausgeschlossen werden.[355] Auch kann die Satzung die Handelndenhaftung nicht auf das Vereinsvermögen beschränken.

C.4.6.2 Genossenschaft

Im Vergleich zum Verein etwas geschlossener gestaltet ist die die eingetragene Genossenschaft (eG). Sie gehört weder zu den Personen- noch zu den Kapitalgesellschaften, kann für Gründungsteams durchaus geeignet sein, dient aber vor allem als Kooperationsmodell für mittelständische (gewerbliche) Unternehmen. Sie erlangt als eG mit der Eintragung ins Genossenschaftsregister den Status einer vollrechtsfähigen Körperschaft, wodurch sie gleichzeitig zur juristischen Person und zum Formkaufmann iSd. HGB wird, § 17 GenG. Zuvor stehen ihr die Rechte und Pflichten der eG nicht zu.[356]

Eine nicht eingetragene Genossenschaft ist denkbar, ihre rechtliche Behandlung richtet sich aber weitestgehend nach den Vorschriften für eine GbR bzw. Personenhandelsgesellschaft oder den Verein, da § 13 GenG die Anwendung des GenG im Wesentlichen auf die eG beschränkt.[357]

Hinweis:
Mit dem **Gesetz zu Bürokratieabbau und zur Förderung der Transparenz bei Genossenschaften** vom 17. Juli 2017 hat der Gesetzgeber insbesondere für **kleine Genossenschaften** für einige **Erleichterungen** gesorgt. So steigt die Bilanzsummen-Grenze für die umfangreiche genossenschaftliche Pflichtprüfung des Jahresabschlusses unter Einbeziehung der Buchführung und des Lageberichts von einer auf 1,5 Millionen Euro bzw. von 2 auf 3 Millionen Euro an Umsatzerlösen.

Weiter entlasten soll auch die neu eingeführte **„vereinfachte Prüfung“**: Jede zweite Prüfung soll lediglich die Durchsicht relevanter Unterlagen unternehmen, so dass die umfassende Prüfung somit nur noch alle zwei Jahre ansteht. Diese Vereinfachung gilt für Genossenschaften mit einer Bilanzsumme von maximal 350.000 Euro und jährlichen Umsatzerlösen von bis zu 700.000 Euro

[354] Siehe zu dieser ausführlich Schöpflin, in: Hau/Poseck, BeckOK BGB, 54. Ed. 2020, Rz. 37ff.

[355] Für einen stillschweigenden Ausschluss müssen besondere Gründe vorliegen, die den zwingenden Schluss auf ihn zulassen. Er ergibt sich noch nicht allein daraus, dass kein Beteiligter die persönliche Haftung des Handelnden gewollt oder auch nur erwogen habe. Es empfiehlt sich jedenfalls, den Ausschluss schriftlich zu fixieren.

[356] Solange eine Eintragung in das Genossenschaftsregister beabsichtigt ist, wird sie als Vorgenossenschaft bezeichnet.

[357] Im Zuge der Europäisierung ist noch die Societas Cooperativa Europaea (SCE), die europäische Genossenschaft, möglich geworden, die aber praktisch im hier interessierenden Zusammenhang (noch) keine besondere Rolle spielen dürfte.

(wobei eine der Grenzen überschritten werden kann, solange maximal zehn Arbeitnehmer beschäftigt werden), sofern sie keine Mitgliederdarlehen entgegennehmen dürfen und ihre Satzung eine Nachschusspflicht der Genossinnen ausschließt.

Zudem trägt das Gesetz den veränderten Rahmenbedingungen (zB. dass Genossenschaften und ihre Mitglieder verstärkt das Internet nutzen) Rechnung, passt das Genossenschaftsrecht an die jüngere Rechtsentwicklung im Kapitalgesellschafts- und Vereinsrecht an und entspricht weiteren Bedürfnissen der Praxis. So gilt nun auch zugunsten des Vorstandes einer Genossenschaft die Business Judgment Rule[358] (§ 34 Abs. 1 S. 2 GenG), sind darüber hinaus Haftungserleichterung für ehrenamtlich tätige Vorstände normiert (§ 34 Abs. 2 S. 3 GenG) und die Finanzierung von Investitionen durch Mitgliederdarlehen erleichtert worden (§ 21b GenG).

Die Gründung der eG, bei der der genossenschaftliche Prüfungsverband unterstützen kann,[359] erfolgt durch eine von mindestens drei Mitgliedern abgefasste **Satzung**, die insbesondere Firma, Sitz und Gegenstand der Genossenschaft sowie die Höhe der Einlagen, Rücklagen für Verluste und die Einberufungsformalitäten der Generalversammlung vorsieht.[360] Der Beitritt zu einem Prüfungsverband bei Gründung ist obligatorisch.

Die Organisationsform Genossenschaft dient per se der Förderung des Erwerbs oder Wirtschaft der Mitglieder bzw. deren sozialen und kulturellen Belangen durch einen gemeinschaftlichen Geschäftsbetrieb. Der **genossenschaftliche Förderzweck** bildet das „charakteristische Merkmal der Rechtsform“[361] einer Genossenschaft. Insbesondere aufgrund ihrer sozialpolitischen Bedeutung erfreut sich die Genossenschaft einiger **Privilegien** und kann sich auch in steuerlicher Hinsicht attraktiv zeigen.[362]

Ein großer Vorteil einer eG liegt insbesondere darin, dass **kein Mindestkapital** vorgeschrieben ist, so dass es auch an einer Mindesthöhe der Einlagen fehlt. Ein weiterer großer Vorteil der Genossenschaft ist der **freie, jederzeit mögliche Eintritt** neuer Mitglieder und Austritt nicht mehr interessierter Mitglieder – ähnlich dem Verein. Den Ein- und Austritt kann die Genossenschaft selbst unkompliziert regeln, ohne dass es der Einschaltung eines Notars oder Registergerichts bedarf. Im Gegensatz dazu entstehen etwa bei der GmbH für den Ein- und Austritt von Gesellschafterinnen nicht unerheblicher Aufwand und Kosten. Die **Mitgliederzahl** der Genossenschaft ist gesetzlich nach oben nicht begrenzt, kann aber durch Satzung beschränkt werden. Die Mitgliedschaft wird durch Gründung oder schriftlichen Beitritt erworben.

Mindestens **drei Personen** sind für Gründung und Aufrechterhaltung der Genossenschaft erforderlich, § 4 GenG. Eine **kurzfristige Unterschreitung** der Mindestmitgliederzahl ist dann unschädlich, wenn die notwendige Anzahl spätestens zum Zeitpunkt der gerichtlichen Entscheidung über die Auflösung der Genossenschaft (§ 80 GenG) wieder erreicht ist.

Gewinne darf die Genossenschaft **nicht als Selbstzweck**, wohl aber zugunsten des Förderzwecks erzielen. Deren Rückvergütung an die Genossinnen erfolgt steuerfrei. Für ihre Verbindlichkeiten haftet das Vermögen der Genossenschaft, § 2 GenG. Eine **Nachschusspflicht** der Genossinnen ist aber möglich, sofern deren Haftung durch die publizierte Satzung nicht **auf die Einlage beschränkt** ist, vgl. § 6 Ziff. 3 GenG. Gleiches gilt auch im Falle der Insolvenz.

Ein für die Genossenschaft wesentliches Prinzip ist das der **Selbstverwaltung/Selbstorganschaft**. Gemäß § 9 Abs. 2 S. 1 GenG müssen die Mitglieder des **Vorstands** und des **Aufsichtsrats** natürliche Personen und vor allem Mitglieder der Genossenschaft sein. Eine Genossenschaft kann im Übrigen streng demokratisch bestimmt werden.[363] Ihr oberstes Organ ist die **Generalversammlung**, die dem Vorstand jedenfalls bei kleineren Genossenschaften von bis zu 20 Mitgliedern unproblematisch Weisungen erteilen kann, sofern die Satzung dies vorsieht, § 27 Abs. 1 S. 3 GenG. Damit ist dann die Generalversammlung das „oberste“ Geschäftsleitungsorgan, ihre Beschlüsse binden den Vorstand. Sie müssen aber so unmissverständlich formuliert sein, dass ihnen der Weisungscharakter eindeutig zu entnehmen ist.

Praxis-Tipp:
Entscheidet sich eine kleine eG mit bis zu 20 Genossinnen zu einer entsprechenden Engführung der Befugnisse des Vorstands, sollte im Hinblick auf § 43 Abs. 7 S. 1 GenG zugleich die Schriftform bzw. elektronische Form der Beschlüsse der Generalversammlung festgeschrieben werden.

Beschlüsse trifft die Generalversammlung grundsätzlich mit einfacher Mehrheit. Für außerordentliche Beschlüsse, etwa über eine Satzungsänderung oder die Auflösung, ist eine qualifizierte Mehrheit von drei Vierteln der Stimmen notwendig.

[358] Es spricht viel für eine umfassende Einführung der Business Judgment Rule in das Gemeinnützigkeitsrecht, so dass den Organen gemeinnütziger Organisationen mehr Rechtssicherheit bei in gutem Glauben getroffenen Entscheidungen gewährt werden kann. Das betrifft Entscheidungen, die ex-post betrachtet als Fehler, ex ante aber als vertretbar erscheinen. Die Diakonie Deutschland setzt sich mit weiteren Verbänden für eine entsprechende Einführung ein. Die derzeit diskutierte Stiftungsrechtsreform sieht dies beispielhaft vor.

[359] Die Einholung dieser Unterstützung ist grundsätzlich sehr anzuraten. Die Prüfungsverbände bieten eine umfassende Betreuung und Beratung auch bereits im Vorfeld der Gründung, etwa bei der Satzungserstellung und bei der Vorbereitung der ersten Generalversammlung. Die Geschäftsführungsprüfung der Verbände (als Kompensation für fehlendes Mindestkapital und Haftung der Genossinnen) ist zudem keine bloße Last, sondern entlastet den häufig ehrenamtlich tätigen Aufsichtsrat; das beim Prüfungsverband eingesetzte Personal hat spezielle Kenntnisse und Erfahrungen im Genossenschaftsbereich, die Prüfung ist auf die besonderen Verhältnisse bei Genossenschaften zugeschnitten.

[360] Der Mindestinhalt der Satzung ist gesetzlich vorgeschrieben, siehe § 6ff. GenG.

[361] BT-Drs. 16/1025, S. 81.

[362] Siehe überblicksweise das Merkblatt zur Steuerpflicht von Genossenschaften bei Neugründungen des Genossenschaftsverbands, https://www.genossenschaftsverband.de/site/assets/files/30787/7_-_merkblatt_steuerpflicht.pdf (zuletzt abgerufen am 24. Juli 2020).

[363] In der Praxis wird allerdings zunehmend eine Fixierung der Kompetenzen beim Vorstand wahrgenommen. Siehe hierzu etwa Beuthien: Entfernen sich zu viele Genossenschaften von ihrer Leitidee?, ZRP 2019, S. 108 ff.

Während in Kapitalgesellschaften in der Regel die Gesellschafterin mit der größten Beteiligung auch den größten Einfluss hat, funktioniert die gemeinnützige Genossenschaft anders: Unabhängig vom eingesetzten Kapital hat **jedes Mitglied eine Stimme**. Insoweit ähnelt die gemeinnützige Genossenschaft dem Verein, bei dem ebenfalls das Prinzip „ein Kopf, eine Stimme“ gilt.

Zu den **Organen** der eG gehört neben dem **Vorstand** (Geschäftsführung und Außenvertretung) und der **Generalversammlung** (u.a. Feststellung des Jahresabschlusses, Weisungen) wie bereits erwähnt auch der **Aufsichtsrat** (Überwachung des Vorstands). Er hat nach § 38 GenG gegenüber dem Vorstand umfangreiche Befugnisse, wird von der Generalversammlung gewählt und besteht gesetzlich aus drei Mitgliedern, sofern die Satzung keine höhere Zahl festlegt, § 36 Abs. 1 S. 1 GenG. Erneut gibt es hier aber **Sonderbedingungen für kleine Genossenschaften**: Bei bis zu 20 Mitgliedern genügt ein Vorstandsmitglied, um die Geschäfte der Genossenschaft zu führen, § 24 Abs. 2 S. 3 GenG, und auf einen Aufsichtsrat kann ganz verzichtet werden, § 9 Abs. 1 S. 2 GenG. Die Rechte und Pflichten des Aufsichtsrats werden in diesem Fall grundsätzlich unmittelbar durch die Generalversammlung wahrgenommen, § 9 Abs. 1 S. 3 GenG.

Für kleinere Genossenschaften (gemessen an der Anzahl der Mitglieder bzw. der Bilanzsumme) gelten zudem vereinfachte Bestimmungen zur Jahresabschlussprüfung und zum Aufsichtsrat, vgl. § 9 Ab. 1 S. 2 sowie § 53 GenG. Der für eine Jahresabschlussprüfung zu betreibende Aufwand ist dem einer GmbH vergleichbar.

C.4.6.2.1 Genossenschaft und Gemeinnützigkeit

Die Genossenschaft kann die Förderung des Allgemeinwohls oder des Wohls von Nichtmitgliedern **nicht** zu ihrem Hauptzweck machen. Die Genossenschaft ist ihrer Natur nach quasi auf **Genossinnennützlichkeit** angelegt. Allerdings muss der Hauptzweck der Mitgliederförderung nicht der **Endzweck** sein. Daher kann die Genossenschaft vermittels der Förderung ihrer Mitglieder unter den Voraussetzungen der §§ 51–68 AO durchaus einen **gemeinnützigen Endzweck** iSd. §§ 52–54 AO verfolgen.[364] Da dies allerdings noch teilweise in Zweifel gezogen wird,[365] ist der Weg noch nicht gesichert, erfolgreiche Gestaltungen entsprechend selten.

Der gemeinnützige Endzweck muss bei der gemeinnützigen Genossenschaft jedenfalls in der Satzung verankert sein und selbstlos iSd. § 55 Abs. 1 AO sowie ausschließlich iSd. § 56 AO verfolgt werden. In der Satzung ist entsprechend die Gewinnauskehrung wie auch die spätere Auszahlung von Vermögensmehrungen an ausscheidende Mitglieder auszuschließen. Eine enge Abstimmung mit der Finanzverwaltung ist zu empfehlen.

Praxis-Tipp:
Die Ausgestaltung der Satzung ist bei angestrebter Gemeinnützigkeit besonders sorgfältig vorzunehmen. Eine frühzeitige Abstimmung mit dem zuständigen Finanzamt ist unbedingt zu empfehlen. In vier Schritten erfolgt so in der Regel die Gründung einer gemeinnützigen Genossenschaft:

1. Entwurf der Satzung;
2. Abstimmung mit dem zuständigen Finanzamt;
3. Gründungsprüfung durch den Prüfverband;
4. Anmeldung und Eintragung ins Genossenschaftsregister.

C.4.7 STIFTUNG[366]

Mit (gemeinnütziger) GmbH und den Vereinen gehört die Stiftung zu den in der Sozialwirtschaft am häufigsten genutzten Rechtsformen. Nicht selten wird ihre Rechtsform beispielsweise zur Begründung einer Holdingstruktur genutzt.

Grundlegende Vorschriften zum Stiftungsrecht bilden die §§ 80ff. BGB. Landesstiftungsgesetze regeln daneben das Verfahren zur stiftungsrechtlichen Anerkennung und die Aufsicht. Da der Bundesgesetzgeber den Ländern insoweit einen gewissen Spielraum gelassen hat, regeln die Landesstiftungsgesetze mitunter auch einige inhaltliche Fragen, die beispielsweise bei der Abfassung der Satzung (vom Gesetzgeber „Stiftungsverfassung“ genannt) zu beachten sind. Allerdings sind die Voraussetzungen, unter denen eine Stiftung Rechtsfähigkeit erlangt, seit dem Inkrafttreten des Gesetzes zur Modernisierung des Stiftungsrechts im BGB **bundeseinheitlich und abschließend** bestimmt. Liegen also die drei in § 80 Abs. 2 BGB genannten Voraussetzungen vor, so besteht ein Anspruch auf Anerkennung. Es ist daher nicht zulässig, die Anerkennung der Stiftung durch Landesgesetz von weiteren Erfordernissen abhängig zu machen. Landesvorschriften über kirchliche oder ihnen gleichgestellte Stiftungen bleiben jedoch unberührt, § 80 Abs. 3 BGB.

Praxis-Hinweis:
Das Auseinanderfallen der stiftungsrechtlichen Kompetenzen in Landes- und Bundeszuständigkeit ist dem (historisch begründeten) Umstand geschuldet, dass

[364] Dies zumal wenn die Förderung ihrer Mitglieder selbst im Interesse der Allgemeinheit liegt.
[365] Vgl. die Nachweise bei Geibel in Henssler/Strohn, Gesellschaftsrecht, 4. Aufl. 2019, Rz. 7 zu § 1 GenG.
[366] Es ist mit einer Reform des Stiftungsrechts zu rechnen. Ein Schwerpunkt der Reform ist nach dem Entwurf die Einführung eines deklaratorischen Stiftungsregisters mit Publizitätswirkung. Es soll beim Bundesamt für Justiz geführt werden. Der Wegfall der bisherigen Vertreterbescheinigung erleichtert die Teilnahme einer Stiftung am Rechtsverkehr. Weitere Schwerpunkte sind die Möglichkeit zur Umwandlung einer Stiftung in eine Verbrauchsstiftung sowie die einheitliche Regelung der Voraussetzungen und des Verfahrens bei Zu- und Zusammenlegung von Stiftungen, Erleichterungen bei Satzungsänderungen sowie Regelungen zum Stiftungsvermögen, insbesondere dem Grundstockvermögen einer Stiftung. Die geplante Einführung der Business Judgment Rule erhöht die Rechtssicherheit für die Organe und bewirkt eine Stärkung des Ehrenamtes.

dem Bundesgesetzgeber die Kompetenz für das öffentlich-rechtliche Stiftungsrecht fehlt. Im Gegensatz zum Vereinsrecht, wo er sie (konkurrierend) sehr wohl besitzt, ist das Stiftungsrecht zweigeteilt. Da der BGB-Gesetzgeber im privatrechtlichen Stiftungsrecht keinen umfassenden Gebrauch von seiner Kompetenz gemacht hat, bleibt auch hier Raum für eine **ergänzende Landesgesetzgebung, die im Einzelfall zu beachten** ist.

Das Normprogramm des § 80 Abs. 2 BGB hat zum Ziel, die Begründung nicht überlebensfähiger Stiftungen zu verhindern. Denn die Stiftung unterscheidet sich von den anderen Organisationsformen durch einen erheblichen Unterschied: Es gibt bei ihr **keine Gesellschafter oder Mitglieder**. Die Stiftung gehört sich gewissermaßen selbst. Im Vordergrund steht ihr Vermögen, das einem festgelegten Stiftungszweck durch Stiftungsgeschäft dauerhaft gewidmet, also zu dienen bestimmt ist.

Die Stiftung ist eine **reine Verwaltungsorganisation**, die sich durch das Vorliegen von

- Stiftungszweck,
- Stiftungsvermögen und eine (dem Zweck angemessene)
- Stiftungsorganisation (zur Verwaltung der Stiftung)

auszeichnet. Unterschieden werden Stiftungen in

- rechtsfähige und nicht rechtsfähige (unselbständige) Stiftungen sowie in
- Stiftungen des Privatrechts und des öffentlichen Rechts sowie des kirchlichen Rechts.[367]

Eine Stiftung ist nur dann als rechtsfähig anzuerkennen, wenn das Stiftungsgeschäft den formalen Anforderungen des § 81 Abs. 1 BGB genügt, der Stiftungszweck das Gemeinwohl nicht gefährdet und seine dauernde (und nachhaltige)[368] Erfüllung als gesichert erscheint.

Als Stiftung unter Lebenden kann eine Stiftung nicht nur von natürlichen, sondern auch von juristischen Personen errichtet werden.[369] Das hierzu notwendige **schriftliche Stiftungsgeschäft** regelt Zweck, Vermögen und Satzung, deren Inhalt das jeweilige Landesrecht zu beachten hat. Mit dem Stiftungsgeschäft verpflichtet sich die Stifterin dazu, das versprochene Stiftungsvermögen an die Stiftung zu übertragen. Diese Verpflichtung ist einem Schenkungsversprechen gewissermaßen vergleichbar.[370]

Das Stiftungsgeschäft muss die **Organe der Stiftung** bestimmen. Zwar ist es gemäß § 86 iVm. § 26 BGB als Mindestanforderung ausreichend, dass eine einzelne Person zum Vorstand bestimmt wird. Zweckmäßig ist das aber nicht, da die Stiftung bei Ausscheiden dieser Person nicht mehr handlungsfähig wäre. In der Praxis wird in der Satzung neben einem mehrköpfigen Vorstand häufig auch noch ein **Stiftungsrat oder ein Kuratorium** vorgesehen.

Bei der rechtsfähigen Stiftung ist der **Sitz der Stiftung** im Hinblick auf das dem Anerkennungsverfahren zugrunde zu legende **Landesstiftungsrecht** maßgeblich, das auch auf den Inhalt der Satzung Einfluss haben kann. Der **Stiftungszweck**[371] muss **auf Dauer angelegt** sein. Soll die Stiftung gemeinnützig sein, so sind bei der Bestimmung des Stiftungszwecks die **Vorgaben des Gemeinnützigkeitsrechts** unbedingt zu beachten.[372]

Hinweis:
Zu beachten ist, dass der Zweck – anders als bei den anderen Organisationsformen – nachträglich nicht mehr ohne Weiteres geändert werden kann. Daher würde sich zwar ein möglichst offen formulierter Zweck empfehlen. Allerdings wird durch Stiftungsaufsicht und insbesondere durch die Finanzverwaltung bei angestrebter Gemeinnützigkeit die **möglichst konkrete Angabe** des Zwecks verlangt, um feststellen zu können, ob die Stiftung tatsächlich im Rahmen ihrer gemeinnützigen Zweckbestimmung satzungsgemäß tätig ist. Daher sollte der Zweck so weit wie möglich und so eng wie nötig gefasst werden. Eine **gute Beratung** ist hier angezeigt.

Der den Zweck bestimmende Stifterwille ist nicht nur im Rahmen der Gründung der Stiftung wichtig. Auch im Hinblick auf die inhaltliche Geschäftsführung der Stiftung ist er stets entscheidend. Daher rührt noch einmal mehr die Notwendigkeit einer **guten Dokumentation des Stifterwillens**. Sollte er aus dieser Dokumentation nicht abgeleitet werden können, muss der mutmaßliche Stifterwille ermittelt werden, was in der Praxis zu erheblichen Schwierigkeiten und von der Stifterin ungewollten Ergebnissen führen kann. Eine Änderung des Stifterwillens nach staatlicher Anerkennung der Stiftung ist dagegen unerheblich.

Das **Stiftungsvermögen muss dem Zweck** angemessen sein. Je anspruchsvoller der Zweck ausgestaltet ist, desto höher sollte das Vermögen der Stiftung ausfallen. Die die An-

[367] Letztere, die entweder als Sonderform einer Stiftung privaten oder – wie zumeist – öffentlichen Rechts ausgestaltet sind, haben im hier interessierenden Zusammenhang aber, wenn überhaupt, wohl nur eine sehr untergeordnete Bedeutung. Soll eine kirchliche Stiftung diakonischen Aufgaben dienen, so wird der Stiftungszweck zwar vom kirchlichen Auftrag umfasst, ist aber nicht-kirchlichen Einrichtungen vorbehalten. Die Behandlung als kirchliche Stiftung muss dem Stifterwillen entsprechen. Das Vorliegen einer kirchlichen Stiftung hat zur Folge, dass die Aufsicht über die Stiftung bei der kirchlichen Aufsichtsbehörde liegt. Siehe zu kirchlichen Stiftungen ferner unter C.4.7.1.

[368] Der Begriff „nachhaltig“ stellt kein eigenes Erfordernis dar, sondern ergänzt und verstärkt den Begriff der „dauernden“ Erfüllung des Stiftungszwecks bloß (vgl. die Ausführungen des Rechtsausschusses, BT-Drs. 14/8894, 10; RegE, BT-Drs. 14/8765, 15). Unzulässig wäre es daher, wenn die Stiftungsbehörde mit Hinweis auf diesen Begriff verlangte, dass der Stiftungszweck nachhaltig iSv „besonders intensiv“ oder „wirkungsvoll“ oder gar „klimaschonend“ erfüllt werden sollte.

[369] Bei einer Stiftung von Todes wegen sind die Formvorschriften einzuhalten, die bei Errichtung eines Testaments oder Erbvertrages zu beachten sind.

[370] Ein Unterschied besteht allerdings darin, dass der Schenker die Schenkung unter bestimmten – gesetzlichen oder vertraglichen – Gründen widerrufen kann. Diese Möglichkeit kann durch das Stiftungsgeschäft dagegen nicht begründet werden.

[371] Dieser muss nicht gemeinnützig sein, sondern kann auch privaten Zwecken dienen.

[372] Siehe insbesondere die Anlage 1 zu § 60 AO.

erkennung der Stiftung prüfende Landesbehörde kann diese aufgrund einer zu geringen Ausstattung ablehnen.[373]

Praxishinweis:
Eine **frühzeitige Abklärung** mit der anerkennenden Behörde, die ja die Lebensfähigkeit der Stiftung sicherstellen soll, ist zu empfehlen, ggf. auch im Hinblick auf die Art des einzubringenden Vermögens (zum Beispiel Anlagewerte, Grundstücke etc.). Reicht das zur Verfügung stehende Vermögen indes nicht aus, sollte über alternative Gründungen nachgedacht werden, etwa über die Gründung einer (gemeinnützigen) GmbH.

Da Stiftungen **dauerhaft gebundene Vermögensmassen** sind, muss ihr Vermögen notwendigerweise erhalten bleiben. Daher sehen die Stiftungsgesetze ausnahmslos vor, dass das Stiftungsvermögen in seinem Bestand **ungeschmälert zu erhalten** ist. Dieses Grundstockvermögen muss aber nicht die einzige Finanzierungsquelle für die Verwirklichung der Zwecke sein. In der Regel ist die Stiftung auf weiteres liquides Vermögen, etwa zusätzliches Stiftungsvermögen der Stifterin, sonstige Zustiftungen, laufende Spenden oder sonstige laufende Einnahmen, zu denen im gemeinnützigen Bereich auch öffentlich-rechtliche Zuwendungen gehören können, angewiesen, um dem Stiftungszweck nachhaltig und dauerhaft nachzukommen. Derlei Aussichten auf zusätzliches Kapital wird von den Stiftungsbehörden bei der Prüfung der Anerkennung im Hinblick auf die dauerhafte Erfüllung der Satzungszwecke berücksichtigt. Ein wesentlicher Unterschied besteht darin, dass Zustiftungen dem Grundstock des Stiftungsvermögens zugerechnet, wogegen Spenden auf den Stiftungszweck direkt zeitnah verwendet werden müssen (und nicht zur Ertragsgenerierung genutzt werden dürfen). Daher kann ein erhöhtes Anfangskapital gut dadurch bereitgestellt werden, dass das in Betracht kommende Stiftungsvermögen in einen Grundstock und eine Spende geteilt wird.

Etwas anders ist die Situation bei der seit 2013 zulässigen **Verbrauchsstiftung** (§ 80 Abs. 2 S. 2 BGB). Diese können auf einen kurzfristigen Zeitraum (mindestens 10 Jahre) angelegt sein und aufgrund des Entfallens des Erhaltungsgebots ihre Zwecke schon mit einem vergleichsweise kleineren Vermögen erreichen. Zuwendungen in den Kapitalstock einer Verbrauchsstiftung können aber steuerlich nur wie Spenden behandelt werden.

Die Wahl des **Namens** der Stiftung ist grundsätzlich frei, muss nur die unverwechselbare Identifikation der Stiftung erlauben und die Rechte Dritter, etwa Markenrechte, wahren.

Mit ihrer Anerkennung durch die Stiftungsbehörde,[374] die mit ihrer Bekanntgabe an den Stiftungsvorstand oder die Antragstellende wirksam wird,[375] entsteht die Stiftung als juristische Person und erwirbt damit einen Rechtsanspruch gegen die Stifterin auf Übertragung des zugesagten Stiftungsvermögens, § 82 S. 1 BGB. Soweit die Organe noch nicht bestellt sind, ist die Bestellung nun vorzunehmen.

C.4.7.1 Sonderform: Kirchliche Stiftung[376]

Rechtsfähige Stiftungen bürgerlichen oder – häufiger – öffentlichen Rechts sind auch die kirchlichen Stiftungen. Sie dienen (überwiegend) kirchlichen Aufgaben[377] und werden entweder von einer Kirche errichtet oder sollen entsprechend des Stifterwillens der Aufsicht einer kirchlichen Stelle unterliegen.[378] Kirchliche Stiftungen nehmen an dem den verfassten Kirchen im Grundgesetz eingeräumten besonderen Recht der Selbstverwaltung teil.

Die **Autonomie der Kirchen** schließt die Befugnis ein, die Verwaltung und die Beaufsichtigung der kirchlichen Stiftungen grundsätzlich selbst zu regeln, sodass in diesem Umfang das staatliche Stiftungsrecht zurücktritt. Eine der Hauptaufgaben der kirchlichen Stiftungsaufsicht besteht vor allem in der **rechtlichen Beratung** der ihrer Aufsicht unterliegenden Stiftungen. Indem die Aufsicht hilft, Rechts- und Satzungsverstöße erst gar nicht aufkommen zu lassen, fördert sie das kirchliche Stiftungswesen.

Drei wesentliche Kriterien machen somit eine kirchliche Stiftung aus: erstens die spezifische Zweckbindung, zweitens die organisatorische Zuordnung zu einer Kirche, drittens die verfahrensmäßige Beteiligung der kirchlichen Behörde.

Die Anerkennung einer kirchlichen Stiftung erfolgt allerdings in jedem Falle durch die Stiftungsbehörde. Anschließend wird auch sie in die von den Stiftungsbehörden geführten Stiftungsverzeichnisse aufgenommen.

C.4.7.2 Rechtsstellung der Stifterin

Mit ihrer Entstehung hat sich die Stiftung gleichzeitig endgültig von der Stifterin emanzipiert. Dieser ist ein Einwirken auf die Stiftung von nun an verwehrt. Dadurch ist aber nicht ausgeschlossen, dass sich die stiftende Person bzw. deren Organe und Vertreter in den Organen der Stiftung wiederfinden und sich so fortdauernden Einfluss auf die Geschäftsführung der Stiftung sichern. Dieser kann aber nur noch im Rahmen des nunmehr quasi kristallisierten Stiftungszwecks ausgeübt werden.

[373] Allgemein lässt sich sagen, dass eine Anerkennung unterhalb eines Stiftungsvermögens von € 50.000,-- in der Praxis schlechterdings nicht vorkommen wird. Die langanhaltende Niedrigzinsphase kann zudem erhöhte Erwartungen rechtfertigen. Stets ist hinsichtlich der Höhe aber in erster Linie deren Verhältnis zum Stiftungszweck entscheidend.

[374] Die zuständige Behörde ergibt sich aus dem jeweiligen Landesstiftungsgesetz.

[375] Die Bekanntmachung im dafür vorgesehenen Medium bzw. die Aufnahme im Stiftungsverzeichnis hat lediglich deklaratorischen Charakter.

[376] Siehe zu diesen ausführlich den Stiftungsleitfaden des Bischöflichen Generalvikariats Münster: https://www.stiftungsforum-im-bistum-muenster.de/fileadmin/redakteure/Downloads/2013-Ersthinhalte/Stiftungsleitfaden_Kapitel3.pdf (zuletzt abgerufen am 22. August 2020).

[377] Wesentlich ist eine sachliche, innere und äußere Verbindung zur Kirche.

[378] Eine Ausnahme machen insoweit die beiden Stadtstaaten Berlin und Hamburg, in denen vergleichbare Stiftungen immer der staatlichen Aufsicht unterliegen.

Für den (in der Satzung ggf. zu regelnden) Fall der **Aufhebung** der Stiftung, kann die Stifterin als **Anfallberechtigte** benannt werden.[379]

C.4.7.3 Organisationsverfassung der Stiftung

Obwohl das Stiftungsrecht mit § 86 BGB im Hinblick auf die Organisation einer Stiftung auf das Vereinsrecht verweist, besteht eine relative große Gestaltungsfreiheit. So kann etwa die Vertretungsbefugnis innerhalb des Vorstands recht frei geregelt werden, also ob etwa – abweichend von der grundsätzlich geltenden Mehrheitsvertretung – Gesamtvertretung oder Einzelvertretung eingeräumt wird und können Beschränkungen der Vertretungsmacht vorgesehen werden.[380] Auch die Befreiung vom **Selbstkontrahierungsverbot** (§ 181 BGB) ist möglich.[381] Wird dagegen tatsächlich eine Befreiung vom Selbstkontrahierungsverbot vorgesehen, muss – unabhängig von zuwendungsrechtlichen Auflagen – besonders auf eine Kontrolle der Ausübung der Vertretungsmacht geachtet werden.

C.4.7.4 Verwaltung des Stiftungsvermögens

Unisono sehen die Landesstiftungsgesetze vor, dass das Vermögen der Stiftung – sofern es sich nicht um eine Verbrauchsstiftung (s.o.) handelt – in seinem Bestand **nicht nur nominal, sondern real grundsätzlich zu erhalten** ist.[382] Ausnahmen von diesem Grundsatz können sich nur ergeben, wenn die Satzung der Stiftung eine Ausnahme zulässt oder der Stifterwille nicht anders zu verwirklichen ist. Das hat zur Folge, dass der Stiftungszweck grundsätzlich nur mit den aus dem Vermögen zu erwirtschaftenden Erträgen verwirklicht werden darf.

Zu dem Vermögen der Stiftung gehören wie bereits erwähnt auch **Zustiftungen**. Diese sind gemeinnützigkeitsrechtlich nicht zeitnah aber satzungsmäßig zu verwenden und müssen stiftungsrechtlich in den eben genannten Grundsätzen in ihrem Bestand erhalten werden.

Anders sieht es dagegen mit **Spenden** aus. Diese sind gemeinnützigkeitsrechtlich zeitnah zu verwenden, dem zu erhaltenden Stammvermögen der Stiftung aber nicht zuzurechnen. Die Unterscheidung von Zustiftung und Spende ist nach dem Willen der zuwendenden Person zu treffen.

C.4.7.5 Nicht rechtsfähige Stiftungen

Nicht rechtsfähige Stiftungen des bürgerlichen Rechts sind Vermögensmassen, die von der Stifterin oder dem Stifter zwar ohne rechtliche Verselbständigung, wohl aber mit einer festgelegten Zweckbestimmung auf eine juristische Person des Privatrechts oder öffentlichen Rechts zur treuhänderischen Verwaltung zum Zwecke der dauerhaften Zweckverfolgung übertragen werden.

Das BGB wie auch die Landesstiftungsgesetze treffen Regelungen lediglich im Hinblick auf rechtsfähige Stiftungen. Nicht rechtsfähige Stiftungen sind also gesetzlich nicht geregelt. Sie bedürfen daher zu ihrer Entstehung keiner staatlichen Anerkennung und unterliegen nicht der Aufsicht durch den Staat.[383]

Sie können aber dadurch auch nicht Träger von Rechten und Pflichten sein. Da sie also keine juristischen Personen sind und somit nicht am Rechtsverkehr teilnehmen können, geht das Vermögen der Stiftung in das Vermögen der Stiftungsträgerin über und ist von dieser treuhänderisch als **Sondervermögen** zu führen. Die Stiftungsträgerin, die jede natürliche oder juristische Person sein kann,[384] schließt Verträge **in eigenem Namen** mit Wirkung für und gegen das Stiftungsvermögen ab. Sie hat damit die gleiche Funktion wie der Vorstand bei der rechtsfähigen Stiftung.

Trotz all der Einschränkungen kann die Errichtung einer nicht rechtsfähigen Stiftung bürgerlichen Rechts von Interesse sein. Dies beispielsweise dann, wenn die Geschäftstätigkeit zur Erfüllung des Stiftungszwecks eher gering ausfallen wird oder aber wenn ein nur verhältnismäßig geringes Stiftungskapital eingebracht wird und deshalb die Errichtung einer rechtsfähigen Stiftung nicht in Frage kommt.

Im Hinblick auf die Steuerbegünstigung wird eine nicht rechtsfähige Stiftung ebenso behandelt, wie eine rechtsfähige Stiftung bürgerlichen Rechts. Sie müsste also gemeinnützigkeitsrechtlichen Anforderungen genügen.

C.4.7.6 Exkurs: Verantwortungseigentum

Eine im Vordringen befindliche Möglichkeit der Unternehmensorganisation ist das Verantwortungseigentum. Kurzgefasst geht es darum, dass Unternehmen langfristig

[379] Aus steuerlichen Gründen kann es angezeigt sein, dass der Stiftungsvorstand (thesaurierte) Erträge bereits vor Beginn des Liquidationsprogresses ausschüttet.

[380] Eine Beschränkung der Vertretungsmacht einer Stiftung aus dem Stiftungszweck wird zwar immer noch vielfach angenommen (Nachweise bei Backert, in: Hau/Poseck [Hrsg.], BeckOK, BGB, 54. Ed. 2020, Rz. 3 zu § 86 BGB). Sie ist aber im Hinblick auf die Tatsache, dass das deutsche Recht der Stellvertretung eine Ultra-vires-Beschränkung nicht kennt, abzulehnen. Beschränkungen der Vertretungsmacht sollten daher in der Satzung möglichst konkret vorgesehen werden.

[381] Allerdings kann auch hier wieder zu beachten sein, dass einige Zuwendungsgeber die Gewährung von Zuschüssen von diesem Verbot abhängig machen, also bereits die Möglichkeit der Befreiung insoweit schädlich sein kann. Außerhalb der Unterhaltung eines Zweckbetriebes kann das selten praktisch relevant werden.

[382] Im Rahmen der Vermögensanlage sind die folgenden Grundsätze zu beachten. Um ggf. die Sicherheit der Kapitalanlage zu garantieren, empfiehlt sich eine breite Streuung der Anlagearten. In diesem sicheren Rahmen sollte die Anlage die höchstmögliche Rendite erwirtschaften, wobei die Stiftung stets über die zur Erfüllung ihres Zwecks angemessene Liquidität verfügen soll.

[383] Eine Aufsicht kann aber dadurch erreicht werden, wenn die Stiftungsträgerin eine Körperschaft ist, die selbst der Aufsicht unterliegt.

[384] Um eine dauerhafte Zweckerfüllung zu ermöglichen, ist die Wahl einer juristischen Person grundsätzlich angezeigt.

sinnorientiert statt gewinnorientiert wirtschaften können. Auf zwei wesentliche Prinzipien kommt es dabei an:

1. **Selbstbestimmung:** Die Führung des Unternehmens obliegt nicht Anteilseignern, sondern den intrinsisch motivierten Mitarbeitenden. Zu diesem Zweck sind nur uneigennützige Eigentümer*innen zugelassen, bei denen Stimmrechte/Governance-Rechte nicht mit dem Recht zur Gewinnentnahme gekoppelt sind.
2. **Sinn-Orientierung:** Die Gewinnmaximierung wird nicht als Selbstzweck verstanden. Gewinne können nicht abgeführt werden. Das Unternehmen scheidet als Spekulationsobjekt aus.

Zwar fehlt es bis dato noch an einer innovativen Rechtsform für solche Modelle. Möglicherweise wird die Novellierung des Gemeinnützigkeitsrechts hierauf reagieren. Bis dahin können gute Ergebnisse aber auch auf bereits existierendem rechtlichen Grund erreicht werden. Insoweit bieten sich insbesondere folgende drei Modelle an: Das Veto-Anteil-Modell, das Modell der Einzelstiftung sowie das Modell der Doppelstiftung.[385]

C.4.8 AUSWAHL DER PASSENDEN RECHTSFORM

Die passende Rechtsform kann nur ausgewählt werden, wenn alle wesentlichen Parameter bekannt sind. Daher kann im Folgenden nur im Allgemeinen eine gewisse Orientierung gegeben werden.[386] Diese kann die **Beratung im Einzelfall** aber nicht ersetzen.

Insbesondere dann, wenn eine Kooperation zwischen verschiedenen gemeinnützigen Organisationen in eine passende Rechtsform eingekleidet werden soll, ist mit Vorsicht vorzugehen. Hierzu werden (unter C.4.8.3) noch nähere Hinweise gegeben.

C.4.8.1 Subjektive Auswahlkriterien hinsichtlich der Rechtsform

Hinsichtlich der Aufgaben und Tätigkeiten unterliegen die Stiftung, der Verein und die GmbH jeweils **in gleicher Weise** den Maßstäben der §§ 51 ff. AO über steuerbegünstigte Zwecke, die jeweils zwingend einzuhalten sind.

Da der Begriff der Stiftung häufig als **positiv konnotiert** bewertet wird, entscheiden sich mitunter Gründungen für diese Rechtsform, ohne besonderes Augenmerk auf die juristischen Konsequenzen gelegt zu haben. Die Verselbständigung des Stiftungsvermögens bedingt den Verlust der Möglichkeit der Einflussnahme, spätere Korrekturen sind kaum möglich. Eine Stiftung kommt daher im Ergebnis wohl nur in Betracht, wenn sie sich aufgrund der Vermögenssituation mehr oder minder aufdrängt, wenn also eine Stifterin/ein Stifter gerade die in Betracht kommende Lösung finanzieren möchte. Aufgrund der regelmäßig hohen Anfangsinvestition bei Digitalisierungsprojekten käme dann insbesondere eine **Verbrauchsstiftung** oder die Stiftung eines Grundstocks für den fortdauernden Betrieb mitsamt der zusätzlichen Spende des notwendigen Anfangskapitals in Betracht.

Die mittlerweile mögliche Gründung einer gGmbH hat die Praxis bereits **stark bereichert**. Nicht wenige entscheiden sich mittlerweile hierfür. Die **Satzung** der gGmbH kann so gestaltet werden, dass eine **Änderung** des Zwecks nur unter **besonderen Bedingungen** möglich ist. Damit kann die gGmbH **funktional** einer Stiftung **angenähert** werden. Allerdings findet das Stiftungsrecht auf eine Stiftungs-gGmbH keine Anwendung. Auch untersteht sie nicht der staatlichen Stiftungsaufsicht.

Auch die Rechtsform des eingetragenen Vereins (e.V.), die die häufigsten Neugründungen im diakonischen Bereich beschreibt, dürfte grundsätzlich positiv konnotiert sein. Für einige Tätigkeitsfelder (wie beispielsweise dem organisierten Sport) ist sie faktische Pflicht, wenn es auf Spenden, Zusammenarbeit und sonstige Unterstützung ankommt. Für einen Verein gilt, dass dieser **eingangs derart mit Vermögen ausgestattet** sein sollte, dass die Verwirklichung des gemeinnützigen Zwecks zumindest für einen gewissen, nicht unerheblichen Zeitraum, ggf. bis zur Generierung regelmäßiger Beiträge, gesichert ist.[387] Ähnliches gilt für eine Stiftung, deren Dotationskapital gesetzlich ebenfalls nicht festgeschrieben ist.[388] Die Stiftungsbehörden der Länder überprüfen die Vermögensausstattung der Stiftung allerdings regelmäßig anhand einer **Mittel-Zweck-Relation**, nach der der Zweck einer Stiftung mit dem Stiftungsvermögen nachhaltig und dauerhaft erfüllbar sein muss. Art und Umfang des Stiftungsvermögens muss so gewählt werden, dass der Stiftungszweck aus den normalerweise erzielbaren Erträgen – auch unter Berücksichtigung üblicher Geldwertentwicklung – dauerhaft zu verwirklichen ist.

[385] Zu den Einzelheiten siehe das Papier der Purpose-Gruppe (S. 15ff.), https://purpose-economy.org/content/uploads/purpose_online_may2020_lowres.pdf (zuletzt abgerufen am 12. August 2020).

[386] Vgl. ergänzend auch die Darstellung einiger Auswahlkriterien auf der Existenzgründerseite der Bundesregierung (BMWi): https://www.existenzgruender.de/SharedDocs/Downloads/DE/Checklisten-Uebersichten/Recht-Verhandlungsgespraeche/01_uebersicht-Rechtsformen.pdf?__blob=publicationFile (zuletzt abgerufen am 12. August 2020).

[387] OLG Köln v. 02. Oktober 1996, NJW-RR 1997, S. 1531.

[388] Unter Hinweis auf die Möglichkeit der Gründung einer unselbständigen Stiftung empfehlen Behörden häufig eine Mindestvermögensmasse von € 50.000. Je nach Zweck kann dieser Wert variieren.

C.4.8.2 Rechtliche Auswahlkriterien hinsichtlich der Rechtsform

Wie bereits erwähnt, kann nur in Kenntnis der genauen Sachlage des Einzelfalls eine Abwägung aller in Betracht kommenden Erwägungen erfolgen. Erste Orientierungspunkte sind die allgemein in der Betriebswirtschaftslehre identifizierten Auswahlkriterien:

- Haftungsrisiko,
- Gewinn- und Verlustbeteiligung,
- Finanzierungsmöglichkeiten,
- Ausgestaltung von Leitung und Kontrolle,
- Flexibilität der gesellschaftsrechtlichen Vertragsgestaltung,
- Rechnungslegung, Prüfung und Publizität sowie
- einmalige und laufende Kosten der Rechtsform.

Freilich können diese Kriterien nicht nur isoliert betrachtet werden, sondern stehen mitunter in Wechselwirkung zueinander (bspw. das Haftungsrisiko mit dem Einfluss auf die Geschäftsführung). Im vorliegenden Zusammenhang interessieren die folgenden Faktoren besonders:

C.4.8.2.1 Haftung

Ein wesentlicher Nachteil aller **Personengesellschaften** besteht in der Tatsache der **grundsätzlich unbeschränkten Haftung** ihrer Gesellschafter. Diese besteht, sobald die Gesellschaft im Rechtsverkehr, also nach außen hin auftritt, **akzessorisch**. Das heißt, dass für die Gesellschafterinnen[389] **automatisch** die Haftung begründet ist, sofern und soweit Verbindlichkeiten gegen die Gesellschaft bestehen. Ferner haftet sie **unmittelbar und primär**, können also direkt ohne Umweg über die Gesellschaft in Anspruch genommen werden.

Zudem ist die Haftung der Gesellschafterinnen **unbeschränkt**; ihr gesamtes Vermögen steht den Gläubigern gegebenenfalls zur Befriedigung zur Verfügung (quasi **„haften alle für alles mit allem“**). Auch im Rahmen der Gemeinnützigkeit sind Ausnahmen zur persönlichen Haftung im Regelfall nur bei **ausdrücklicher Vereinbarung** mit den Haftungsgläubigern denkbar. Leistet eine Gesellschafterin gegenüber den Gläubigern, hat sie allerdings einen entsprechenden **Ausgleichsanspruch** gegen die Gesellschaft (§ 713 bzw. 670 BGB) sowie – subsidiär – gegenüber den übrigen Gesellschafterinnen (§ 426 BGB).

Praxis-Hinweis:
Die Frage der Haftung dürfte bei der Auswahl der richtigen Rechtsform eine der wesentlichsten, wenn nicht gar die wesentliche, sein. Ist der **Einsatz größeren Kapitals** angestrebt, empfiehlt sich schon deshalb die **Gründung einer Personengesellschaft regelmäßig nicht**.

Unabhängig davon ist die Haftung bei Kooperationen ein Problem, da über einen möglicher Weise notwendig werdenden (und der Höhe nach unbegrenzten) **Verlustausgleich** immer auch eine **Mittelfehlverwendung** droht, die zum Verlust der Gemeinnützigkeit führen kann.

Durch

- den **richtig bestimmten Zweck** der Kooperation,
- die **Sicherstellung seiner Verfolgung** und
- die **passende Auswahl der zur Verfügung gestellten Mittel**

können entsprechende Risiken aber durchaus eingegrenzt werden.

Auch beim Verein kann sich eine persönliche Haftung des Vorstands ergeben, sofern es sich um einen **nicht rechtsfähigen** (also nicht eingetragenen) Verein handelt.

Gänzlich anders sieht die Rechtslage bei **Kapitalgesellschaften** aus. Bei diesen ist die Haftung der handelnden Geschäftsführung sowie der Gesellschafterinnen im Regelfall aufgrund der besonderen Haftungsstruktur der Kapitalgesellschaften **ausgeschlossen**. Besonderheiten bestehen insbesondere vor und während der Gründung.

C.4.8.2.2 Gründungsaufwand und Vermögen

Soweit es nur um kurzfristige, einfache und kaum haftungsbedingte Projekte geht, spielt der Gründungsaufwand die entscheidende Rolle. Dann kommt etwa die aufwendige Gründung einer Stiftung, die in anderen Fällen – vor allem aufgrund ihrer Bestandsgarantie – interessant sein kann, nicht in Betracht. Eher wird die Zusammenarbeit in Form einer GbR attraktiv sein, die sich ohne Aufwand und Stammkapital gründen lässt.

Das Stammkapital für eine **GmbH** beträgt grundsätzlich mindestens € 25.000. Bei der **UG**, der sogenannten **Mini-GmbH** kann das Gründungskapital schon mit € 1 erbracht werden, ist aber – aufgrund jährlicher Rücklagepflichten – zügig auf € 25.000 zu erhöhen.[390] Die Gesellschafteranteile der GmbH können prinzipiell frei veräußert und abgetreten werden. Allerdings bedürfen Gründungsakt und die Übertragung von Geschäftsanteilen der notariellen Beurkundung. Gleiches gilt für eine Kapitalerhöhung und die mit dieser verbundenen Schaffung weiterer Gesellschafteranteile. Auch für eine UG wird für die Gebührenermittlung das Mindeststammkapital von 25.000 Euro unterlegt. Bei einer Standardgründung mit Musterprotokoll reduzieren sich die Kosten; das Gründungsverfahren ist vereinfacht.

[389] Ausgenommen ist insoweit die Kommanditistin bei der KG.
[390] Die gesetzlich vorgeschriebene Rücklagenbildung bis zum Erreichen des Stammkapitals von 25.000 Euro verstößt freilich nicht gegen den Grundsatz der zeitnahen Mittelverwendung (§§ 55 Nr. 5 AO).

Allerdings ist eine Standardgründung einer **gemeinnützigen GmbH** nicht möglich, weil die Satzung im Hinblick auf Selbstlosigkeit und Vermögensbindung sowie Unmittelbarkeit und Ausschließlichkeit **anzupassen** wäre.[391]

Vertiefung:
Drei wesentliche Grundsätze bestimmen das Gemeinnützigkeitsrecht. Neben dem in § 57 AO verankerten Prinzip der Unmittelbarkeit (auf das unter C.4.8.6 näher eingegangen wird), sind Ausschließlichkeit (§ 56 AO) und Selbstlosigkeit (§ 55 AO) zu garantieren, will man die unter „Gemeinnützigkeit" gefassten Steuerbegünstigungen in Anspruch nehmen. Ein gemeinnützig tätiger Akteur muss seine Zwecke selbstlos, ausschließlich und unmittelbar verfolgen. Bei der Selbstlosigkeit geht es darum, dass nicht in erster Linie eigene wirtschaftliche Interessen verfolgt werden. Das wäre vor allem dann der Fall, wenn die Erzielung von Gewinnen im Vordergrund steht. Aber auch die Zahlung deutlich überhöhter Gehälter kann die Selbstlosigkeit in Frage stellen.[392] Ein Verstoß gegen das Ausschließlichkeitsgebot kann beispielsweise dann vorliegen, wenn ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb in der Gesamtschau zum Selbstzweck wird und damit eigenständig neben den steuerbegünstigten Zweck tritt oder diesen gar verdrängt.[393]

Weil sie im Gegenzug Anteile an der Kapitalgesellschaft erhalten, stellt für die Gesellschafter die Leistung der Stammeinlage bei Errichtung der GmbH eine reine **Vermögensumschichtung** dar. Das gleiche gilt im Falle des Erwerbs von Anteilen an einer bestehenden GmbH. Für die Leistung der Stammeinlage kann – zumindest sofern die Notwendigkeit dafür begründbar ist – die **freie Rücklage** eingesetzt werden, und zwar unabhängig davon, ob es sich um eine steuerbegünstigte oder eine steuerpflichtige Gesellschaft handelt.

Der Grundsatz der Vermögensbindung schließt die Bezahlung **angemessener** Vergütungen nicht aus. Eine erhebliche Überhöhung kann aber gegen das Selbstlosigkeitsgebot verstoßen.[394]

Sind die Gesellschafter der GmbH selbst steuerbegünstigte Körperschaften[395], ist die **Gewinnausschüttung** gemeinnützigkeitsrechtlich als **Mittelzuwendung** im Sinne des § 58 Ziff. 2 bzw. 3 AO anzusehen.[396]

Die **Beteiligung an einer GmbH** ist gemeinnützigkeitsrechtlich zwar in der Regel dem Bereich der **Vermögensverwaltung** zuzurechnen und damit grundsätzlich steuerfrei. Handelt die GmbH **gewerblich**, gilt für die die Geschäftsführung bestimmenden Gesellschafterinnen die Steuerbegünstigung nur dann, wenn die GmbH selbst steuerbegünstigt oder rein vermögensverwaltend tätig ist, vgl. Ziff. 3 AEAO zu § 64 AO. Auch finden die Grundsätze der Betriebsaufspaltung keine Anwendung, wenn die GmbH wie auch ihre Gesellschafterinnen gemeinnützig sind.

Sofern die Zuordnung zum Bereich der Vermögensverwaltung[397] in Betracht kommt (es also an der Bestimmung der Geschäftsführung fehlt), kann auch die Gründung einer **nichtgemeinnützigen GmbH** durchaus **vorteilhaft** sein, wenn etwa **Finanzierungsquellen** wie die der allgemeinen Wirtschaftsförderung nur im Falle gewerblicher Gründung genutzt werden können (und im Hinblick auf die Eigenmittel keine Mittelfehlverwendung droht). Hier muss **abgewogen** werden, ob das Erschließen von ggf. nur nichtgemeinnützigen Unternehmen zugänglichen Förderungen wichtiger ist als die steuerliche Begünstigung im Falle der Gemeinnützigkeit.

Beim **Verein** ist der Gründungsaufwand **gering**. Ein Mindestkapital wird ebenso wenig vorausgesetzt wie eine formalisierte Abschlussprüfung. Das Mitgliedschaftsrecht begründet anders als bei der GmbH **keine eigentümerähnliche Vermögensposition**.[398] Die Mitgliedschaft ist ein Personenrechtsverhältnis, so dass dem Mitglied beim Ausscheiden **grundsätzlich keine Abfindungs- oder sonstigen vermögenswerten Ausgleichsansprüche** zustehen. Auch scheidet – im entsprechenden Gegensatz zu Kapitalgesellschaften – die Ü**bertragung der Mitgliedschaft auf Dritte** aus. Die Mitgliedschaft besteht schlicht zwischen Ein- und Austritt aus dem Verein, die aber – wiederum anders als etwa bei einer GmbH – **rasch und unkompliziert** vollziehbar ist.[399]

Die Wahl der Rechtsform des Vereins wird daher insbesondere häufig dann erfolgen, wenn eine **Vielzahl von (fluktuierenden) Mitgliedern** vorgesehen ist, ohne dass es strukturell einer besonders starken Bindung an diese bedarf. Dagegen kann sich die Gründung einer im Vergleich schwerfälligeren GmbH anbieten, wenn eine **stabile Zusammensetzung des Gesellschafterkreises** gewünscht ist.

Ein Nachteil des Vereins kann sich bei seiner **Auflösung** zeigen. Da die Mitglieder eines Vereins keinen Anteil am

[391] Vgl. im Übrigen zur Gründung einer gemeinnützigen GmbH: Gilberg, Die gemeinnützige GmbH in der notariellen Praxis, RNotZ 2020, 193ff.
[392] Vgl. hierzu zuletzt BFH Urteil vom 12. März 2020 – V R 5/17: Da sich der Bereich des Angemessenen auf eine Bandbreite erstreckt, sind nur diejenigen Bezüge als unangemessen zu bewerten, die den oberen Rand dieser Bandbreite um mehr als 20% übersteigen. Liegt ein unangemessen hohes Geschäftsführergehalt vor, ist unter Berücksichtigung des Verhältnismäßigkeitsprinzips ein Entzug der Gemeinnützigkeit allerdings erst dann gerechtfertigt, wenn es sich nicht lediglich um einen geringfügigen Verstoß gegen das Mittelverwendungsgebot handelt.
[393] BFH BStBl 07, S. 631; Ziff. 1 zu § 56 AEAO. Soweit es an einer anderen ausreichenden Finanzierung fehlt und zwingende wirtschaftliche Umstände es erfordern, darf nach der Rechtsprechung des BFH der wirtschaftliche Geschäftsbetrieb im Einzelfall dennoch überwiegen, um Mittel für den steuerbegünstigten Zweck zu beschaffen (BFH BStBl 02, S. 162; aA. allerdings BMF BStBl I 02, S. 267). Es muss aber gewährleistet sein, dass die Körperschaft damit ausschließlich die Förderung ihres Zwecks anstrebt (BFH BStBl 07, S. 631).
[394] Siehe hierzu Fn. 388.
[395] Zum Begriff der Körperschaft vgl. § 1 Abs. 1 KStG, auf den § 51 Abs. 1 S. 2 AO für das Gemeinnützigkeitsrecht verweist.
[396] § 58 Ziff. 2 AO wird wohl kurzfristig mit Ziff. 1 verschmolzen werden (siehe dazu den Hinweis sub C.4.8.2.5.10).
[397] Zu prüfen ist dann, ob die Anlageform ein vertretbares Risiko übersteigt. Zu große Risiken dürfen im Bereich der Vermögensverwaltung durch Gemeinnützige nicht eingegangen werden.
[398] § 58 Ziff. 2 AO wird wohl kurzfristig mit Ziff. 1 verschmolzen werden (siehe dazu den Hinweis sub C.4.8.2.5.10).
[399] Zu prüfen ist dann, ob die Anlageform ein vertretbares Risiko übersteigt. Zu große Risiken dürfen im Bereich der Vermögensverwaltung durch Gemeinnützige nicht eingegangen werden.

Verein halten, kann dieser im Falle einer Auflösung auch nicht im Sinne des § 55 Abs. 1 Ziff. 2 (ggf. iVm. Abs. 3) AO an sie zurückfallen. Das Vermögen des Vereins kann damit zwar bei den Mitgliedern, etwa nach § 45 Abs. 3 BGB anfallen. Dies wird aber von der Finanzverwaltung ggf. nicht als durch § 55 AO privilegiert angesehen.

Die **Stiftung** ist die Rechtsform, die grundsätzlich den **höchsten Kapitalbedarf** hat, wobei sie aufgrund ihrer nach Gründung eher starren Natur gleichzeitig **besonders unflexibel** ist. Sie kommt daher in der Regel nur als **Förderkörperschaft** in Betracht.

C.4.8.2.3 Eigentümerstellung und Einflussnahme auf die Geschäftsführung

Vermittels ihrer jeweiligen Beteiligungen, die sie als Vermögenswerte halten, sind die Gesellschafterinnen die **Eigentümerinnen** einer Gesellschaft. Der Einsatz des zum Teil hohen Vermögens gemeinnütziger Organisationen wird auch durch die Ausübung der Gesellschafterrechte – im Rahmen der Zweckbindung – gesteuert. Neben den Steuerungsmöglichkeiten der geschäftsführenden Gesellschaftsorgane, besitzen auch die Gesellschafter Einfluss auf das Schicksal der Organisation; abhängig von ihrer jeweiligen Rechtsform und ggf. den Regelungen des Gesellschaftsvertrages. Zu beachten ist, dass im Falle der angestrebten Gemeinnützigkeit die Freiheit bei der Satzungsgestaltung **eingeschränkt** ist, um den gemeinnützigkeitsrechtlichen Anforderungen Genüge zu tun.

Bei der **AG** ist die Einflussnahme **äußerst beschränkt**. Gemeinnützige AGs finden sich **besonders selten**, weil bei der Gestaltung der Satzung wegen des Grundsatzes der Satzungsstrenge im Aktienrecht (§ 23 Abs. 5 AktG) erheblich **weniger Gestaltungsspielraum** besteht.

Dagegen unterliegt die **GmbH** dem entscheidenden Einfluss ihrer Gesellschafter*innen in allen wesentlichen Fragen der Organisation und Geschäftstätigkeit der Gesellschaft; und zwar unabhängig davon, ob es sich um Gründungsgesellschafter oder später hinzugetretene Gesellschafter handelt. So können die Gesellschafter durch qualifizierten Beschluss die Geschäftsführung ernennen, abwählen und ihr einzelne Aufgaben oder Aufgabenfelder zuweisen. Damit liegt die **bestimmende Verantwortung** für die Gesellschaft im Ergebnis grundsätzlich bei den Gesellschafter*innen der GmbH, obwohl sie im Außenverhältnis weder eine bestimmende Funktion noch die Haftung für das Handeln der Gesellschaft übernehmen.

Gerade im Vergleich zur selbständigen Stiftung bietet sich die GmbH daher immer dann an, wenn den Gründer*innen an einer **dauerhaften Kontroll- und Steuerungsfunktion** gelegen ist. Sie eignet sich besonders für einen **kleineren Kreis von Investor*innen mit gemeinsamen Ziel** – auch im Bereich eines Public-Private-Partnership (PPP) –, die lenkend auf die Gesellschaftsgeschicke **einwirken**. Im Falle von steuerlich denkbaren oder aus anderen Gründen wünschenswerten Kooperationen mit nichtgemeinnützigen Unternehmen (etwa im Bereich der Vermögensverwaltung) kann durch eine Begrenzung eines einzurichtenden Aufsichtsrats auf gemeinnützige Mitglieder ggf. gewünschter Einfluss auf die Geschäftsführung gesichert werden.

In einer **Genossenschaft** kann die alle Genossinnen umfassende Willensbildung mitunter schwierig sein, so dass sie sich insbesondere im Bereich eines Start-ups mitunter nur schwer steuern lässt. In geeigneten Fällen kann sich daher der Start eines Vorhabens als GmbH anbieten, die im Falle einer späteren Erweiterung der Gesellschaftersphäre entweder in eine Genossenschaft **formumgewandelt** wird oder der eine Beteiligungsgesellschaft zur Seite gestellt wird.

Auch bei einem **Verein** kann das geschäftsführende Organ, der Vorstand, nicht unabhängig handeln. Durch Beschluss der Mitgliederversammlung wird der Vereinsvorstand ernannt und abgewählt sowie **an Weisungen gebunden**. Der Einfluss der Mitglieder ist aber anders als bei der GmbH nicht an die jeweilige Kapitalbeteiligung gebunden, sondern durch das **Prinzip der Stimmengleichheit** bestimmt. Aufgrund der naturgemäß höheren Anzahl von Mitgliedern ist die Beschlussfassung hier im Gegensatz zu einer GmbH häufig **schwerfälliger**, was die **Unabhängigkeit des Vorstands erhöhen und die Kontrolldichte verringern** kann. Daher ist der Verein für ein PPP, in welchem sich der Staat oft eine inhaltliche Bestimmungsmöglichkeit sichern möchte, **nur selten geeignet**. Weitere Gremien, wie Beiräte, Ausschüsse, Aufsichtsräte oder Kuratorien können neben der Mitgliederversammlung dem Verein beigestellt werden. Es gilt aber der Grundsatz der **Verbandsautonomie**, so dass die Entscheidungsgewalt nicht uneingeschränkt auf Nichtmitglieder übertragen werden kann.

Überhaupt keine Eigentümerstellung findet sich im Bereich der rechtsfähigen **Stiftung**. Denn diese, vollkommen mitgliederlos, ist eine reine „Selbstverwaltungsorganisation“. Mit dem Stiftungsgeschäft, das der staatlichen Anerkennung bedarf, erwecken die Stifter die rechtsfähige Stiftung zum Leben, die sich fortan selbstständig verwaltet und gehört. Sie ist selbst von dem Willen ihrer Gründerinnen vollkommen unabhängig und allein dem Stiftungszweck verpflichtet. Der **Stiftung** einziges und damit auch einzig bestimmendes Organ ist der Vorstand. Er unterliegt nicht der Kontrolle von Gesellschaftern oder Mitgliedern, die es bei der Stiftung naturgemäß nicht gibt, sondern ist – sofern kein Beirat oder Kuratorium zur Kontrolle bestimmt ist – nur der Stiftungsaufsicht unterworfen. Letztere beschränkt sich auf ganz grundsätzliche Gesichtspunkte, die das Tagesgeschäft nicht mit umfassen.

Den Stifter*innen bleibt es allerdings vorbehalten, den Vorstand und ggf. die Mitglieder von Beirat oder Kuratorium selbst zu bestimmen und auszuwechseln. Der Stiftungsvorstand, der seinen Fortbestand regelmäßig durch Kooptation sichert, dh. die nachträgliche Hinzuwahl neuer Mitglieder durch die alten Mitglieder, ist allein dem Willen der Stifter*innen verbunden. Meist sind die Vorgaben allerdings so angelegt, dass sie auf unbestimmte Dauer angelegte Tätigkeiten nicht unnötig im Voraus einengen. Bei zu eng gefassten Vorgaben kann es nämlich im ungünstigsten Fall zu einem **Zweckerfüllungsnotstand** kommen. Aufgrund der besonderen Eigenständigkeit einer Stiftung und der nur beschränkten Kontrolle ist es auf Dauer fraglich, ob der Stiftungszweck im Rahmen gesellschaftlich, politisch und wirtschaftlich veränderter Rahmenbedingungen tatsächlich noch verfolgt werden kann oder muss.

C.4.8.2.4 Lebensdauer und Auflösung

Sowohl die Gesellschafter einer **GmbH** als auch die **Vereins**mitglieder können die Auflösung der Körperschaft durch qualifizierten Mehrheitsbeschluss beschließen. Die **Stiftung** besteht dagegen grundsätzlich in alle Ewigkeit fort, sofern nicht die Satzung andere Regelungen enthält oder die Stiftung aufsichtsrechtlich aufgelöst werden muss.[400]

Zusammenfassend lässt sich sagen, dass die (g)**GmbH in vielen Fällen die angemessenste Lösung** ist, insbesondere wenn ein **hoher Einfluss** der Gesellschafter auf die Geschäftsführung angestrebt wird (insbesondere im Bereich des PPP), ein **höherer Kapitaleinsatz** notwendig ist bzw. sich **besondere Haftungsrisiken** ergeben können.

Bei kurzfristigen Projekten, die wenig Kapital benötigen, **kaum Haftungsrisiken** begründen und eine **besondere Flexibilität** voraussetzen, kann aber auch die **GbR** vollkommen ausreichend sein.

Steht dagegen vor allem die **(dauerhafte) Vermögenswidmung** zugunsten eines vordefinierten gemeinnützigen Zwecks im Vordergrund, kann die **Stiftung** die richtige Rechtsform sein, sofern der relativ große Aufwand für ihre Gründung und ihre Inflexibilität kein Hindernis darstellen und eine staatliche Anerkennung erwünscht ist.

Bei einer größeren Anzahl von Leistungsbegünstigten oder Beitragenden kann sich die Rechtsform des **Vereins** besonders dann anbieten, wenn die Mitglieder auch **eigene Verantwortung** innerhalb der Körperschaft übernehmen wollen. Wird allerdings auf eine konstante Beteiligung der sich zusammenfindenden Akteure Wert gelegt, scheidet der Verein grundsätzlich aus. Denn das Ausscheiden eines Mitglieds berührt den Bestand des Vereins nicht. Wollen die Beteiligten anderes, ist der Verein schon daher nicht geeignet. Auch ist ein Verein längerfristig angelegt, eignet sich also auch nicht für kurzfristige Projekte. Der Verein erfordert zudem die Beteiligung von mindestens sieben Personen.

Mitunter kann aber die **Genossenschaft** zum Verein die bessere Alternative sein. Dies etwa, wenn eine noch festere und längerfristige Bindung gewünscht ist, da sich die Kündigungsmöglichkeiten bei der Genossenschaft weitergehend beschränken lassen.

C.4.8.2.5 Gemeinnützigkeit/ Steuerbegünstigung

Man mag es bedauern, aber allein die Tatsache, dass eine **gemeinnützige Körperschaft** gemeinwohlorientiert arbeitet, schützt freilich nicht vor Auseinandersetzungen mit dem Finanzamt. Die Anerkennung ist nur befristet und wird in periodischen Abständen durch die Finanzverwaltung überprüft. Vereinzelt kommt es zur Aberkennung der Gemeinnützigkeit und/oder einer persönlichen Haftung der Organmitglieder.

Durch Steuervorteile wird die Arbeit der steuerbegünstigten Körperschaften unterstützt.[401] Dies geschieht auf doppelte Weise. Zum einen direkt durch Befreiung von Steuerpflichten auf Seiten der Körperschaft; zum anderen dadurch, dass für Dritte (zB. Spender) aufgrund einer Zuwendungsbescheinigung steuerliche Anreize bestehen, Körperschaften zu unterstützen. Insgesamt soll gemeinnützige Arbeit durch die Vorteile attraktiver werden, was wiederum den Staat bei der Förderung sozialer Zwecke entlastet.[402]

Die Anerkennung der Gemeinnützigkeit einer jeden Organisationsform setzt voraus, dass eine Anzahl an Bedingungen erfüllt ist, namentlich im Hinblick auf die Ausgestaltung der Satzung und der satzungsmäßigen Tätigkeit der Organisation.[403]

C.4.8.2.5.1 Voraussetzungen für die Anerkennung der Gemeinnützigkeit

Voraussetzung ist zunächst, dass es sich bei der in Betracht kommenden Organisation um ein **Körperschaftssteuersubjekt** handelt. Laut in § 1 KStG sind dies insbesondere sämtliche Kapitalgesellschaften, Genossenschaften[404] und (sonstige) juristische Personen des Privatrechts.[405] Zudem muss die Körperschaft **gemeinnützige, mildtätige oder kirchliche Zwecke ausschließlich, selbstlos und grundsätzlich unmittelbar verfolgen**.

C.4.8.2.5.2 Die vier Sphären der Tätigkeit gemeinnütziger Organisationen

Kann dergestalt auf die Gemeinnützigkeit der betreffenden Organisation geschlossen werden, ist aber noch nicht gesagt,

[400] Dies ist selten der Fall und setzt etwa voraus, dass das Erreichen des Stiftungszwecks unmöglich geworden ist oder die Stiftung das Gemeinwohl gefährdet, § 87 Abs. 1 BGB.

[401] Im Hinblick auf die Corona-Krise beachte zudem die durch den Billigkeitserlass vom 09. April 2020 für den Gemeinnützigkeitssektor außerhalb der Reihe begründeten Vorteile (https://www.fgs.de/fileadmin/user_upload/PDFs/200409_steuerliche-massnahmen-zur-foerderung-der-hilfe-fuer-von-der-corona-krise-betroffene.PDF, zuletzt abgerufen am 01. Oktober 2020).

[402] Steuerbefreiungen und steuerliche Vergünstigungen aufgrund der Verfolgung kirchlicher, gemeinnütziger oder mildtätiger Zwecke enthalten beispielsweise § 5 I Ziff. 9 KStG, § 10b EStG, § 13 I Ziff. 16 und 17 ErbStG, § 3 Ziff. 6 GewStG, § 3 Ziff. 3b, § 3 Ziff. 4, § 4 Ziff. 6 GrStG, § 4 UStG (vgl aber vor §§ 51 ff Rz. 10), § 12 II Ziff. 8 UStG, § 18 Ziff. 2 Rennwett- und LotterieG. Wer Steuervorteile in Anspruch nehmen will, muss grundsätzlich nachweisen, dass die Voraussetzungen dafür vorliegen

[403] Gersch, in: Klein (Hrsg.), AO, 15. Aufl., 2020, Rz. 2 zu Vor § 51: „Das Gemeinnützigkeitsrecht ist so gegliedert, dass einleitend grundlegende Begriffe (§ 51) und steuerbegünstigte Zwecke geregelt werden. Steuerbegünstigte Zwecke ist der Oberbegriff für gemeinnützige (§ 52), mildtätige (§ 53) und kirchliche Zwecke (§ 54). §§ 55–58 enthalten die für alle steuerbegünstigten Körperschaften verpflichtenden Grundsätze für ihre ideelle Tätigkeit. §§ 59–63 betreffen die Verankerung dieser Grundsätze in der Satzung einer steuerbegünstigten Körperschaft und die Bindung der Geschäftsführung daran. Dem schließen sich die §§ 64 ff zur wirtschaftlichen Betätigung steuerbegünstigter Körperschaften in wirtschaftlichen Geschäftsbetrieben und Zweckbetrieben an.“

[404] Auch die nicht eingetragenen, also nicht rechtsfähigen Genossenschaften.

[405] Personengesellschaften, insbesondere die GbR sind keine Körperschaftssteuersubjekte (auch arg. e contrario § 15 Abs. 1 Ziff. 2 EStG) und können so nicht nach §§ 51ff. AO steuerbegünstigt sein. Sie haben aber gleichwohl Bedeutung im gemeinnützigen Sektor (dazu sogleich unter C.4.8.6). Auch kann ihnen durchaus immerhin zivilrechtlich die Gemeinnützigkeit zuerkannt werden, was etwa zu Haftungserleichterungen führen kann.

dass alle Tätigkeiten dieser Organisation auch gleichbehandelt werden, sich insbesondere alle Privilegien stets in Anspruch nehmen lassen.

Da der Tätigkeitsrahmen einer gemeinnützigen Organisation sehr vielfältig sein kann, hat die Verwaltungspraxis die sogenannte **Vier-Sphären-Theorie** übernommen, nach der die einzelnen Tätigkeiten steuerlich zugeordnet werden müssen. Die Tätigkeiten der Körperschaft sind so entweder dem ideellen Bereich, der Vermögensverwaltung, einem steuerpflichtigen wirtschaftlichen Geschäftsbetrieb oder einem steuerbegünstigten Zweckbetrieb zuzuordnen. Denn es kann steuerrechtlich einen erheblichen Unterschied machen, ob Spenden für Notleidende gesammelt werden oder ein Bistro betrieben wird. Die Abgrenzung dieser vier Sphären ist also von entscheidender Bedeutung. Für jede Sphäre gelten unterschiedliche Regelungen bei der Verwendung von Mitteln und der Besteuerung von Einnahmen.

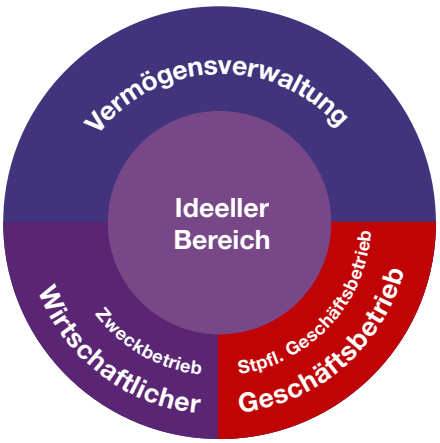


Fig. C.9: Die vier Sphären steuerbegünstigter Organisationen

Tätigkeiten des **ideellen Bereichs** verwirklichen einen gemeinnützigen Zweck und sind unentgeltlich. Entstehende Kosten werden vor allem durch Spenden, Mitgliedsbeiträge und Zuschüsse, insbesondere Fördermittel bestritten. Sowohl die Vermögensverwaltung als auch der Geschäftsbetrieb werden in § 14 AO definiert.

Eine Tätigkeit ist danach der **Vermögensverwaltung** zuzuordnen, wenn Vermögen zur Generierung von Erträgen eingesetzt wird, zB. die Anlage von Kapitalvermögen, die Vermietung von Grundstücken oder Einräumung von Lizenzen. Eventuell daraus resultierende Gewinne unterliegen der Zweck- und Fristenbindung.

Ein **wirtschaftlicher Geschäftsbetrieb** ist eine selbständige und nachhaltige[406] Tätigkeit, durch die Einnahmen oder andere wirtschaftliche Vorteile erzielt werden und die über den Rahmen der Vermögensverwaltung hinausgeht.[407] Die Absicht, Gewinne zu erzielen, ist insoweit unerheblich. Sobald also Einnahmen (zB. aufgrund eines Entgelts) erzielt werden sollen, wird in der Regel ein wirtschaftlicher Geschäftsbetrieb vorliegen.[408] Liegt ein solcher vor, ist noch danach zu unterscheiden, ob es sich um einen **steuerpflichtigen Geschäftsbetrieb** (dazu auch sogleich unter C.4.8.2.5.3) oder einen **Zweckbetrieb** (dazu auch sogleich unter C.4.8.2.5.5) handelt.

Dient der wirtschaftliche Geschäftsbetrieb in seiner Gesamtrichtung der Verwirklichung der steuerbegünstigten satzungsgemäßen Zwecke und können diese nur durch einen solchen Geschäftsbetrieb verwirklicht werden, wobei dieser zu nicht begünstigten Betrieben nicht in größerem Umfang in Wettbewerb tritt, als dies zur Erfüllung der steuerbegünstigten Zwecke unvermeidbar ist,[409] dann handelt es sich um einen Zweckbetrieb, § 65 AO.

Neben der Generalklausel des § 65 AO kann sich ein Zweckbetrieb aber davon unabhängig bereits nach den §§ 66 – 68 AO ergeben, die **vor zu prüfen** sind.[410] Bei Vorliegen der Voraussetzungen dieser Vorschriften, wird § 65 AO **verdrängt**, so dass es auf das Vorliegen dessen Voraussetzungen nicht mehr ankommt. Insbesondere kommt es nicht mehr auf die Erfüllung der Wettbewerbsklausel an.

Im **Zweckbetrieb** werden die entgeltlichen Leistungen und die dafür erforderlichen Aufwendungen zur Umsetzung der satzungsmäßigen Ziele einer Körperschaft abgebildet. Der Zweckbetrieb unterscheidet sich von Tätigkeiten im ideellen Bereich im Wesentlichen dadurch, dass für die Tätigkeit eine **Gegenleistung** im Sinne der Erzielung eines **wirtschaftlichen Vorteils** vereinbart ist. Und von der Vermögensverwaltung unterscheidet sich der Zweckbetrieb dadurch, dass erstere sich in der Nutzung eines Vermögenswertes erschöpft, letztere dagegen eine **aktive Tätigkeit** voraussetzt.

Die präzise Unterscheidung der Sphären ist äußerst relevant, da sie gemeinnützigkeitsrechtlich sehr unterschiedlich behandelt werden.

[406] An den Begriff der Nachhaltigkeit sind keine zu strengen Anforderungen zu stellen. Bei Vorliegen von Wiederholungsabsicht ist er bereits gegeben. Eine konkrete Planung der Wiederholung ist nicht erforderlich. Auch muss sich die Absicht der Wiederholung nicht auf die Erzielung von Einnahmen, sondern (nur) auf die konkrete Tätigkeit selbst beziehen (vgl. v. Twickel, in Blümich [Hrsg.], KStG, 152. EL, Mai 2020, Rz. 191 zu § 5, mwN.).

[407] Die Tätigkeit muss sich als Beteiligung am allgemeinen wirtschaftlichen Verkehr darstellen. Sie muss gegen Entgelt für Dritte äußerlich erkennbar angeboten werden. Unter Selbständigkeit iSd. 14 AO versteht der BFH nicht die persönliche Selbständigkeit der juristischen Person, sondern die sachliche Selbständigkeit der Betätigung im Sinne der Abgrenzbarkeit vom steuerbegünstigten Bereich (BFH I R 65/12 vom 7. Mai 2014, DStRE 14, S. 1312; v. Twickel, in Blümich [Hrsg.], KStG, 152. EL, Mai 2020, Rz. 191 zu § 5, mwN.). Sollte die Tätigkeit mit anderweitigen Tätigkeiten der Körperschaft verflochten sein, darf dies nicht so eng sein, dass ihre Ausübung ohne diese anderweitigen Tätigkeiten nicht möglich wäre (BFH I R 2/97 vom 15. Oktober 1997, BStBl II 98, S. 175).

[408] Die Entgelte eines wirtschaftlichen Geschäftsbetriebes müssen aufgrund des Drittbegünstigungsverbots (§ 55 Abs. 1 Ziff. 3 AO – Ausdruck des Gebots der Selbstlosigkeit) sowie des Gebots der wirtschaftlichen Geschäftsführung grundsätzlich den Marktpreisen entsprechen.

[409] Je wichtiger die wirtschaftliche Betätigung für die Förderung des privilegierten Zwecks, desto mehr muss der wirtschaftliche Wettbewerb seine Schlechterstellung hinnehmen. Es ist eine Abwägung zwischen dem Interesse der Allgemeinheit an einem nicht durch steuerrechtliche Begünstigungen beeinträchtigten Wettbewerb und dem Interesse der Allgemeinheit an der Förderung des steuerbegünstigten Zwecks erforderlich. Zu betonen ist, dass § 65 Ziff. 3 also nicht jeglichen Wettbewerb verbietet, sondern nur den über das erforderliche Maß hinausgehenden Wettbewerb. Unschädlich ist der Wettbewerb insbesondere, soweit der steuerbegünstigte Zweck ohne die konkurrierende Betätigung in ihrem konkreten Ausmaß nicht erreicht werden könnte, also andere oder weniger beeinträchtigende Maßnahmen zur Zweckerfüllung nicht zur Verfügung stehen (BFH I R 35/93, BStBl. II 1995, S. 767).

[410] Zu beginnen ist mit der Prüfung des § 68 AO. Liegen dessen Voraussetzungen vor, so kommt es weder auf die Erfüllung des Programms des § 66 bzw. 67 noch des § 65 AO an.

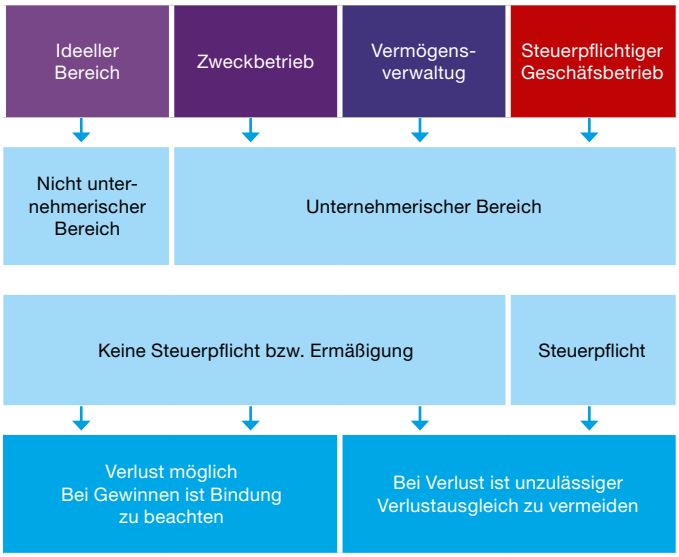


Fig. C.10: Vereinfachte Darstellung der Wirkung der Sphären

Die Vorteile der Gemeinnützigkeit liegen in der steuerlichen Begünstigung.[411] Im geeigneten Fall verzichtet der Staat auf die Erhebung bestimmter Steuern etwa ganz (zB. Körperschaftsteuer und Gewerbesteuer) oder – ebenfalls – ganz bzw. teilweise (zB. Umsatzsteuer). Zudem sind Zuwendungen an die gemeinnützige Organisation ggf. begünstigt.

Mit Gewährung der Vergünstigungen greift der Gesetzgeber in den **Wettbewerb** zulasten der nicht begünstigten Marktteilnehmer ein. Zum Ausgleich bringen die Vorteile daher auch einige **Nachteile** mit sich. So ist das Vermögen einer steuerbegünstigten Organisation nicht frei verfügbar, sondern **dauerhaft für steuerbegünstigte Zwecke gebunden** (Grundsatz der selbstlosen Vermögensbindung).

Das **Gebot der gemeinnützigen Mittelverwendung** setzt voraus, dass die Körperschaft sämtliche ihr zur Verfügung stehenden gebundenen Mittel **ausschließlich für die satzungsmäßigen Zwecke** verwendet. Eine abweichende Verwendung gilt als **Mittelfehlverwendung**, die zu einem Absprechen der Gemeinnützigkeit führen kann.[412] Zudem sind die Mittel grundsätzlich **zeitnah zu verwenden** (Grundsatz der zeitnahen Mittelverwendung). Die Erfüllung beider Grundsätze ist **nachzuweisen**.

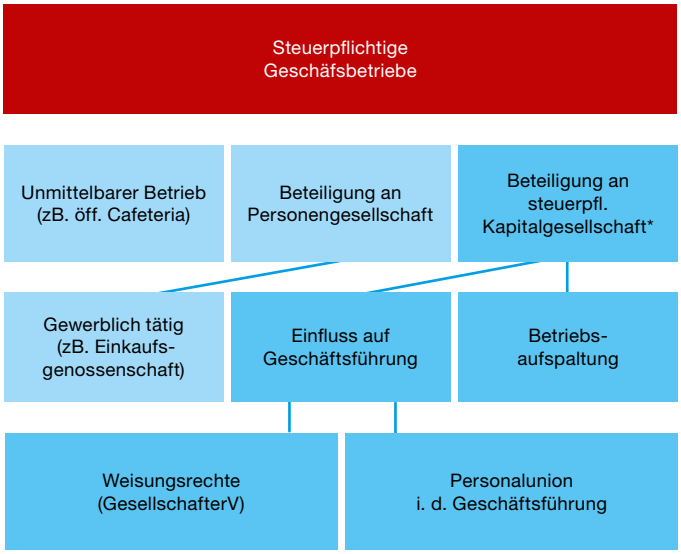
Allerdings schließt das Verfolgen von eigenwirtschaftlichen Zwecken die Anerkennung als gemeinnützig nicht zwingend aus (dazu sogleich genauer unter C.4.8.2.5.3).

Die **Beteiligung an einer Kapitalgesellschaft** kann je nach Ausgestaltung Vermögensverwaltung oder ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb sein. Wenn weisungsmäßiger Einfluss auf die Geschäftsführung oder Personalunion in der Geschäftsführung besteht bzw. eine Betriebsaufspaltung vorliegt, ist ein steuerpflichtiger Geschäftsbetrieb gegeben, sofern die Tätigkeit der Kapitalgesellschaft selbst nicht als gemeinnützig zu klassifizieren ist.

Der wirtschaftliche Geschäftsbetrieb wird gemäß § 64 Abs. 3 AO jedenfalls dann nicht besteuert, wenn die Brutto-Einnahmen (also einschließlich einer ggf. anfallenden Umsatzsteuer) € 35.000,-- bzw. € 45.000,--[413] nicht übersteigen.[414] Werden mehrere steuerpflichtige Geschäftsbetriebe unterhalten, so sind die Gewinne und Verluste gegeneinander zu saldieren. Überschüsse sind grundsätzlich zeitnah für steuerbegünstigte Zwecke zu verwenden; ausnahmsweise ist die Bildung von Rücklagen möglich.

C.4.8.2.5.3 Steuerpflichtiger wirtschaftlicher Geschäftsbetrieb und Gemeinnützigkeit

Ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb ist **generell erlaubt**. Es kommen für ihn aber Steuerbefreiungen grundsätzlich nicht in Betracht. Regelmäßig besteht also eine Steuerpflicht bei Körperschaft- und Gewerbesteuer. Dies gilt sowohl für Körperschaften, die ausschließlich einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb unterhalten als auch für Körperschaften, die neben dem ideellen Bereich (als Zweckbetrieb oder Vermögensverwaltung) auch einen steuerpflichtigen Geschäftsbetrieb unterhalten.



*sofern die Gesellschaft keine reine Vermögensverwaltung betreibt

Fig. C.11: Übersicht über die Erscheinungsformen steuerpflichtiger Geschäftsbetriebe

[411] Ob eine Organisation die Steuerbefreiung für sich in Anspruch nehmen kann, ergibt sich nicht aus der Abgabenordnung, sondern aus den Einzelsteuergesetzen, also etwa dem KStG oder dem UStG. Allerdings knüpfen die dortigen Ausnahmetatbestände an die Anerkennung der Steuerbegünstigung an, die wiederum in der AO (§ 51ff.) geregelt ist.

[412] Klassisch ist insoweit die Abdeckung von Verlusten aus wirtschaftlichen Geschäftsbetrieben, vgl. hierzu AEAO Ziff. 3 zu § 55 Abs. 1 Ziff. 1 AO, sowie die unangemessene Höhe des Geschäftsführergehalts (siehe zu dieser Frage BFH, Urt. v. 12.3.2020 – V R 5/17 [Fn. 388]).

[413] Mit einer Korrektur auf diese Höhe durch das Jahressteuergesetz 2020 ist zum Zeitpunkt des Redaktionsschlusses zu rechnen. Der von der Finanzministerkonferenz der Bundesländer eingebrachte und durch den Entwurf umgesetzte Vorschlag liegt bei € 45.000.

[414] Dabei handelt es sich um eine Freigrenze, bei deren auch nur geringfügigen Überschreitung die Einnahmen vollen Umfangs (ggf. abzüglich des Freibetrags nach § 24 KStG) besteuert werden.

Die Körperschaften verlieren also ihre Steuerbegünstigungen für alle dem steuerpflichtigen wirtschaftlichen Geschäftsbetrieb zuzuordnenden Besteuerungsgrundlagen (Einkünfte, Umsätze, Vermögen), § 64 Abs. 1 AO. Nach § 64 Abs. 3 AO werden allerdings betreffende Erträge unter € 35.000,-- bzw. € 45.000[415] dergestalt privilegiert, dass diese nicht der Körperschafts- und der Gewerbesteuer unterworfen sind;[416] anderes gilt indes für die Kapitalertragsteuer im Hinblick auf die im Bereich des wirtschaftlichen Geschäftsbetriebes anfallenden Erträge. Alle **Gewinne sind für steuerbegünstigte Zwecke** zu verwenden.

Ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb kann die Gemeinnützigkeit einer Organisation allerdings dann insgesamt ausschließen, wenn er zum **Selbstzweck** wird und selbständig neben den gemeinnützigen Zweck tritt oder diesen verdrängt; nicht dagegen, wenn er lediglich zur **Mittelbeschaffung** zugunsten des steuerbegünstigten Zweckes dient. Er darf also an der Verwirklichung des Prinzips der **Selbstlosigkeit** und (insbesondere) der **Ausschließlichkeit** nicht rütteln und muss **immer im Dienst des gemeinnützigen Zwecks** stehen, indem durch ihn Mittel für den gemeinnützigen Zweck beschafft werden.[417]

Insbesondere schädlich sind zudem steuerpflichtige Geschäftsbetriebe, die **auf Dauer defizitär** arbeiten. Da der steuerpflichtige wirtschaftliche Geschäftsbetrieb nur der Mittelbeschaffung dient, ist ein Verlustausgleich aus ideellen Mitteln ausgeschlossen und führt grundsätzlich zum **Verlust der Gemeinnützigkeit** der Körperschaft.[418] War allerdings beim Aufbau eines neuen steuerpflichtigen Geschäftsbetriebes mit Anfangsverlusten zu rechnen, kann die Verwendung von Mitteln des ideellen Bereichs insoweit zulässig sein.[419]

Die Errichtung eines wirtschaftlichen Geschäftsbetriebes aus Mitteln der **freien Rücklage** ist grundsätzlich möglich. Gebundene Rücklagen sind immer zweckbestimmt zu verwenden, können daher nur für die Errichtung eines Zweckbetriebes in Betracht kommen.

C.4.8.2.5.4 Praxis-Hinweis: Zweckgebundene Rücklage

Sollen – beispielsweise für ein größeres Digitalisierungsprojekt – **erst Mittel angespart** werden, so ist dies im Rahmen der Grundsätze der zeitnahen Mittelverwendung möglich, und zwar im Hinblick auf § 62 Abs. 1 Ziff. 1 AO (zweckgebundene Rücklage). Dafür müssen die der Rücklage zugeführten Mittel erstens dazu bestimmt sein, die **satzungsmäßigen Zwecke nachhaltig zu erfüllen**. Und zweitens muss die Bildung einer Rücklage zwecks nachhaltiger Erfüllung des satzungsmäßigen Zwecks erforderlich sein, was in jedem Prüfungszeitraum **erneut zu überprüfen** ist.[420]

Es sollte für die Durchführung des Vorhabens ein **konkreter Zeitplan** vorliegen. Fehlt dieser, muss die Durchführung des geplanten Vorhabens gleichwohl in Ansehung der (finanziellen) Verhältnisse der steuerbegünstigten Körperschaft in einem angemessenen Zeitraum realistisch sein (AEAO Ziff. 4 zu § 62). Ein Zeitraum von sechs Jahren sollte grundsätzlich nicht überschritten werden.[421] Es fehlt an der Erforderlichkeit einer Rücklage, wenn sie ein in unabsehbarer Ferne liegendes Ziel verwirklichen soll.

C.4.8.2.5.4.1 Checkliste zweckgebundene Rücklage

- Mittel zur nachhaltigen Erfüllung satzungsmäßiger Zwecke bestimmt?
- Bildung der Rücklage erforderlich?
- Liegt ein konkreter Zeitplan für die Umsetzung des Vorhabens vor bzw. ist die Durchführung des Vorhabens in Ansehung der (finanziellen) Verhältnisse der durchführenden Körperschaft realistisch?
- Ist eine turnusmäßige Überprüfung der Voraussetzungen sichergestellt?
- Ist die Umsetzung des Vorhabens in – weniger als – sechs Jahren möglich?

[415] Mit einer Korrektur auf diese Höhe durch das Jahressteuergesetz 2020 ist zum Zeitpunkt des Redaktionsschlusses zu rechnen. Der von der Finanzministerkonferenz der Bundesländer eingebrachte und durch den Entwurf umgesetzte Vorschlag liegt bei € 45.000.

[416] Sofern keine Gewinnpauschalierung vorgenommen werden kann (§ 64 Abs. 6 AO) erfolgt die Veranlagung nach den allgemeinen Grundsätzen. Zur Ermittlung eines möglicherweise gemeinnützigkeitsschädlichen Verlusts werden die Ergebnisse mehrerer steuerpflichtiger wirtschaftlicher Geschäftsbetriebe allerdings saldiert (§ 64 Abs. 2 AO)

[417] Ausnahmsweise darf nach der Rechtsprechung der wirtschaftliche Geschäftsbetrieb überwiegen, um Mittel für den steuerbegünstigten Zweck zu beschaffen, wenn zwingende wirtschaftliche Umstände es erfordern (BFH BStBl. I 02, S. 162, anderer Ansicht ist allerdings das BMF, BStBl. I 02, S. 267). Bei steuerbegünstigten Körperschaften, insbesondere Mittelbeschaffungskörperschaften, die sich im Rahmen ihrer tatsächlichen Geschäftsführung an die in ihrer Satzung enthaltene Pflicht zur Verwendung sämtlicher Mittel für die satzungsmäßigen Zwecke halten, ist das Ausschließlichkeitsgebot selbst dann als erfüllt anzusehen, wenn sie sich vollständig aus Mitteln eines steuerpflichtigen wirtschaftlichen Geschäftsbetriebs oder aus der Vermögensverwaltung finanzieren (AEAO Ziff. 1 zu § 56).

[418] Anders ist dies nur im Hinblick auf Anlaufverluste, mit denen zu rechnen war. Nach Ziff. 8 des AEAO zu § 55 müssen die Mittel aber dem ideellen Bereich innerhalb von drei Jahren nach dem Verlustentstehungsjahr wieder zugeführt werden.

[419] Siehe insgesamt AEAO Ziff. 4ff. zu § 55 AO.

[420] Vgl. BFH BStBl 90, S. 28; OFD Frankfurt DStR 14, S. 803.

[421] OFD Frankfurt, a.a.O. (Fn. 217).

C.4.8.2.5.5 Zweckbetrieb[422]

Besondere Privilegien bestehen für wirtschaftliche Geschäftsbetriebe, die als **Zweckbetriebe** einzustufen sind. Wenn ein Zweckbetrieb nach §§ 65 bis 68 AO vorliegt,[423] kann eine steuerliche Begünstigung bestehen bleiben, die für einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb nicht anzuwenden wäre. So wird etwa die Steuerbefreiung nach § 5 Abs. 1 Nr. 9 KStG Körperschaften gewährt, die nach der Satzung und der tatsächlichen Geschäftsführung ausschließlich und unmittelbar gemeinnützigen, mildtätigen oder kirchlichen Zwecken dienen (§ 51 bis § 68 AO). Wird ein wirtschaftlicher Geschäftsbetrieb (§ 14 AO) unterhalten, ist die Steuerbefreiung grundsätzlich ausgeschlossen (§ 5 Abs. 1 Nr. 9 Satz 2 KStG). Die Körperschaft verliert die Steuerbegünstigung jedoch nur, soweit der wirtschaftliche Geschäftsbetrieb kein Zweckbetrieb (§§ 65 bis 68 AO) ist (§ 64 Abs. 1 AO).

In der Praxis ist es also bei Vorliegen eines wirtschaftlichen Geschäftsbetriebes zu unterscheiden zwischen – steuerbegünstigtem – Zweckbetrieb und – steuerpflichtigem – wirtschaftlichen Geschäftsbetrieb. Diese Abgrenzung hat nicht nur ertrag-, gewerbe- und umsatzsteuerliche Auswirkungen, sondern betrifft auch die Festlegung von Entgelten, die Möglichkeit des Ausgleichs von Verlusten bzw. Bezuschussungen.

Da der Zweckbetrieb in erster Linie ganz vorrangig satzungsgemäßen Zwecken dienen muss, darf er zwar Gewinne erzielen, es aber **nicht in erster Linie** auf deren Erzielung **absehen**, selbst wenn diese für den gemeinnützigen Zweck verwendet werden. Das für seine Leistungen verlangte Entgelt muss sich also mehr oder minder im **Kostenersatz**, also dem konkreten Finanzierungsbedarf des jeweiligen wirtschaftlichen Geschäftsbetriebes **einschließlich zulässiger Rücklagen** erschöpfen.[424]

Der Zweckbetrieb ist aber durchaus **als Zuschussgeschäft zulässig**, darf also dauerhaft Verluste machen, (sofern) deren Ausgleich durch ideelle Mittel möglich ist; dies ganz im Gegensatz zum steuerpflichtigen wirtschaftlichen Geschäftsbetrieb, der bei dauerhafter Verlusterwartung umgehend einzustellen wäre und bei dem der Verlustausgleich aus ideellen Mitteln grundsätzlich zum Verlust der Gemeinnützigkeit der Körperschaft führte (s.o.). Allein aber die Tatsache, dass lediglich kostendeckende Entgelte erhoben werden, führt wie oben gezeigt noch nicht zum Vorliegen eines Zweckbetriebes.[425]

Ein Zweckbetrieb scheidet nach bisheriger Rechtslage aus, wenn und soweit für den Kooperationspartner nur allgemeine Geschäftsführung und Verwaltungstätigkeiten erbracht werden. Dann handelt es sich in der Regel um eine sogenannte **Servicegesellschaft** (siehe dazu den sogleich folgenden Exkurs).

Hinweis:
Zum Zeitpunkt des Redaktionsschlusses ist noch unklar, ob die im Entwurf des Jahressteuergesetzes 2020 beschlossene Neufassung des § 57 Abs. 3 AO tatsächlich in Kraft treten wird und dadurch unmittelbar gemeinnütziges Handeln im Sinne der AO schon dann anzunehmen ist, wenn die Organisation planmäßig mit mindestens einer weiteren steuerbegünstigten Organisation zusammenwirkt.[426] Die Gesetzesbegründung führt als Beispiel für ein solches planmäßiges Zusammenwirken Wäschereileistungen einer Tochtergesellschaft für den Krankenhausbetrieb der Muttergesellschaft an. Nach bisheriger Rechtslage wurde nur der Krankenhausbetrieb der Muttergesellschaft als Zweckbetrieb eingestuft; die Wäschereileistungen der Tochtergesellschaft waren nicht steuerbegünstigt. Derlei Unternehmen werden bisher als sogenannte Service-Gesellschaften in gewerblicher Form geführt. Aufgrund des gegebenen planmäßigen Zusammenwirkens sollen zukünftig auch die Leistungen der Tochtergesellschaft einen Zweckbetrieb begründen. Das Zusammenwirken beider Gesellschaften wäre dann gemäß § 57 Abs. 3 AO-Entwurf einheitlich zu beurteilen. Damit könnten auch Gesellschaften als gemeinnützig anerkannt werden, die ausschließlich derartige Funktionsleistungen an andere steuerbegünstigte Körperschaften erbringen. Nach aktuellem Stand ist hierfür weder ein Über-Unterordnungs-Verhältnis noch eine Konzernstruktur vorauszusetzen.

Sollte die Gesetzesänderung so beschlossen werden, wären zahlreiche Fragestellungen der Betriebsprüfung, etwa der Abgrenzung von Zweckbetrieb zu steuerpflichti-

[422] Zur Definition siehe schon oben sub C.4.8.2.5.2.

[423] Besonders praxisrelevant ist vorliegend der konstitutive Zweckbetrieb nach § 66 AO. Liegen die Voraussetzungen der §§ 66 – 68 AO vor, ist auf die Prüfung der allgemeinen Voraussetzungen eines Zweckbetriebs nach § 65 AO zu verzichten. Das gilt auch für dessen Wettbewerbsklausel. Soweit es sich aber nicht um einen Katalogfall eines konstitutiven Zweckbetriebs nach §§ 66 – 68 AO handelt, kann er nur angenommen werden, wenn er den satzungsmäßigen Zwecken dient, zur Erfüllung dieser Zwecke erforderlich ist und nicht zu steuerpflichtigen Betrieben derselben oder ähnlicher Art in größerem Umfang als bei der Erfüllung des Zweckes unvermeidlich in Wettbewerb tritt (§ 65 AO). Alle drei Voraussetzungen müssen kumulativ erfüllt sein, damit es sich bei einem wirtschaftlichen Geschäftsbetrieb um einen Zweckbetrieb handelt. Allein der Umstand, dass die Tätigkeit von einer gemeinnützigen Körperschaft, etwa einem Wohlfahrtsverband durchgeführt wird, begründet noch keinen Zweckbetrieb.

[424] Vgl. im Rahmen der hier besonders einschlägigen Zweckbetriebe nach § 66 AO Ziff. 2 zu § 66 AEAO: Die Wohlfahrtspflege darf nicht des Erwerbs wegen ausgeübt werden. Eine Einrichtung wird dann „des Erwerbs wegen“ betrieben, wenn damit Gewinne angestrebt werden, die den konkreten Finanzierungsbedarf des jeweiligen wirtschaftlichen Geschäftsbetriebs übersteigen, die Wohlfahrtspflege mithin in erster Linie auf Mehrung des eigenen Vermögens gerichtet ist. Dabei kann die Erzielung von Gewinnen in gewissem Umfang – z.B. zum Inflationsausgleich oder zur Finanzierung von betrieblichen Erhaltungs- und Modernisierungsmaßnahmen – geboten sein, ohne in Konflikt mit dem Zweck der steuerlichen Begünstigung zu stehen (BFH-Urteil vom 27.11.2013, I R 17/12, BStBl. 2016 II S. 68). Werden in drei aufeinanderfolgenden Veranlagungszeiträumen jeweils Gewinne erwirtschaftet, die den konkreten Finanzierungsbedarf der wohlfahrtspflegerischen Gesamtsphäre der Körperschaft übersteigen, ist widerlegbar (z.B. unbeabsichtigte Gewinne aufgrund von Marktschwankungen) von einer zweckbetriebsschädlichen Absicht der Körperschaft auszugehen, den Zweckbetrieb des Erwerbs wegen auszuüben. Gewinne aufgrund staatlich regulierter Preise (z.B. auf Grundlage einer Gebührenordnung nach Maßgabe des § 90 SGB XI) sind kein Indiz dafür, dass der Zweckbetrieb des Erwerbs wegen ausgeübt wird.

[425] Vgl. die weiteren in Fn. 420 genannten Faktoren.

[426] Konkretisierungen wird ggf. ein Anfang 2021 zu erwartender Anwendungserlass bringen.

gem Gewerbebetrieb oder der Angemessenheit von Verrechnungspreisen bzw. Gewinnaufschlägen hinfällig.[427]

Die Abgrenzung machte in der Praxis unter bestimmten Umstände keine Probleme. Denn die notwendige Unmittelbarkeit ist gegeben, wenn der im Rahmen der Wohlfahrtspflege privilegierte Empfängerkreis (vgl. § 53 AO)[428] die ihnen dienenden Leistungen unmittelbar – also nicht erst am Ende einer mehrstufigen Leistungskette – durch die als Hilfsperson tätige Körperschaft erhält.[429] Ein faktisch-direktes Zugutekommen reicht dabei aus.[430]

Unschädlich ist, ob damit gleichzeitig vertragliche Leistungen für eine weitere gemeinnützige Körperschaft erbracht werden bzw. mehrere Körperschaften arbeitsteilig zur Verwirklichung eines gemeinsamen Zwecks der Wohlfahrtspflege zusammenwirken.[431]

C.4.8.2.5.6 Exkurs: Service-Gesellschaften[432]

Die entgeltliche Übernahme von allgemeinen Leistungen,[433] namentlich Verwaltungsdienstleistungen war bislang (siehe zur anstehenden Gesetzesänderung durch das Jahressteuergesetz 2020 den vorgenannten Hinweis) auch dann, wenn sie für steuerbegünstigte Körperschaften erfolgt, grundsätzlich kein Zweckbetrieb, also nicht steuerlich gemeinnützig. Dies folgt(e) im Regelfall schon daraus, dass die Leistung zum einen nicht unmittelbar gegenüber dem von § 53 AO eingefassten Adressatenkreis Hilfsbedürftiger erfolgt und zum anderen auch durch Wettbewerber erbracht werden könnte (§ 65 Ziff. 3 AO). Den Hintergrund des **Outsourcings** stellen zudem eigennützige ökonomische Ziele dar, als deren Vehikel die Servicegesellschaft zu gelten hat.

Auch die Übernahme von IT-Dienstleistungen kann einen solchen Servicebetrieb begründen. Dessen Gründung kann sich beispielsweise für eine zentrale Auslagerung der IT-Dienste empfehlen.

> Beispiel Agaplesion: Dort sind alle IT-Service-Leistungen auf eine Servicegesellschaft ausgelagert. Diese stellt auch den (externen) Datenschutzbeauftragten für die Betriebe.

Ist also in diesen Fällen auf das Vorliegen eines wirtschaftlichen Geschäftsbetriebes (Gegenleistung) zu erkennen, so dürfen Mittel aus gemeinnützigkeitsrechtlich privilegierten Quellen für die Ausgliederung nicht verwendet werden. Als Anschaffung einer Beteiligung ist die Kapitalausstattung einer Kapitalgesellschaft als Vermögensumschichtung anzusehen. Gemeinnützigkeitsrechtlich ohne weiteres unbedenklich ist das nur im Falle der Steuerbegünstigung der Empfängerkörperschaft. Anderenfalls dürfen keine zeitnah zu verwendenden Mittel eingesetzt werden. Denn die Empfängerkörperschaft setzt diese Mittel eben nicht zeitnah für steuerbegünstigte Zwecke ein.[434]

Neben dem Aspekt der zeitnahen Mittelverwendung ist auch der **Grundsatz der satzungsgemäßen Mittelverwendung** zu beachten. Sind etwa Dritte auf der Gesellschafterebene der Servicegesellschaft beteiligt, so kann sich ein Verstoß gegen die satzungsgemäße Mittelverwendung durchaus ergeben. Denn dieses Gebot verlangt im Falle der Ausgründung eines steuerpflichtigen wirtschaftlichen Geschäftsbetriebes,[435] dass die gemeinnützige Körperschaft durch die Ausgliederung nicht die **Kontrolle** über das von ihr eingesetzte Vermögen verliert – was einem Verlust des Vermögens gleichkäme. Daher sind Ausgliederungen nur unproblematisch, wenn die ausgliedernde Körperschaft 100% der Anteile an der Ausgliederung hält. Wird dieser Einfluss unterschritten, kann etwa durch einen durch die Dritten zu leistenden **Ausgleich** der Vermögenswerte sichergestellt werden, dass kein Wertverlust erfolgt. Gleichermaßen problematisch ist es, wenn die Anteile später **verkauft** werden sollen.

[427] Es könnte dadurch ferner möglich werden, dass auch der Erwerb bzw. das Halten von Beteiligungen an derartigen steuerbegünstigten Tochter-(Service-)Gesellschaften bzw. die Vermietung von Immobilen für steuerbegünstigte Zwecke auf Ebene der Gesellschafterin der steuerbegünstigten Zweckverwirklichung zugeordnet würde.

[428] Diesem müssen mindestens zwei Drittel der Leistung zugutekommen.

[429] Der BFH und ein wesentlicher Teil der Literatur verstehen Unmittelbarkeit (auch) als „sachliche Nähe“ zwischen dem in

[430] BFH BStBl 13, S. 603.

[431] Siehe BFH BStBl 10, 1006.

[432] Siehe zu diesen auch Weber, Praxisleitfaden: Gründung von Servicegesellschaften, http://www.bkpv.de/ver/pdf/gb2003/weber.pdf (zuletzt abgerufen am 12. August 2020).

[433] Klassische Beispiele sind etwa die Übernahme des Rechnungswesens, eines Wäschereibetriebes, Facility Management, IT-Dienste, Hosting der Website etc.

[434] Auf § 63 Abs. 4 AO, wonach das Finanzamt eine Frist für die Verwendung der Mittel setzen kann, wird hingewiesen. Eine im Vordringen befindliche Meinung betont, dass die Ausgliederung einer Servicegesellschaft dem gemeinnützigkeitsrechtlichen Zweck aufgrund der erreichten Effizienzsteigerung diene. Im Sinne einer Gesamtbetrachtung sei daher auch die Verwendung zeitnah zu verwendender Mittel nicht schädlich. Allerdings entspricht eine solche Gesamtbetrachtung – man mag es bedauern – nicht der Gesetzeslage. Bis zu einer entsprechenden Reform ist daher nicht davon auszugehen, dass die Finanzverwaltung einer entsprechenden Argumentation folgte. Auch § 58 Ziff. 3 AO kann hier nicht weiterhelfen, da es sowohl an der Steuerbegünstigung der Empfängerkörperschaft als auch an der endgültigen Vermögensentäußerung fehlt, wenn die Geberkörperschaft einen Anteil der Empfängerkörperschaft erwirbt.

[435] Es geht hier im Sinnzusammenhang einer Service-Gesellschaft also weder um Vermögensverwaltung noch um die Beteiligung an einer Gesellschaft, die ausschließlich Vermögensverwaltung betreibt oder selbst steuerbegünstigt ist.

Auch die **Preisgestaltung** kann einige Schwierigkeiten bergen. Bei gemeinnützigen Unternehmensverbünden ist sie ist ein „Dauerbrenner“ im Rahmen der steuerlichen Außenprüfung.[436/437] Es empfiehlt sich also bei Festlegung der Vergütungshöhe einen **gut dokumentierten Fremdvergleich** vor Ausführung der Leistung vorzunehmen, der bei Änderung der Umstände zu wiederholen ist. Auch ist vor Leistungserbringung ein **schriftlicher Vertrag** zu schließen, der sämtliche Vertragsbedingungen festhält. Im Falle der Neufassung des § 57 (Abs. 3) AO könnte der Fremdvergleich indes entfallen, da er bei Zweckbetrieben nicht angewendet werden muss.

C.4.8.2.5.7 Einordnung der Einkünfte

Ob die Einkünfte der steuerbegünstigten Körperschaft dem Zweckbetrieb bzw. dem wirtschaftlichen Geschäftsbetrieb **zuzuordnen** sind, muss im Rahmen der Körperschafts- und Gewerbesteuerveranlagung der steuerbegünstigten Körperschaft erwogen werden. Auch die Beteiligung an einer Personengesellschaft, etwa einer GbR zur Durchführung eines gemeinsamen Projekts verschiedener steuerbegünstigter Körperschaften, kann so **Zweckverwirklichung** sein.

Dagegen stellt die Beteiligung an (nicht steuerbegünstigten[!]) Kapitalgesellschaften grundsätzlich **Vermögensverwaltung** dar. Auf das Vorliegen eines steuerpflichtigen wirtschaftlichen Geschäftsbetriebes kann aber erkannt werden, wenn die steuerbegünstigte Körperschaft **entscheidenden Einfluss** auf die Geschäftsführung einer nicht ausschließlich vermögensverwaltenden Körperschaft ausübt, etwa durch Personalunion in der Geschäftsführung, oder eine Betriebsaufspaltung vorliegt.

C.4.8.2.5.8 Beteiligungen an steuerbegünstigten Kapitalgesellschaften

Beteiligungen an **steuerbegünstigten** Kapitalgesellschaften stellen im Regelfall keinen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb dar. Sie werden von der Finanzverwaltung vielfach als der **Vermögensverwaltung** unterfallend angesehen, während die überwiegende Auffassung in der Literatur, jedenfalls bei Ausübung entscheidenden Einflusses auf die Geschäftsführung, eine Zuordnung zum Zweckbetrieb annimmt. Auswirkungen hieraus ergeben sich insbesondere im Hinblick auf die Bildung freier Rücklagen aus Überschüssen. Hier sollte **mit der Finanzverwaltung die Einordnung vorab geklärt** werden.

C.4.8.2.5.9 Vertiefung Ausgliederungen in Tochterkapitalgesellschaften[438]

In einigen Fällen ist die (Aus)Gründung angemessen, zB. wenn ein Pilotprojekt erfolgreich getestet wurde und verstetigt werden soll. Auch können die Bündelung von Knowhow sowie Aspekte der betriebswirtschaftlichen Optimierung das bestimmende Motiv sein. Die Ausgliederung eines steuerpflichtigen wirtschaftlichen Geschäftsbetriebes bietet sich insbesondere dann an, wenn dieser einen **selbständigen Umfang** annimmt, so dass der Gemeinnützigkeitsstatus der Organisation insgesamt gefährdet ist.

Derlei Entscheidungen sollten aber gut durchdacht werden. Insoweit kann sich die Auslagerung der Tätigkeit in eine eigenständige Körperschaft (zB. eine GmbH) empfehlen. Die Anteile an dieser werden dann grundsätzlich[439] im Rahmen der Vermögensverwaltung gehalten, die den Status der Gemeinnützigkeit der Organisation unberührt lässt, sofern die steuerbegünstigte Körperschaft keinen steuernden Einfluss auf die Geschäftsführung der anderen Körperschaft ausübt[440] und auch keine Betriebsaufspaltung vorliegt. Es dürfen natürlich keine zeitnah zu verwendenden Mittel in diesen wirtschaftlichen Geschäftsbetrieb fließen und die Ausstellung von Spendenbescheinigungen ist nicht möglich.

Auch die **Ausgliederung von Zweckbetrieben** ist möglich. Sie ist gemeinnützigkeitsrechtlich zulässig,

[436] Siehe dazu auch die OFD Nordrhein-Westfalen, Verfügung vom 18. Januar 2017 – S 0174-2016/0006-St 15, DStR 2017, S. 1213.

[437] Auf der Ebene der Servicegesellschaft kann beispielsweise eine verdeckte Gewinnausschüttung (vGA) anzunehmen sein; im Falle ihrer Gemeinnützigkeit kommt eine Mitgliederbegünstigung (§ 55 AO) in Betracht. Auf der Ebene der gemeinnützigen Mutter kommen Verstöße gegen die Grundsätze der Ausschließlichkeit (§ 56 AO) bzw. der Mittelverwendung (§ 55 AO) in Betracht. Ein besonderes Spannungsverhältnis kann sich beispielsweise dann ergeben, wenn eine gemeinnützige Körperschaft Leistungen einer Service-Gesellschaft empfängt, deren Gesellschafterin sie ist. Die Vergütung muss dann einerseits so bemessen sein, dass sie aus Sicht der gemeinnützigen Körperschaft angemessen ist, sie darf andererseits weder eine Mittelfehlverwendung, insbesondere keine vGA an die gemeinnützige Gesellschafterin darstellen. Die gemeinnützige Körperschaft darf in einer solchen Konstellation nur einen angemessenen marktüblichen Preis zahlen, wobei die Service-Gesellschaft ihrerseits einen vertretbaren Gewinn einkalkulieren muss, um eine vGA zu vermeiden. Ergibt eine Betriebsprüfung die Überhöhung des Entgelts, kann sich im schlimmsten Fall der Verlust der Gemeinnützigkeit ergeben (vgl. zum Folgenden Schienke-Ohletz/Kühn, Zielkonflikt zwischen Gemeinnützigkeit und Ertragsteuerrecht, DStR 2018, S. 2117).

[438] Siehe in diesem Zusammenhang auch schon oben C.4.8.2.5.6. Insbesondere auch zu den sich ggf. im Rahmen einer Neufassung des § 57 (Abs. 3) AO ergebenden Erleichterungen für Kooperationen.

[439] Lässt sich die Tätigkeit der Kapitalgesellschaft als Zweckbetrieb einordnen, wäre nach Meinung der Literatur auch eine Einordnung als solcher auf Ebene der Gesellschafterinnen möglich. Allerdings dürfte die Finanzverwaltung dieser Argumentation nur selten folgen.

[440] Anderenfalls sieht die Finanzverwaltung gewissermaßen durch die Kapitalgesellschaft hindurch und geht davon aus, dass die steuerbegünstigte Körperschaft am allgemeinen wirtschaftlichen Verkehr teilnimmt. Ist die steuerbegünstigte Körperschaft Mehrheitsgesellschafterin, so kann ihr Weisungsrecht durch die Satzung ausgeschlossen werden oder auf einen Beirat übertragen werden, der allerdings mehrheitlich nicht aus der Geschäftsführung der steuerbegünstigten Körperschaft rekrutiert sein darf. Bei einer AG, bei der es keine Weisungsrechte gibt, gilt das Gesagte gleichermaßen für die Zusammensetzung ihres Vorstands. Verwaltet die Kapitalgesellschaft selbst nur Vermögen, ist eine Weisungsgebundenheit dagegen unproblematisch.

wenn es hierbei zu keinem Vermögensverlust kommt, dem Gebot der Unmittelbarkeit entsprochen wird und die aus dem Gebot der zeitnahen Mittelverwendung resultierenden Einschränkungen beachtet werden. Bei Auslagerung eines Zweckbetriebs auf Tochterkapitalgesellschaften, deren Geschäftsleitungen nicht entscheidend beeinflusst werden können, ist die Beteiligung – nach der Finanzverwaltung – grundsätzlich der Vermögensverwaltung zuzuordnen.

Das hat zur Konsequenz, dass die übertragenen Vermögenswerte bzw. die Beteiligung mit sogenannten nicht zeitnah zu verwendenden Mitteln zu finanzieren sind. Gleiches gilt für die in den übertragenen Zweckbetrieben gebundenen stillen Reserven. Anderenfalls würde ja die Wertsteigerung des bislang steuerbegünstigt eingesetzten Vermögens aus der zeitnahen Verwendungspflicht herausgelöst werden. Um die Grundsätze der Mittelbindung nicht zu verletzen, sollte die Übertragung auf nicht entscheidend beeinflusste Tochterkapitalgesellschaften grundsätzlich zu echten Teilwerten/ Verkehrswerten erfolgen.

Problematisch ist immer die **Beteiligung von Dritten an Ausgliederungen**. Nach dem Gebot der satzungsgemäßen Mittelverwendung darf das gebundene Vermögen der steuerbegünstigten Körperschaft **nicht verloren gehen**. Die Steuerbegünstigung der ausgliedernden Körperschaft ist anderenfalls gefährdet. Bei einem rechtlich selbständigen Rechtsträger, der selbst nicht gemeinnützig ist und nicht nur Vermögensverwaltung betreibt, kann der Vermögensverlust nur durch eine 100%ige Einwirkungsmöglichkeit, also etwa dem Halten aller Anteile an der Gesellschaft, vermieden werden, sofern die Beteiligung selbst keine reine Vermögensverwaltung darstellt. Die Vermögensbindung gerät also in Gefahr, wenn Dritte beteiligt werden, die den eintretenden Verlust dem Wert nach nicht ausgleichen, oder ein späterer Verkauf des Rechtsträgers geplant ist.

C.4.8.2.5.9.1 Besonderheiten zur Umsatzsteuer

Eine Besonderheit ist im Falle der sogenannten **umsatzsteuerlichen Organschaft**[441] zu beachten:

Nimmt eine Tochtergesellschaft nach ihrer Ausgründung Leistungen ihrer Muttergesellschaft (zB. Verwaltungsleistungen) in Anspruch, und ist die Tochter finanziell (Stimmrechtsdominanz), organisatorisch (zB. durch [teilweise] Personalunion in der Führung) und wirtschaftlich (gegenseitige Förderung oder Ergänzung) in das Unternehmen der Gesellschafterin eingegliedert, so unterliegen diese grundsätzlich der Umsatzsteuer, da die Tochter steuerrechtlich gesondert zu betrachten ist. Erbringt nun die Tochter umsatzsteuerfreie Leistungen, ist sie nicht zum Abzug der ihr von der Mutter in Rechnung gestellten Umsatzsteuer berechtigt, ist durch diese also **zusätzlich belastet**.

C.4.8.2.5.10 Mittelweitergabe nach § 58 Ziff. 2 AO

Hinweis:
Zum Zeitpunkt des Redaktionsschlusses ist noch unklar, ob die im Entwurf des Jahressteuergesetzes 2020 beschlossene Neufassung des § 58 AO tatsächlich in Kraft treten wird. Diese sieht eine Vereinheitlichung der Regelungen des § 58 Ziff. 1 und 2 AO vor. Es soll § 58 Ziff. 2 AO ersatzlos entfallen und § 58 Nr. 1 AO ergänzt werden. § 58 Nr. 1 AO-E regelt konkret, dass die Mittelweitergabe an andere steuerbegünstigte Körperschaften unabhängig von ihrer Höhe und einer Zweckidentität möglich sein soll. Die Regelung dessen in der Satzung soll nur für reine Förderkörperschaften erforderlich sein; immer dann also, wenn die Mittelweitergabe die einzige Art der Zweckverwirklichung ist.

Dazu soll eine Vertrauensschutzregelung eingeführt werden. Nach dieser ist der Gute Glaube die Geberkörperschaft geschützt, wenn sie sich die Gemeinnützigkeit der Empfängerkörperschaft hat nachweisen lassen. Der Nachweis kann dabei durch Vorlage der Anlage zum Körperschaftsteuerbescheid oder des Feststellungsbescheids nach § 60a AO erfolgen.

Sofern ein Zweckbetrieb als gemeinnützige Körperschaft Überschüsse generiert,[442] können diese an eine andere gemeinnützige Organisation (beispielsweise die Gesellschafterinnen oder Mitglieder) – quasi als Ausnahme zu § 55 Abs. 1 Ziff 1. AO – im Sinne des § 58 Ziff. 2 AO **weitergeleitet** werden, wenn es sich bei dieser ebenfalls um eine anerkannt

[441] Die umsatzsteuerliche Organschaft bedeutet die finanzielle, wirtschaftliche und organisatorische Eingliederung der Organgesellschaft in das Unternehmen der Organträgerin. Anders als bei der körperschaft- und gewerbesteuerlichen Organschaft ist damit das (zusätzliche) Vorliegen der wirtschaftlichen und organisatorischen Eingliederung erforderlich. Wiederum im Gegensatz zur körperschaft- und gewerbesteuerlichen Organschaft ist ein Gewinnabführungsvertrag indes nicht erforderlich. Das bringt es mit sich, dass die umsatzsteuerliche Organschaft mitunter auch ungeplant entstehen kann, wenn ihre Voraussetzungen gegeben sind, ohne dass dies der Geschäftsleitung bewusst ist.

[442] Die Mittelweiterleitung nach § 58 Ziff. 2 AO ist allerdings nicht auf die Weiterleitung von Überschüssen beschränkt.

gemeinnützige Organisation handelt. Dabei muss sichergestellt sein, dass die Mittel für steuerbegünstigte Zwecke eingesetzt werden.[443]

Zu beachten ist nach der Finanzverwaltung ferner der **Halbteilungsgrundsatz**, dass also die Mittel **nicht überwiegend** weitergegeben werden. Hergeleitet wird dies aus der Gesetzesbegründung, die von einer „teilweisen" Weitergabe spricht. Soll nämlich der Mittelbeschaffungszweck klar im Vordergrund der Tätigkeit der Organisation stehen, ist die Gestaltung der Satzung entsprechend § 58 Ziff. 1 AO angemessen und zumutbar. Der Unterschied der Ziff. 1 und 2 des § 58 AO besteht gerade darin, dass die Weitergabe von Mitteln im Falle der Ziff. 2 kein Satzungszweck zu sein braucht.

Anmerkung:
Rechtsprechung und Wissenschaft gehen mit dieser Maßgabe allerdings gemeinhin **deutlich großzügiger um**.[444] Als erforderlich wird angenommen, dass es nicht sämtliche Mittel sein dürfen, ohne dass ein konkreter Prozentsatz fixiert wird. Auch könnten nach der Rechtsprechung **mitunter verschiedene Veranlagungszeiträume zusammen betrachtet** werden (periodenübergreifende Sicht), so dass die zuwendende Körperschaft nicht in jedem Veranlagungszeitraum Mittel für eigene Zwecke zurückbehalten müsste. Im Einzelfall ist eine frühzeitige Abstimmung mit der Finanzverwaltung zu suchen.

Unter „Mitteln" iSd. § 58 Ziff. 2 AO werden von der Finanzverwaltung nicht nur die in einem Veranlagungszeitraum zufließenden Mittel, sondern – auf der Grundlage sämtlicher Vermögenswerte – das gesamte Nettovermögen (Vermögenswerte abzüglich Verbindlichkeiten) einer Körperschaft verstanden.[445] Wie oben schon angesprochen, können die Mittel – ebenso wie bei § 58 Ziff. 1 AO – auch aus Gewinnausschüttungen aus Vermögensverwaltung oder aus wirtschaftlichem Geschäftsbetrieb stammen.

Da es sich um eine Gewinnausschüttung im Sinne des Gesellschaftsrechts handelt, bedarf es eines **Gewinnverwendungsbeschlusses**. Das **Stammkapital** darf nicht angegriffen werden.

C.4.8.2.5.11 Mittelweitergabe nach § 58 Ziff. 3 AO

Darüber hinaus kann unter bestimmten Voraussetzungen nach § 58 Ziff. 3 AO weitergeleitet werden. So können Gewinne aus den wirtschaftlichen Geschäftsbetrieben ganz oder teilweise einer anderen steuerbegünstigten Körperschaft zur **Vermögensausstattung** zugewendet werden, sofern die aus den Vermögenserträgen zu verwirklichenden steuerbegünstigten Zwecke den steuerbegünstigten satzungsmäßigen Zwecken der zuwendenden Körperschaft entsprechen.[446] Sind die Mittel den zeitnah zu verwendenden Mitteln zuzuordnen, so ist die Weitergabe auf höchstens 15% der nach § 55 Abs. 1 Ziff. 5 AO zeitnah zu verwendenden Mittel begrenzt. Zudem ist eine Kettenweiterleitung ausgeschlossen.

Praxis-Hinweis:
Die Weitergabe von Mitteln zur Vermögensausstattung erfordert eine entsprechende Dokumentation des Vorliegens ihrer gesetzlichen Voraussetzungen, § 63 Abs. 3 AO. Anderenfalls wird schwer nachweisbar sein, dass die Geschäftsführung im Rahmen des § 58 Ziff. 3 AO gehandelt und sich damit innerhalb der Satzung bewegt hat.

C.4.8.2.5.12 Umsatzsteuer

Erfolgt eine Leistung gegen Entgelt, ist sie **grundsätzlich umsatzsteuerpflichtig**, § 1 Abs. 1 Ziff. 1 UStG. Lediglich ideelle Tätigkeiten gehören der nichtunternehmerischen Sphäre an, so dass sie per se nicht umsatzsteuerbar sind. Das heißt im Umkehrschluss, dass sowohl Umsätze im Bereich der Vermögensverwaltung, des steuerpflichtigen wirtschaftlichen Geschäftsbetriebs wie auch des Zweckbetriebs grundsätzlich der Umsatzsteuerpflicht unterfallen. Von dieser Regel macht § 4 UStG weitreichende Ausnahmen zugunsten der Freien Wohlfahrt, insbesondere nach Ziff. 14, 16, 22, 23. Nach Ziff. 18 UStG sind zudem Leistungen der steuerbegünstigten Einrichtungen der Wohlfahrtspflege von der Umsatzsteuer befreit, die **eng mit der Sozialfürsorge und der sozialen Sicherheit verbunden** sind und ohne Gewinnerzielungsabsicht erbracht werden.[447]

Für wirtschaftliche Geschäftsbetriebe, denen keine Umsatzsteuerbefreiung zuteilwird, kann ggf. ein **ermäßigter Steuer-**

[443] Die empfangende/n steuerbegünstigte/n Körperschaft/en kann/können einen anderen steuerbegünstigten Zweck verfolgen als die gebende Körperschaft (siehe auch AEAO zu § 58 Ziff. 2). Nicht durch § 58 Ziff. 2 AO erlaubt sind Zuwendungen für andere als steuerbegünstigte Zwecke (BFH BStBl 12, S. 226). Da allerdings § 58 Ziff. 2 AO keine Ausnahme zum Grundsatz der Ausschließlichkeit (§ 56 AO) begründet, muss die Weitergabe der Mittel auch eigene satzungsmäßige Zwecke erfüllen. Die Tätigkeit darf sich außerhalb des § 57 Abs. 1 S. 2 AO und des § 58 Ziff. 1 AO nicht in der Hingabe von Mitteln – zu denen auch Sachmittel gehören – erschöpfen. Die OFD Münster (20. September 2012 – D 2729-82 – St 13-33) hält im Übrigen dafür, dass der unter zeitnah einzusetzenden Mitteln getätigte Erwerb von Anteilen einer gGmbH gegen das Gebot der Selbstlosigkeit verstieße und auch von § 58 Ziff. 2 AO nicht mehr gedeckt sei. Zur anstehenden Veränderung bei § 58 Ziff. 1 und 2 AO siehe den einleitenden Hinweis sub C.4.8.2.5.10.

[444] Vgl. die Nachweise bei Gersch, in: Klein (Hrsg.), AO, 15. Aufl. 2020, Rz. 3 zu § 58.

[445] Siehe etwa OFD Frankfurt StEd 14, S. 459; AEAO Ziff. 2.2 zu § 58.

[446] Die Finanzverwaltung betont in diesem Zusammenhang, dass die weitergegebenen Mittel nur dem Zweck zugutekommen dürfen, den Geber- und Empfängerkörperschaft übereinstimmend fördern.

[447] Aufgrund der unbestimmten Rechtsbegriffe bestehen allerdings in der Praxis viele Unklarheiten, um deren Beseitigung die Diakonie Deutschland bemüht ist.

satz von derzeit 7% greifen. Das kann nach § 12 Abs. 2 Ziff. 8 lit. a UStG der Fall sein, wenn es sich um einen Zweckbetrieb nach § 65 bis 68 AO handelt und der Zweckbetrieb die fraglichen Leistungen selbst erbringt bzw. der Zweckbetrieb nicht in erster Linie der Erzielung von Umsätzen dient, die in unmittelbarer Konkurrenz zum freien Wettbewerb stehen.

C.4.8.3 Formen der Zusammenarbeit von gemeinnützigen Körperschaften

Für gemeinnützige Organisationen ist es häufig attraktiv, sich zur Erreichung eines gemeinsamen Zwecks, etwa im Rahmen eines besonderen Projekts, zusammenzuschließen. Die Bündelung von Wissen, Sachmitteln und Personalkräften, verbunden mit der durch einen gemeinsamen Auftritt erreichten Außenwirkung und den Vorteilen der Arbeitsteilung, die auch kleineren Organisationen die Mitwirkung an größeren Projekten ermöglicht, führen mitunter zu umfassenden Synergien.

Hinweis:
Zum Zeitpunkt des Redaktionsschlusses ist noch unklar, ob die im Entwurf beschlossene Neufassung des § 57 Abs. 3 AO tatsächlich in Kraft treten wird und dadurch unmittelbar gemeinnütziges Handeln im Sinne der AO schon dann anzunehmen ist, wenn die Organisation planmäßig mit mindestens einer weiteren steuerbegünstigten Organisation planmäßig zusammenwirkt.[448] Die Gesetzesbegründung führt als Beispiel für ein solches planmäßiges Zusammenwirken Wäschereileistungen einer Tochtergesellschaft für den Krankenhausbetrieb der Muttergesellschaft an. Nach bisheriger Rechtslage wurde nur der Krankenhausbetrieb der Muttergesellschaft als Zweckbetrieb eingestuft; die Wäschereileistungen der Tochtergesellschaft waren nicht steuerbegünstigt. Derlei Unternehmen werden bisher als sogenannte Service-Gesellschaften in gewerblicher Form geführt. Aufgrund des gegebenen planmäßigen Zusammenwirkens sollen zukünftig auch die Leistungen der Tochtergesellschaft einen Zweckbetrieb begründen. Das Zusammenwirken beider Gesellschaften wäre dann gemäß § 57 Abs. 3 AO-Entwurf einheitlich zu beurteilen. Damit könnten auch Gesellschaften als gemeinnützig anerkannt werden, die ausschließlich derartige Funktionsleistungen an andere steuerbegünstigte Körperschaften erbringen. Nach aktuellem Stand ist hierfür weder ein Über-Unterordnungs-Verhältnis noch eine Konzernstruktur vorauszusetzen.

Sollte die Gesetzesänderung so beschlossen werden, wären zahlreiche Fragestellungen der Betriebsprüfung, etwa der Abgrenzung von Zweckbetrieb zu steuerpflichtigem Gewerbebetrieb oder der Angemessenheit von Verrechnungspreisen bzw. Gewinnaufschlägen hinfällig.[449]

Die Möglichkeiten der Gestaltung einer solchen Kooperation sind vielfältig, was ihre rechtliche Einordnung mitunter erschwert.[450] Entsprechend vielfältig sind auch die den Kooperationen zugrundeliegenden Kooperationsverträge. Nicht selten fehlt es an einer **klaren Bestimmung der jeweiligen Beiträge**, was zu **tatsächlichen und (steuer)rechtlichen Schwierigkeiten in der Umsetzung** führen kann. In gemeinnützigkeitsrechtlicher Hinsicht sind dabei neben der Frage der zweckentsprechenden Mittelverwendung der Grundsatz der Unmittelbarkeit (§ 57 Abs. 1 AO) und der zeitnahen Mittelverwendung (§ 55 Abs. 1 Ziff. 5 AO) besonders relevant. In einigen Fällen bleibt zum Beispiel unklar, inwieweit die Kooperationspartner eigene Zwecke unmittelbar verwirklichen bzw. die Leistungen einem anderen Kooperationspartner zuzurechnen sein sollen.

Daher ist in der Praxis zu empfehlen, die **Vereinbarungen möglichst klar und konkret** zu fassen. Damit kann insbesondere sichergestellt werden, dass die steuerliche Behandlung wie geplant erfolgt.

Um den Grundsatz der Unmittelbarkeit zu verwirklichen, ist es nicht erforderlich, dass die Beiträge der Kooperationspartner bereits für sich betrachtet die satzungsmäßigen Zwecke verwirklichen. Es reicht vielmehr aus, wenn durch **arbeitsteiliges Zusammenwirken eine gemeinsame Zweckverwirklichung** erfolgt, dass also erst durch das Zusammenwirken der Kooperationsbeiträge die Zweckverwirklichung realisiert wird. Ob jeder einzelne Kooperationspartner seine Zwecke unmittelbar selbst verwirklicht, richtet sich nach der (Mit-)Verantwortung für das Gesamtprojekt (siehe dazu auch C.4.8.6). Beiträge ohne inhaltlichen Einfluss können daher hinter den Anforderungen zurückbleiben.

C.4.8.4 Kooperation und Haftung

Innerhalb von Kooperationen können **unterschiedliche Haftungsrisiken** begründet werden. Jede Kooperationsvereinbarung sollte daher **auch hinreichende Auskunfts- und Nachweispflichten** beinhalten, so zB. zu Tätigkeitspflichten, um den eigenen Pflichten gegenüber der Finanzverwaltung nachkommen zu können. Auch die Vorlage des

[448] Konkretisierungen wird ggf. ein Anfang 2021 zu erwartender Anwendungserlass bringen.

[449] Es könnte dadurch ferner möglich werden, dass auch der Erwerb bzw. das Halten von Beteiligungen an derartigen steuerbegünstigten Tochter-(Service-)Gesellschaften bzw. die Vermietung von Immobilen für steuerbegünstigte Zwecke auf Ebene der Gesellschafterin der steuerbegünstigten Zweckverwirklichung zugeordnet würde.

[450] Beispielsweise kann es sein, dass eine der beteiligten Organisationen im Außenbereich allein auftritt und die weiteren Beteiligten sich auf eine Mitwirkung im Innenverhältnis begrenzen, etwa durch das Bereitstellen von Sachmitteln oder bestimmten Arbeitsergebnissen. Beispielsweise kann es sein, dass eine der beteiligten Organisationen im Außenbereich allein auftritt und die weiteren Beteiligten sich auf eine Mitwirkung im Innenverhältnis begrenzen, etwa durch das Bereitstellen von Sachmitteln oder bestimmten Arbeitsergebnissen.

Feststellungsbescheides nach § 60a AO sollte erfolgen. Schadensersatz- und Strafklauseln können im Einzelfall das Risiko weiter verringern.

C.4.8.5 Gemeinnützigkeitsreform

Lange wurde eine **substanzielle Gemeinnützigkeitsreform** gefordert;[451] insbesondere im Hinblick auf die Vereinfachung der Kooperation steuerbegünstigter Körperschaften und der Mittelweitergabe. Es sieht derzeit danach aus, dass diese Forderungen vom Gesetzgeber umgesetzt werden. Weitere wünschenswerte Veränderungen werden im Folgenden en passant angesprochen.

C.4.8.6 Kooperationen und der Unmittelbarkeitsgrundsatz, GbR und OHG

Hinweis:
Eine Erleichterung für Kooperationen im gemeinnützigen Bereich kann sich zukünftig aus einem neu gefassten § 57 Abs. 3 AO ergeben. Nach dem Entwurf soll das planmäßige Zusammenwirken mit einer weiteren gemeinnützigen Organisation privilegiert werden, was viele bislang bestehende Unklarheiten und Unwägbarkeiten vermeiden könnte. Nähere Einzelheiten sind zum Redaktionsschluss noch nicht bekannt.

§ 57 AO fordert, dass die Satzungszwecke von der Körperschaft selbst verwirklicht werden. Dagegen zeichnen sich Kooperationen naturgemäß durch Arbeitsteilung und Mitwirkung aus. Das Unmittelbarkeitsgebot erscheint so als unmittelbares Hindernis. Wie schwer dieses Hindernis wiegt, hängt von der konkreten Kooperationsform ab.

Für die Gewährung der Steuerbegünstigung ist nach § 57 Abs. 1 AO Voraussetzung, dass die Körperschaft ihre steuerbegünstigten Satzungszwecke unmittelbar verfolgt. Dies kann nach S. 2 der genannten Vorschrift auch durch Hilfspersonen geschehen, wenn das Wirken der Hilfsperson wie eigenes Wirken der Körperschaft anzusehen ist.[453] Als Hilfspersonen kommen natürliche Personen, Personenvereinigungen oder juristische Personen in Betracht.

Sofern durch die Kooperationspartner keine Körperschaften im Sinne des § 1 Abs. 1 KStG, insbesondere Kapitalgesellschaften, Genossenschaften, Vereine und Stiftungen, (aus) gegründet werden, können die Zusammenschlüsse von steuerbegünstigten Körperschaften insbesondere eine Personengesellschaft in Form der GbR (§ 705 BGB) oder gar – in selteneren Fällen – eine Personenhandelsgesellschaft in Form der OHG (§ 105 HGB) ergeben.

In der Praxis bedeutet das: Schließen sich also zwei oder mehrere gemeinnützige Partner zwecks der gemeinsamen Durchführung eines Projektes auf gleicher Stufe zusammen, also ohne dass es zu einer Über- bzw. Unterordnung kommt, dann begründet dieser Zusammenschluss in aller Regel eine Gesellschaft bürgerlichen Rechts, sofern nicht explizit eine andere Rechtsformwahl getroffen wurde. Denn für die Errichtung einer GbR bedarf es **keiner besonderen Form**, sie entsteht **unmittelbar** bereits mit der mündlichen Abrede oder ggf. aus einer willentlichen tatsächlichen gemeinsamen Zweckverfolgung. Sie eignet sich sowohl für die zeitlich begrenzte wie auch die dauerhafte Zusammenarbeit.

Praxis-Hinweis:
In der einfachen Begründbarkeit liegt auch der Grund, warum das Entstehen einer GbR von ihren Gesellschaftern **häufig unerkannt** bleibt. Das ist insofern **problematisch**, weil das Vorliegen einer GbR **erhebliche steuerliche Folgen** auslösen kann. Auch eine GbR kommt als Umsatzsteuersubjekt in Betracht und kann einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb begründen. Im Folgenden werden Hinweise dazu gegeben, wie unbeabsichtigte steuerliche Folgen vermieden werden.

Um eine GbR zu gründen, ist die rechtsverbindliche Verabredung zur Förderung eines **gemeinsamen Zwecks** notwendig. Dieses gemeinsame Ziel kann etwa die Verwirklichung eines gemeinsamen Projektes sein, wobei sich die Partner darüber einigen, wer welchen konkreten **Beitrag** zur Zweckverwirklichung leistet.[454] Der jedenfalls vorauszusetzende **Rechtsbindungswille** muss über ein bloßes Zusammenwirken als rein faktische Tatsache hinausgehen. Im Falle einer ausdrücklichen Vereinbarung dürften **selten Probleme** entstehen.

Gesellschaftsvertragliche Vereinbarungen zur Gründung einer GbR können grundsätzlich aber auch **formlos** erfolgen.[455] Ein wichtiges Indiz hierfür ist das **feststellbare Interesse** eines jeden Kooperationspartners an der Erreichung des Gesellschaftszwecks im Sinne des jeweiligen Satzungszweckes und eine feststellbare Verpflichtung, den gemeinsamen Zweck zu fördern.

Eine **OHG** kann dann gegeben sein, wenn zusätzlich zu dem Vorgenannten der gemeinsame Zweck auf den Betrieb eines

[451] Siehe etwa Schauhoff, Die Gemeinnützigkeitsreform kommt, in: npoR 2020. Es ist insbesondere zu hoffen, dass die Gemeinnützigkeitsreform hier Abhilfe schaffen wird und der Geschäftsführung eines gemeinnützigen Unternehmens mehr Entscheidungsspielraum einräumen wird. Entsprechend der Business-Judgment-Rule sollte pflichtgemäßes Ermessen schon dann bejaht werden, wenn die Geschäftsführung vernünftiger Weise annehmen darf, auf der Grundlage adäquater Information angemessen zur Förderung des Zwecks zu handeln. Siehe hierzu näher Schauhoff, a.a.O., S. 4. Die derzeit diskutierte Stiftungsrechtsreform sieht die Einführung dieser Regel vor.

[452] Konkretisierungen wird ggf. ein Anfang 2021 zu erwartender Anwendungserlass bringen.

[453] Siehe zur Hilfsperson auch: C.4.8.6.1

[454] Typisch für gemeinnütziges Wirken ist, dass zwei gemeinnützige Körperschaften eine Arbeitsgemeinschaft bilden, um auf eine gemeinschaftliche, gemeinnützige Zweckverwirklichung abzuzielen. Denkbar ist aber auch die Begründung einer Arbeitsgemeinschaft mit steuerpflichtigen Anbietern.

[455] Anders etwa bei der Einbringung von Grundstücken oder der Begründung von Erwerbspflichten der beitretenden Gesellschafter. Der Vertragsschluss begründet die GbR zumindest als schuldrechtliche Innengesellschaft. Durch die Teilnahme am Rechtsverkehr kann sie als Außen-GbR zum verselbstständigten Rechtssubjekt erwachsen.

Handelsgewerbes unter gemeinschaftlicher Firma gerichtet ist. Als Handelsgewerbe kommt grundsätzlich jeder Gewerbebetrieb in Betracht, es sei denn, dass das Unternehmen nach Art oder Umfang einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb nicht erfordert, § 1 Abs. 2 HGB.[456]

Für beide Gesellschaftsformen gilt aber, dass sie das **Privileg der Gemeinnützigkeit ganz grundsätzlich**[457] **nicht erlangen können**. Gemäß § 51 Abs. 1 S. 2 AO ist dieses den Körperschaften, Personenvereinigungen und Vermögensmassen im Sinne des § 1 Abs. 1 KStG vorbehalten. Die nach §§ 51 bis 68 AO möglichen steuerlichen Vergünstigungen können also nur von diesen in Anspruch genommen werden,[458] von den Personen(handels)gesellschaften – nach aktueller Lesart – hingegen nicht.

Hintergrund-Anmerkung:
Die **Gemeinnützigkeitsunfähigkeit von Personen-(handels)Gesellschaften** wird gemeinhin mit dem Hinweis darauf erklärt, dass selbstloses Handeln praktisch nur bei Körperschaften sichergestellt werden könne. Dem ist allerdings entgegenzuhalten, dass die Verselbständigung der Gesellschaftssphäre gegenüber der Gesellschaftersphäre zivilrechtlich schon lange angenommen wird. Dass sich die Frage der Gemeinnützigkeit aber auch ohnehin weniger als Frage der Rechtsform stellt, zeigt auch das Beispiel der Ein-Mann-GmbH, die zwar nach derzeitiger Rechtslage ihrer Rechtsform nach unproblematisch gemeinnützig sein kann, deren tatsächliche Gemeinnützigkeit im Hinblick auf ihre Gesellschafterstruktur aber mitunter weniger sichergestellt werden kann, als bei einer GbR und die auch gegenüber der Ein-Mann-GmbH & Co. KG insoweit keinen entscheidenden Vorteil bringt.[459]

Personengesellschaften (wie OHG, KG und GbR) sind die Steuervergünstigungen ebenso wenig eröffnet wie Privatpersonen. Daraus darf aber nicht geschlossen werden, dass die Rechtsformen der Personengesellschaften im gemeinnützigen Sektor per se ohne Funktion blieben. Im Gegenteil: Gerade die Gesellschaft bürgerlichen Rechts kann eine sinnvolle gesellschaftsrechtliche Form für eine Kooperation zwischen gemeinnützigen Unternehmen darstellen.[460]

Auch das Gebot der unmittelbaren Zweckverwirklichung steht der Begründung einer GbR grundsätzlich nicht entgegen. Denn „unmittelbar“ in diesem Sinne bedeutet nicht „allein“ oder „allein verantwortlich“. Es genügt bereits eine **Mitverantwortung** dergestalt, dass das Projekt auch als eigenes Projekt der fraglichen Körperschaft angesehen werden kann.

Allerdings erfolgt die gemeinnützigkeitsrechtliche Einordnung einer Personengesellschaft **nicht automatisch**. Aufgrund der Ausgrenzung aus dem steuerrechtlich zentralen Begriff der Körperschaft ist zur Bestimmung der Gemeinnützigkeit **nicht** auf die Personengesellschaft selbst abzustellen. Ihr fehlt die eigene sogenannte Steuersubjektivität, so dass insoweit auf die Ebene der Gesellschafter abgestellt werden muss. Es wird quasi durch die Personengesellschaft **hindurch** auf die Ebene der Gesellschafterinnen geschaut.[461] Entscheidend ist , wie die Tätigkeit der Personengesellschaft im Hinblick auf ihre Gesellschafterinnen wirkt, was nach den allgemeinen Grundsätzen zu behandeln ist. Insoweit kann eine Zurechnung nach § 57 Abs. 1 S. 2 AO in Betracht kommen, also über das Konstrukt der Hilfsperson (siehe zu dieser auch C.4.8.6.1).

Für die Annahme der Unmittelbarkeit ist es nicht erforderlich, dass die Tätigkeiten eines/r Gesellschafters/in für sich genommen und losgelöst von den Beiträgen der weiteren Kooperationspartnerinnen die gemeinnützigen Zwecke verwirklicht. Es genügt die gemeinsame Zweckverwirklichung durch **arbeitsteiliges Zusammenwirken**, so dass **erst kumulativ** durch die weiteren Beiträge die Zweckverwirklichung anzunehmen ist. Ob die eigenen Zwecke selbst unmittelbare Verwirklichung finden, richtet sich nach der (Mit-)Verantwortung der einzelnen Gesellschafterin für alle einschlägigen Projektbeiträge.

Der Beitrag einer oder mehrerer Gesellschafterinnen kann sich aber auch auf rein finanzielle oder sachliche Leistungen beschränken. In diesen Fällen fehlt es an einem eigenen operativen Beitrag. Eine gemeinnützigkeitsrechtliche Zurechnung über die Hilfsperson ist ebenfalls nicht möglich. Es kommt aber eine Unterstützung nach § 58 Ziff. 1 bis 5 AO in Betracht.

Die **Abgrenzung zum Einsatz einer Hilfsperson** kann in der Praxis schwierig sein, insbesondere wenn die Unterstützung mit weitreichenden Auflagen zur Mittelverwendung verbunden ist. Anders als beim Einsatz als Hilfsperson setzt die Empfängerkörperschaft die empfangenen Mittel jedenfalls für eigene satzungsmäßige Zwecke ein. Sie darf der Förderkörperschaft keine bestimmte Gegenleistung schulden. Es darf also kein Austauschverhältnis vorliegen.

[456] Dann liegt ein Kleingewerbe vor, dass den Regelungen des HGB grundsätzlich nicht unterfällt.

[457] Ganz ausnahmsweise können besondere Gestaltungen möglich sein. So beispielsweise im nichtgewerblichen Bereich (Vermögensverwaltung) und dann, wenn die Mitunternehmerschaft aufgrund besonderer „stiftungsnaher“ Gestaltung fehlt, etwa weil eine Gesellschafterin bei Leistung eines festen Beitrags vom Mitunternehmerrisiko ausgeschlossen ist, die andere Gesellschafterin ohne Einlage die Geschäfte der Gesellschaft im Außenverhältnis führt, weder aber am Ergebnis partizipiert noch hinsichtlich der Zweckverwirklichung eigenständige Unternehmerinitiative entwickeln darf (vgl. Geibel, in: Winheller, Geibel, Jachmann-Michel, Gesamtes Gemeinnützigkeitsrecht, 2. Aufl. 2020, 3.9, Rz. 9 – 15).

[458] Dabei handelt es sich um: Kapitalgesellschaften (AG, Europäische Gesellschaften, KG auf Aktien, Gesellschaften mit beschränkter Haftung [insbesondere die gGmbH]); Erwerbs- und Wirtschaftsgenossenschaften; Versicherungsvereine auf Gegenseitigkeit; sonstige juristische Personen des privaten Rechts; nichtrechtsfähige Vereine, Anstalten, Stiftungen und andere Zweckvermögen des privaten

[459] Siehe insgesamt Hüttemann, Gemeinnützigkeits- und Spendenrecht, 4. Aufl. 2020; Rz. 2.93 (S. 137); ferner Stock: Wahl der Rechtsform im gemeinnützigen Nonprofit-Bereich, NZG 2001, S. 440 (443).

[460] Weitere Nachweise bei Hüttemann, Gemeinnützigkeit und Spendenrecht, Rz. 2.95.

[461] Nach diesem Transparenzprinzip können die Vermögenswerte einer Personengesellschaft nach § 39 Abs. 2 Ziff. 2 AO anteilig als „eigene“ Mittel der steuerbegünstigten Gesellschafter anzusehen sein. Im Gewerbe- und Umsatzsteuerrecht sind Personengesellschaften indes eigene Steuerrechtssubjekte. Eine Befreiung sieht der Gesetzgeber nur in § 12 Abs. 2 Ziff. 8 lit. b UStG vor. Entsprechendes fehlt in § 3 GewStG. Die Gewerbesteuerbefreiung der ggf. gewerbesteuerbefreiten Gesellschafter greift insoweit also nicht.

Exkurs zur Mittelweitergabe nach § 58 Ziff. 1 AO[462]

Hinweis:
Zum Zeitpunkt des Redaktionsschlusses ist noch unklar, ob die im Entwurf des Jahressteuergesetzes 2020 beschlossene Neufassung des § 58 AO tatsächlich in Kraft treten wird. Diese sieht eine Vereinheitlichung der Regelungen des § 58 Ziff. 1 und 2 AO vor. Es soll § 58 Ziff. 2 AO ersatzlos entfallen und § 58 Nr. 1 AO ergänzt werden. § 58 Nr. 1 AO-E regelt konkret, dass die Mittelweitergabe an andere steuerbegünstigte Körperschaften unabhängig von ihrer Höhe und einer Zweckidentität möglich sein soll. Die Regelung dessen in der Satzung soll nur für reine Förderkörperschaften erforderlich sein; immer dann also, wenn die Mittelweitergabe die einzige Art der Zweckverwirklichung ist.

Dazu soll eine Vertrauensschutzregelung eingeführt werden. Nach dieser ist der Gute Glaube die Geberkörperschaft geschützt, wenn sie sich die Gemeinnützigkeit der Empfängerkörperschaft hat nachweisen lassen. Der Nachweis kann dabei durch Vorlage der Anlage zum Körperschaftsteuerbescheid oder des Feststellungsbescheids nach § 60a AO erfolgen.

Kommt im Einzelfall eine Mittelweitergabe als Kooperationsbeitrag nach § 58 Ziff. 1 AO in Betracht, so sind – jedenfalls bis zu einer ggf. erfolgenden Anpassung der Gesetzeslage – einige Punkte zu beachten, um die steuerliche Unschädlichkeit der Weitergabe zu sichern. So setzt eine entsprechende Weitergabe voraus, dass die

- Satzung der Förderkörperschaft eine Weitergabe zulässt, und

die Empfängerkörperschaft selbst

- als steuerbegünstigt anerkannt ist und
- die Mittel tatsächlich für die Verwirklichung der eigenen steuerbegünstigten Zwecke einsetzt.[463]

Lässt man die Weisungsgebundenheit, dh. die willentliche Einbindung in die Verwirklichung der eigenen gemeinnützigen Zwecke, für das Vorliegen einer Hilfspersonentätigkeit als Kriterium gelten, kann hiermit eine erste Abgrenzung erfolgen. Eine Mittelweiterleitung kommt bei Fehlen der Weisungsgebundenheit **statt** der Hilfspersonentätigkeit in Betracht.

Praxis-Hinweis:
Im Rahmen einer Kooperation sind die gewollte Konstruktion und die einzelnen Beiträge der Kooperationspartnerinnen vertraglich **sehr klar zu bezeichnen und zu regeln**, da anderenfalls eine **abweichende rechtliche Einordnung** der Beiträge durch die Finanzverwaltung erfolgen kann. Fehlt dann die **satzungsgemäße Grundlage für die Leistungen**, können diese zu einem gemeinnützigkeitsrechtlichen Verstoß führen.

C.4.8.6.1 Die Hilfsperson

Anmerkung:
Zur Verdeutlichung wird im Folgenden bezüglich der Hilfsperson auf die GbR zurückgegriffen. Allerdings kann auch jede andere Organisationsform die Eigenschaft einer Hilfsperson annehmen, beispielsweise eine gGmbH oder eine Genossenschaft etc. Die folgenden Ausführungen gelten dann im übertragenen Sinne.

Vermittels des Instruments der Hilfsperson (§ 57 Abs. 1 S. 2 AO) kann die Tätigkeit der GbR ihren Gesellschaftern unter Umständen als unmittelbares Wirken im gemeinnützigkeitsrechtlichen Sinne **zugerechnet** werden. Das ist dann der Fall, wenn das Wirken der GbR wie eigenes Wirken der Gesellschafter anzusehen ist; was sich wiederum nach den Umständen des Einzelfalls richtet. Ausschlaggebend sind vor allem die **rechtlichen und tatsächlichen Beziehungen**, die zwischen der GbR und ihren Gesellschaftern bestehen. Die tatsächlichen Verhältnisse müssen den Vereinbarungen entsprechen. Die einsetzende Körperschaft muss daher auch **ggf. durch Kontrollen sicherstellen**, dass die Vereinbarungen auch **eingehalten** werden.[464]

[462] Vgl. zum Folgenden im Einzelnen Weiten/Marquardsen, Gemeinnützigkeitskonforme Mittelweitergabe durch Förderkörperschaften, DStR 3/2020, S. 85ff.

[463] Darüber hinaus ist fraglich, ob und inwieweit eine Übereinstimmung der steuerbegünstigten Satzungszwecke zwischen der mittelbeschaffenden und der mittelempfangenden Körperschaft übereinstimmen müssen (Zweckidentitätsgebot). Bis zur gesetzlichen bzw. höchstrichterlichen Klärung ist die Beachtung folgender Grundsätze angezeigt: Für den Fall, dass die Zwecke nicht übereinstimmen, sollte die Mittelweitergabe zunächst unterbleiben. Sofern sie vollständig übereinstimmen, dürfte selbst eine freie Zuwendung unschädlich sein. Sofern sie teilweise übereinstimmen, ist zu unterscheiden: fördert die Förderkörperschaft weitere Zwecke, dürfte selbst eine freie Zuwendung unschädlich sein; fördert die Empfängerkörperschaft weitere Zwecke, sollte die Weitergabe zweckgebunden (auf die Übereinstimmung bezogen) erfolgen. Noch ist unklar, ob unter § 58 Ziff. 1 AO – in seiner bisherigen Fassung – auch die unentgeltliche oder verbilligte Erbringung von Dienstleistungen zu fassen sein kann. Des Weiteren ist entsprechend auch noch unklar, ob (im Holdingverbund) unentgeltlich oder verbilligt überlassene Sachmittel von der Geberkörperschaft mit zeitnah zu verwendenden Mitteln finanziert werden dürfen. Die Diakonie Deutschland bemüht sich auch hier um eine Abhilfe. Ist einer oder sind beide Punkte für die Planung erheblich, sollte möglichst früh mit der Finanzverwaltung die Klärung in diese Richtung versucht werden.

[464] Um als Hilfsperson iSd. § 57 Abs. 1 S. 2 AO anerkannt zu werden, muss die Tochtergesellschaft nicht nach außen hin im Namen und auf Rechnung der Mutterkörperschaft auftreten. Der Nachweis der Abreden im Innenverhältnis ist ausreichend. Ist beispielsweise zwischen der Mutterkörperschaft und ihrer Tochtergesellschaft ein Beherrschungsvertrag iSd. § 291 AktG gegeben bzw. steht die Tochtergesellschaft unter der einheitlichen Leitung der Mutterkörperschaft, ist (unwiderlegbar) zu vermuten, dass die Tochtergesellschaft als Hilfsperson i. S. von § 57 Abs. 1 Satz 2 AO tätig wird. Ist die Tochtergesellschaft als Hilfsperson anzuerkennen, kann ihr Stamm- bzw. Grundkapital im Einklang mit § 55 Abs. 1 Nr. 5 AO aus zeitnah zu verwendenden Mitteln stammen. Bei Fremdfinanzierung des Beteiligungsengagements können die Zins- und Tilgungsverpflichtungen zudem mit zeitnah zu verwendenden Mitteln erfüllt werden.

Vorbehaltlich einer abweichenden Vereinbarung steht nach dem Gesellschaftsvertrag die Führung der Geschäfte allen Gesellschaftern **gemeinsam** zu; Beschlüsse sind einstimmig zu treffen. Vor dem Hintergrund einer derart umfassenden Einwirkungsmöglichkeit der Gesellschafter und damit gegebenen Weisungsgebundenheit der GbR, ist das Wirken der GbR grundsätzlich allen Projektpartnern im genannten Sinne zuzurechnen. Anderes könnte aber dann gelten, wenn die Mitwirkung einzelner Gesellschafter nach dem Gesellschaftsvertrag ausgeschlossen oder erheblich beschränkt ist, so dass die betreffende Körperschaft **ohne wesentlichen Einfluss** auf die Tätigkeit der GbR bleibt. Durch Vorlage von Vereinbarungen muss die steuerbegünstigte Körperschaft gegenüber der Finanzverwaltung – schriftlich – nachweisen, dass sie Inhalt und Umfang der Tätigkeit der Hilfsperson **im Innenverhältnis bestimmen** kann (AEAO zu § 57 Ziff. 2 S. 4). Es muss auch ersichtlich sein, wie die Hilfsperson **Rechenschaft** ablegt. Zudem ist die **Überwachung** der Hilfsperson sicherzustellen (AEAO zu § 57 Ziff. 2 S. 6).

C.4.8.6.2 Checkliste: Vereinbarung der Einschaltung als Hilfsperson[465]

Die schriftliche Vereinbarung mit einer ggf. einzuschaltenden Hilfsperson sollte – um Schwierigkeiten mit der Finanzverwaltung zu vermeiden – Folgendes beinhalten:

- das Verständnis, dass eine der Vertragsparteien die Hilfsperson iSd. § 57 Abs. 1 S. 2 AO der diese einsetzenden Körperschaft ist;
- dass die Hilfsperson bei der Verwendung der ihr zugewendeten Mittel den Weisungen der sie einsetzenden Körperschaft unterliegt;
- dass die einsetzende Körperschaft den Inhalt und den Umfang der Tätigkeit der Hilfsperson im Innenverhältnis bestimmen kann;
- die Tätigkeit der Hilfsperson den Satzungsbestimmungen der einsetzenden Körperschaft entsprechen muss;
- die einsetzende Körperschaft die Tätigkeit der Hilfsperson überwachen und die weisungsgemäße Verwendung der Mittel sicherstellen kann; und
- dass die Hilfsperson, sofern sie die Mittel der einsetzenden Körperschaft an eine weitere Hilfsperson weitergeben darf, sich zum Abschluss einer entsprechenden eigenen schriftlichen Vereinbarung mit der weiteren Hilfsperson im Sinne der einsetzenden Körperschaft verpflichtet.

Hinweis:
Zu Recht wird kritisiert, dass ein derart starkes Einwirken nicht notwendig ist.[466] Die Praxis ist häufig überfordert. Allein die willentliche Einschaltung eines Dritten in die Verwirklichung der eigenen Zwecke sollte zukünftig von der Finanzverwaltung als ausreichend anerkannt werden.

Gemeinnützigkeitsrechtlich relevant ist ferner, dass die Hilfsperson **sowohl die gemeinnützigen Zwecke ihrer Gesellschafterinnen wie auch die eigenen Satzungszwecke** verfolgen kann.[467] Das Handeln als Hilfsperson allein begründet die Steuerbegünstigung der eigenen Tätigkeit noch nicht, da die Hilfsperson zunächst nur fremde (etwa der Gesellschafter oder Auftraggeber)[468] gemeinnützige Zwecke verwirklicht.

Anders ist dies, wenn die Hilfsperson **zugleich auch eigene** steuerbegünstigte Satzungszwecke verfolgt.[469] Um steuerbegünstigt zu sein, muss die als Hilfsperson tätige Organisation also alle Voraussetzungen der §§ 51 ff. AO erfüllen, insbesondere auch iSv. § 57 AO unmittelbar selbst einen steuerbegünstigten Zweck erfüllen.[470]

Hinweis:
In diesem Zusammenhang zeigt sich ein Zielkonflikt: Um noch von einer eigenen Tätigkeit im Sinne des § 57 Abs. 1 S. 1 AO ausgehen zu können, muss der Hilfsperson trotz der nach § 57 Abs. 1 S. 2 AO zugunsten der Gesellschafter vorauszusetzenden Weisungsgebundenheit ein gewisser eigener Spielraum zur eigenverantwortlichen Handlungsgestaltung bleiben. Daher wird zuweilen nur verlangt, dass die Tätigkeit immerhin im Wesentlichen veranlasst ist. Auch nach dem BFH ist es nicht notwendig, dass die Körperschaft auf die konkrete Abwicklung der Tätigkeit Einfluss nimmt.[471] Idealerweise wird der Hilfsperson im Sinne einer Zieldimension also vorgegeben, welche Aufgabe zu erfüllen ist. Andererseits wird der Hilfsperson bei der Verwirklichung so viel Raum gelassen, dass sie die Tätigkeit selbständig und eigenverantwortlich realisieren kann.

[465] Die konkrete Ausgestaltung sollte im Einzelfall steuer- bzw. rechtsberatend begleitet werden.
[466] Nach Auffassung der Literatur (und Teilen der Rechtsprechung [FG Niedersachsen, Entscheidung vom 08. April 2010, 6 K 139/09]) ist eine Weisungsgebundenheit nicht erforderlich. Maßgeblich sei lediglich, ob die gemeinnützige Körperschaft die Hilfsperson willentlich eingeschaltet habe.
[467] Nach der Entscheidung des BFH vom 17. Februar 2010 (IR 2/08), BStBl. II 2010, 1006, Rz. 24, ist es nicht mehr fraglich, ob eine Hilfsperson gleichzeitig eigene wie fremde steuerliche Zwecke verwirklichen kann. AEAO zu § 57 Ziff. 2 S. 9 vollzieht dies ausdrücklich nach.
[468] Neben Zusammenschlüssen auf gesellschaftsrechtlicher Ebene kommen auch Auftragsverhältnisse in Betracht. Wichtig ist stets, dass die jeweils infrage stehenden Beiträge „selbständig und eigenverantwortlich“ erbracht werden.
[469] Das ist insbesondere dann nicht der Fall, wenn die Hilfsperson Dienstleistungen gegenüber der sie einschaltenden Körperschaft erbringt.
[470] BFH BStBl 13, 603; BMF BStBl I 03, 107. Mittlerweile ist es insbesondere nicht mehr fraglich, dass eine Hilfsperson gleichzeitig eigene wie fremde steuerliche Zwecke verwirklichen kann (s.o. Fn. 303). Von der Verfolgung eigener satzungsmäßiger Zwecke ist im Regelfall auszugehen, wenn mehrere nach § 5 Abs. 1 Nr. 9 KStG steuerbefreite Körperschaften arbeitsteilig zur Verwirklichung eines steuerbegünstigten Zwecks zusammenwirken. Insoweit kommen nicht nur Zusammenschlüsse auf gesellschaftsrechtlicher Grundlage in Betracht, sondern auch Fälle, in denen beispielsweise eine steuerbefreite Organisation, die öffentlich mit der Erbringung der steuerbegünstigten Tätigkeit beauftragt ist, einzelne Tätigkeiten an andere steuerbefreite Körperschaften vergibt (BFH, Urteil vom 17. 2. 2010 - I R 2/08, DStRE 2010, S. 755 [756f.]).
[471] Nachweise bei Schunk, DStR 2014, S. 934, 937.

In der Praxis wird das Vorliegen der umsatzsteuerlichen Organschaft in der Regel als wichtiges Indiz für das Vorliegen einer Hilfsperson angenommen.

Wie oben gesehen, ist das für die GbR allerdings nicht möglich, da es ihr an dem vorauszusetzenden Körperschaftscharakter (§ 1 KStG) fehlt. Auch dann, wenn die GbR keine wirtschaftliche Tätigkeit im Sinne des § 14 AO ausübt, also allein der ideellen Zweckerfüllung dient, kann sie den Status der Steuerbegünstigung nicht erreichen. Solange sie keine Einnahmen bzw. nur Einnahmen unterhalb der steuerlichen Freigrenze erzielt, ist dies aber im Ergebnis unproblematisch.

Sobald eine GbR bei Überschreitung der Freigrenzen auch der Erzielung von Einnahmen dient (auch wenn nur ein „Unkostenbeitrag“ erhoben wird), wird ohnehin ein (ggf. steuerpflichtiger) wirtschaftlicher Geschäftsbetrieb zu bejahen sein, wenn von einer selbständigen und nachhaltigen Tätigkeit auszugehen ist. Auf Ebene der GbR fällt ggf. Gewerbesteuer an (siehe dazu sogleich C.4.8.6.3.1). Das Privileg der Gemeinnützigkeit lässt sich dann für ihre Gesellschafterinnen überhaupt nur noch auf deren Ebene im Rahmen eines Zweckbetriebes aufrechterhalten.

(Auch) die Beteiligung an einer Personengesellschaft kann dabei als Zweckbetrieb iSd. §§ 65 ff. AO zu qualifizieren sein, wenn das Handeln der Tochterpersonengesellschaft den steuerbegünstigten Satzungszwecken der Mutterkörperschaft entspricht und die Voraussetzungen der Zurechnung als Hilfsperson nach § 57 Abs. 1 Satz 2 AO vorliegen.

Hinweis:
Da das Verhalten der Hilfsperson der Geberkörperschaft wie eigenes Wirken zugerechnet wird, ist beispielsweise eine Mittelfehlverwendung durch die Hilfsperson für die Geberkörperschaft selbst schädlich.

C.4.8.6.3 Steuerliche Aspekte der Kooperation im Rahmen der GbR

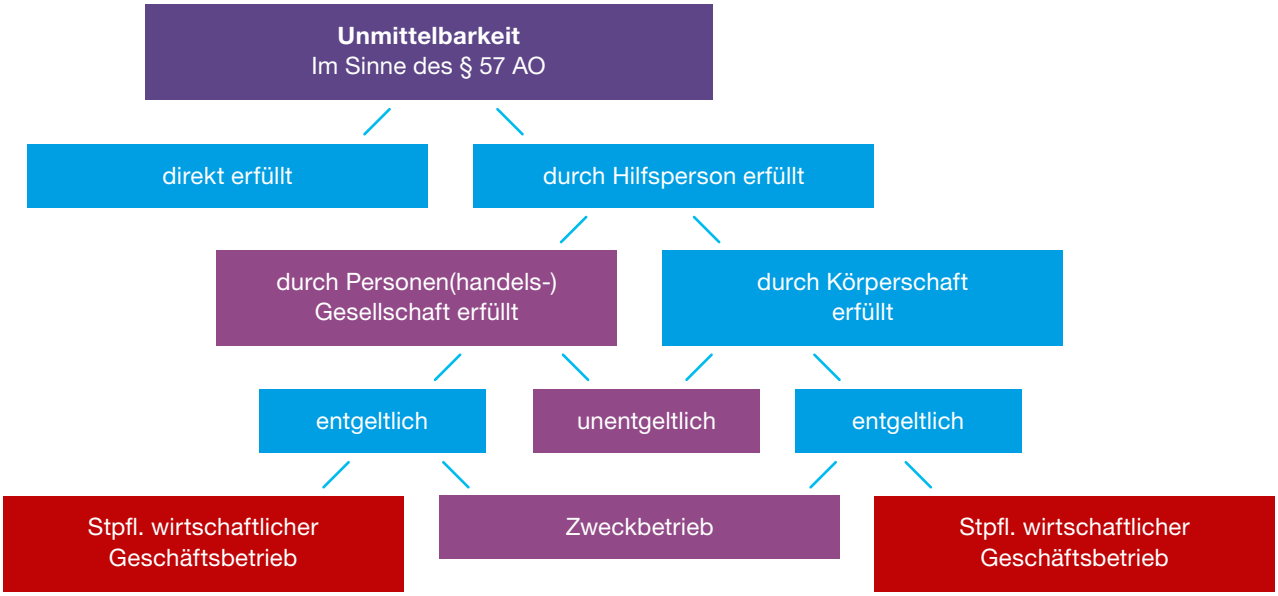


Fig. C12: Die gemeinnützigkeitsrechtlichen Auswirkungen der Einschaltung einer Hilfsperson zur Zweckerreichung (in Ansehung ihrer Rechtsform und der Frage der Entgeltlichkeit der Leistung) auf die Körperschaft. Vorausgesetzt wird, dass das Wirken der Hilfsperson aufgrund der (gesellschafts-)vertraglich geregelten Befugnisse der Körperschaft wie eigenes Wirken zugerechnet werden kann.

Ist die Personengesellschaft nicht lediglich vermögensverwaltend tätig, beziehen gemeinnützige Körperschaften **kraft Rechtsform** grundsätzlich gewerbliche Einkünfte, so dass schon auf Ebene der Personengesellschaft gewerbliche Einkünfte vorliegen können.[472] Die Einkünfte der Personengesellschaft sind den beteiligten Gesellschafterinnen nach dem Transparenzprinzip zuzurechnen. Da die Personengesellschaft ein vorgelagertes Subjekt der Einkünfteerzielung und -Ermittlung darstellt, wird ihr Gewinn in einem ersten Schritt zunächst nach § 180 Abs. 1 Ziff. 2 lit. a AO einheitlich und gesondert festgestellt, um dann in einem zweiten Schritt ihren Gesellschaftern anteilig zugerechnet zu werden. Örtlich zuständig ist das Betriebsstättenfinanzamt, § 18 Abs. 1 Ziff. 2 AO. Die von diesem festgestellte Natur der Einkünfte – gewerblich oder nicht – ist auch für die Ebene der Gesellschafter grundsätzlich bindend (AEAO Ziff. 3 S. 1 zu § 64). Das jeweilige Veranlagungsfinanzamt entscheidet auf zweiter Ebene allerdings darüber, ob ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb oder ein Zweckbetrieb vorliegt (AEAO Ziff. 3 S. 2 zu § 64). In letzterem Falle sind die anteiligen Einkünfte nach § 5 Abs. 1 Ziff. 9 KStG von der Ertragsteuer befreit.

C.4.8.6.3.1 Besonderheiten bezüglich GbR und Gewerbesteuer

Problematisch bei der Ausgestaltung einer Kooperation in Form einer GbR ist derzeit noch ein besonderer steuerrechtlicher Umstand: Während die GbR nach der Systematik des Einkommen- und Körperschaftsteuerrechts – namentlich dem Transparenzprinzip – kein Steuersubjekt sein und also die Privilegierungen der §§ 51ff. AO auch nicht für sich beanspruchen kann (dies können nur die beteiligten Körperschaften als Gesellschafterinnen), sieht das Gewerbesteuerrecht aufgrund seines Objektsteuercharakters die GbR sehr wohl als Steuersubjekt an.[473] Begründet die Kooperation zweier oder mehrerer gemeinnütziger Träger eine Tätigkeit, die als Gewerbebetrieb nach § 15 Abs. 2 EStG anzusehen ist, laufen daraus resultierende Gewinne nach § 2 Abs. 1 S. 2 GewStG Gefahr, als **gewerbesteuerpflichtig** behandelt zu werden. Im Bereich der Gewerbesteuer fehlst es an einem (umfassenden) **ausdrücklichen** Befreiungstatbestand für personengesellschaftsrechtliche Kooperationsformen.[474]

Praxis-Hinweis:
Die GbR kann **im Falle formeller Satzungsmäßigkeit**[475] versuchen, sich auf die Befreiung nach § 3 Nr. 6 GewStG zu berufen.[476/477] Hierzu ist allerdings **sowohl eine entsprechende Beratung als auch vorherige Abstimmung mit der Finanzverwaltung dringend** zu empfehlen.

Nach § 180 AO werden folgerichtig die Einkünfte einer GbR einheitlich und gesondert – einschließlich der Einkunftsart(en) – festgestellt. Ziff. 3 zu § 64 AEAO besagt entsprechend:

> „Ob eine an einer Personengesellschaft oder Gemeinschaft beteiligte steuerbegünstigte Körperschaft gewerbliche Einkünfte bezieht, wird im gesonderten und einheitlichen Gewinnfeststellungsbescheid der Personengesellschaft bindend festgestellt (BFH-Urteil vom 27.7.1988, I R 113/84, BStBl. 1989 II S. 134). Ob ein steuerpflichtiger wirtschaftlicher Geschäftsbetrieb oder ein Zweckbetrieb (§§ 65 bis 68 AO) vorliegt, ist dagegen bei der Körperschaftsteuerveranlagung der steuerbegünstigten Körperschaft zu entscheiden."

Wenn daher erst auf der Ebene der einzelnen gemeinnützigen Gesellschafterin entschieden wird, ob ihr Ergebnisanteil aus der GbR dem steuerpflichtigen wirtschaftlichen Geschäftsbetrieb zuzuordnen ist, ist die Gewerbesteuer auf Ebene der GbR **bereits angefallen**. Auf der Ebene der Gesellschafterin kann dann nur noch eine Steuerbefreiung hinsichtlich der Körperschaftsteuer eintreten.[478]

[472] Übt der Zusammenschluss einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb aus, ist das Vorliegen einer Mitunternehmerschaft iSd. § 15 Abs. 1 S. 1 Ziff. 2 EStG zu prüfen.

[473] Die Crux besteht also darin, dass das Gewerbesteuerrecht an die Gesellschaft als Steuersubjekt (§ 2 Abs. 1 S. 2 GewStG) anknüpft, wogegen die Personengesellschaft nach der Logik des Einkommen- und Körperschaftsteuerrechts gerade nicht als Steuersubjekt gilt und daher von den Befreiungen wegen Gemeinnützigkeit der §§ 51 ff. AO nicht erfasst wird.

[474] Auf die durch § 2a GewStG begünstigte Situation wird es im vorliegenden Zusammenhang wohl regelmäßig nicht ankommen. Der Zweck der Arge, die ebenfalls (nur) eine GbR ist, muss sich insoweit nämlich auf die Erfüllung eines einzigen Werkvertrags oder Werklieferungsvertrags beschränken. Besteht ein weiterer Zweck, schließt dieser die Anwendung des § 2a aus, und zwar nicht nur in Bezug auf diesen, sondern insgesamt.

[475] Aus ihrer Satzung muss sich ergeben, dass die GbR ausschließlich und unmittelbar gemeinnützige, mildtätige oder kirchliche Zwecke verfolgt (§ 59 AO). Dabei müssen die Satzungszwecke und die Art ihrer Verwirklichung so genau bestimmt sein, dass bereits aufgrund der Satzung geprüft werden kann, ob die satzungsmäßigen Voraussetzungen für Steuervergünstigungen gegeben sind (§ 60 Abs. 1 Satz 1 AO). Dieser sogenannte Buchnachweis kann allerdings auch mit dem Gesellschaftsvertrag einer Personengesellschaft geführt werden, die als „sonstige Verfassung" bzw. „Satzung" im Sinne der genannten Vorschriften gelten kann. Dabei darf allerdings nicht einfach auf die Satzungen der Gesellschafterinnen verwiesen werden. Zudem sollte Gesellschaftsvertrag auch die „Festlegungen" der Mustersatzung enthalten (§ 60 Abs. 1 Satz 2 AO). Zu vielversprechenden Konstellationen siehe im Übrigen oben Fn. 372.

[476] Weitemeyer/Klene, Notwendige Weiterentwicklung des Gemeinnützigkeitsrechts, DStR 2016, S. 937 (944). Siehe ferner Orth, Zur Gewerbesteuerbefreiung von Kooperationen gemeinnütziger Körperschaften, DStR 2012, S. 116 (119). Eine Fortentwicklung des Gemeinnützigkeitsrechts in dieser Richtung ist angezeigt.

[477] Dabei kann (zusätzlich) im Sinne einiger Literaturstimmen argumentiert werden, die die Entscheidung des BFH vom 25. Mai 2011, BFH 25.05.2011 Aktenzeichen I R 60/10 in diese Richtung weiterentwickeln wollen; siehe Schotenroehr: Kooperation von Zweckbetrieben gemeinnütziger Körperschaften in Form der Gesellschaft bürgerlichen Rechts - Relevanz der BFH-Entscheidung I R 60/10 vom 25. 5. 2011?, DStR 2012, S. 14 (zusammenfassend S. 17).

[478] Eine Verschärfung des Problems kann sich ggf. zudem durch die sogenannte Abfärbetheorie ergeben, wenn beispielsweise Einkünfte aus selbständiger Tätigkeit gegeben sind. Fallen daneben in der GbR auch gewerbliche Einkünfte an, sind gemäß § 15 Abs. 3 Ziff. 1 EStG auch Einkünfte aus anderen Einkunftsarten in gewerbliche Einkünfte umzuqualifizieren. Trotz vielfacher Kritik ist diese Regelung vom BVerfG für unbedenklich erklärt worden (BVerfG v. 15. Januar 2008, 1 BvL 2/04, DStRE 2008, S. 1003). Wo möglich und sinnvoll, können durch die Schaffung einer weiteren Gesellschaft, in der alle gewerblichen Einkünfte gesammelt werden, immerhin die sich aus der Abfärbetheorie ergebenden Probleme teilweise beseitigt werden.

C.4.8.6.3.2 Lösungsmöglichkeiten

- Neben der oben beschriebenen aber nicht immer erfolgversprechenden Lösung über die formelle Satzungsmäßigkeit kann in der Praxis der Weg der **„Nicht-GbR“** versucht werden. Dann muss jeder der gemeinnützigen Kooperationspartner sämtliche Verträge mit Dritten unterschreiben, sodass keine Personenmehrheit, sondern die einzelnen Gesellschafterinnen mit Dritten in Vertragsbeziehungen treten. Allerdings ist dieser Weg mit der Unsicherheit behaftet, ob die Finanzverwaltung die zivilrechtliche Gestaltung auch im Rahmen der steuerlichen Einordnung nachvollziehen wird und so die einheitliche Feststellung nach § 180 AO vermieden werden kann.
- Ein erfolgreich erprobter Ansatz ist dagegen die **Innen-GbR**. Bei dieser tritt nur eine der Gesellschafterinnen nach außen auf und handelt auch ausschließlich im eigenen Namen. Zusätzlich bestehen Abreden im Innenverhältnis mit den anderen Gesellschafterinnen im Hinblick auf die gemeinsame Verfolgung eines gemeinsamen Zwecks. Eine solche Innen-GbR ist keine Personengesellschaft im steuerlichen Sinne.[479] Daher kann sie auch nicht umsatzbesteuert werden.[480] Aus den gleichen Gründen scheitert auch die Gewerbebesteuerung der Innen-GbR.[481] Bei Vorliegen einer Mitunternehmerschaft erfolgt die Ertragsbesteuerung allein auf Ebene der Gesellschafterinnen. Auf die Gestaltung des Ausgleichs im Hinblick auf Risiko und Gewinn ist in solchen Konstellationen besondere Sorgfalt anzuwenden, um andere Schwierigkeiten zu vermeiden.

Hinweis:
Eine Innen-GbR kann leicht in eine Außen-GbR **umschlagen**. Das ist regelmäßig der Fall, wenn die GbR im Rechtsverkehr, nach außen auftritt. Problematisch kann das besonders dann werden, wenn die GbR Verluste macht, da ein **Verlustausgleich** im Falle einer **Mittelfehlverwendung** Folgen für die Gemeinnützigkeit der Gesellschafterinnen haben kann. Solange nur eine Innen-GbR besteht, haftet nach außen nur die im Rechtsverkehr auftretende Gesellschafterin. Weder die GbR noch die anderen Gesellschafterinnen kommen dann im Außenverhältnis unmittelbar als Zurechnungssubjekt für gesetzliche oder vertragliche Ansprüche in Betracht. Die Regressmöglichkeiten der nach außen auftretenden Gesellschafterin richten sich allerdings nach dem Auftragsrecht, §§ 713 iVm. 670 BGB. Ist die Haftung im Innenverhältnis **nicht beschränkt**, kann es auch im Rahmen einer bloßen Innen-GbR zu einer Mittelfehlverwendung kommen.

- Teilweise veranlagt die Finanzverwaltung im Feststellungsverfahren das Ergebnis aus Einkünften, die auf Gesellschafterebene einem Zweckbetrieb zugeordnet werden können, auf der Ebene der GbR als **Einkünfte aus selbständiger Tätigkeit** nach § 18 EStG, wodurch die Gewerbebesteuerung der GbR ausgeschlossen ist.

Anmerkung:
Im Rahmen der anstehenden Veränderungen des Gemeinnützigkeitsrechts sollte insbesondere darauf hingewirkt werden, dass die Gewerbesteuererleichterung des § 3 Ziff. 6 GewStG auch auf Kooperationen gemeinnütziger Körperschaften in der Rechtsform der GbR erweitert wird, wie es die Diakonie Deutschland fordert.[482]

C.4.8.6.3.3 Umsatzsteuerrechtliche Aspekte bei der Kooperation im Rahmen der GbR

Sind Leistungen einer einzelnen gemeinnützigen Körperschaft umsatzsteuerbar,[483] können sie insbesondere nach den Tatbeständen des § 4 UStG (insbesondere nach Ziff. 18 und 29[484]) befreit sein. Nach **neuer Rechtslage** können beide Befreiungstatbestände auch von Personenvereinigungen wie der GbR in Anspruch genommen werden.[485] Damit dürfte es auf die Geltendmachung der Steuerbefreiung nach Art. 132 Abs. 1 lit. f MwStSystRL nicht mehr ankommen.[486]

Praxis-Hinweis:
Insbesondere das neue Institut der **Kostenteilungsgemeinschaft** (§ 4 Ziff. 29 UstG) kann im Einzelfall eine interessante Lösung sein. Die Kostenteilung darf dabei nur dem **genauen Kostenersatz** entsprechen. Seine Inanspruchnahme könnte allerdings häufig an der aus der MwStSystRL übernommenen **Wettbewerbsklausel** scheitern. Auch die Erfüllung des Kriteriums der Unmittelbarkeit kann problematisch sein, wenn nicht über die Neufassung des § 57 Abs. 3 AO-E (planmäßiges Zusammenwirken) Abhilfe geschaffen werden

[479] Ertragsteuerlich kann aber auf Mitunternehmerschaft erkannt werden, denn dafür kann das Vorliegen von Mitunternehmerinitiative und Mitunternehmerrisiko ausreichen. Die Besteuerung erfolgt auf Ebene der Beteiligten.
[480] Eine Umsatzbesteuerung findet nur auf Ebene der Beteiligten statt.
[481] Auf der Ebene der Gesellschafterinnen greift die Befreiung des § 3 Ziff. 6 GewStG.
[482] So zum Beispiel vermittels eines anzufügenden S. 3: „Satz 1 gilt auch für Zusammenschlüsse der in Satz 1 genannten Körperschaften, Personenvereinigungen und Vermögensmassen.“
[483] Die Steuerbarkeit ergibt sich aus § 1 Ziff. 1 UStG.
[484] Der Personenzusammenschluss muss nach § 2 Abs. 1 UStG Unternehmer sein und seine Leistungen (nur „sonstige“, also keine Lieferungen) an einen oder mehrere seiner Mitglieder bewirken; zudem muss das die Leistung empfangende Mitglied eine Person sein, welche nicht steuerbare oder steuerfreie, dem Gemeinwohl dienende Leistungen der in § 4 Nummer 11b, 14 bis 18, 20 bis 25 oder Nummer 27 UStG bezeichneten Art erbringt. Insoweit handelt es sich um einen abschließenden Katalog.
[485] Nach alter Rechtslage war die Inanspruchnahme der Ziff. 18 durch Personenvereinigungen nicht möglich. Siehe zur jetzt geltenden Rechtslage nur Oelmaier, in: Sölch/Ringleb (Hrsg.), UStG, 89. EL Juni 2020, Rz. 16 zu § 4 Ziff. 18.
[486] Die Inanspruchnahme der Ziff. 29 dürfte allerdings gleichermaßen häufig an der übernommenen Wettbewerbsklausel scheitern wie die Inanspruchnahme der Befreiung nach Art. 132 Abs. 1 lit. f MwStSystRL. Die diesbezügliche Ermittlung erfolgt auf Grundlage der Art der erbrachten Leistung sowie auf Grund der objektiven Marktumstände der jeweiligen Leistungserbringung

kann. Gleichwohl ist dieser Ausnahmetatbestand in jedem Einzelfall gut zu prüfen. Für zukünftige Projekte ist die weitere Entwicklung in diesem Bereich im Auge zu behalten.

Kommt eine Befreiung nach § 4 UStG nicht in Betracht, unterliegt eine GbR, die als Kooperationsform mehrerer gemeinnütziger Körperschaften Leistungen erbringt, grundsätzlich dem vollen Umsatzsteuersatz bzw. dem ermäßigten Steuersatz von 7%. Letzterer gilt, wenn die Voraussetzungen des § 12 Abs. 2 Ziff. 8 lit. b UStG vorliegen, die Leistungen also, falls die Körperschaften sie anteilig selbst ausführten, insgesamt ermäßigt besteuert würden (nach lit. a).[487] Sind hingegen **nicht gemeinnützige Partnerinnen** beteiligt, kommt es für die ganze GbR zu einer Besteuerung mit 19 %. Tatsächlicher **„Schaden“** entsteht im Ergebnis (nur) dann, **wenn und soweit die Leistungsempfängerinnen nicht zum Vorsteuerabzug berechtigt** sind.

C.4.8.6.3.4 Gestaltungshinweise zu den Besonderheiten der GbR

Das gesetzliche Leitbild einer GbR impliziert, dass grundsätzlich alle Gesellschafterinnen gesamtgeschäftsführungs- und gesamtvertretungsberechtigt sind. Allerdings kann der Gesellschaftsvertrag hiervon **Ausnahmen** vorsehen, was in der Praxis häufig erfolgt.

Im Gesellschaftsvertrag sollte geregelt werden, wann und wie die Gesellschafter ihre Beteiligungen **kündigen bzw. übertragen** können. Dabei sollte auch überlegt werden, an wen die Übertragung möglich sein soll (zB. nur gemeinnützige Körperschaften). Bei der Ausgestaltung des Kündigungsrechts sollte beachtet werden, dass das außerordentliche Kündigungsrecht, die Kündigung aus wichtigem Grund, nicht abbedungen werden kann.

Der Vorteil der GbR, kein Mindestkapital zu benötigen, wird durch den Nachteil erkauft, dass alle Gesellschafter **grundsätzlich uneingeschränkt mit ihrem gesamten Vermögen für die Verbindlichkeiten der GbR haften**. Ein gewisser Ausgleich dieses Haftungsrisikos lässt sich dadurch erreichen, dass mit den jeweiligen Vertragspartnern eine **Haftungsbeschränkung auf das Gesellschaftsvermögen vereinbart** wird.

Besonders wichtig – aufgrund des drohenden Verlustausgleichs, der auch gemeinnützigkeitsschädlich sein kann – ist, dass die Gesellschafterinnen sich die Möglichkeit verschaffen, ihre Kontrollrechte effektiv auszuüben, um das durch die Tätigkeit der GbR begründete **Haftungsrisiko zu kontrollieren**.

C.4.8.6.3.5 Reformbedarf

Gemeinnützige Vorhaben sind aufgrund ihres projektbezogenen Charakters oft zeitlich beschränkt. Das vergleichsweise aufwendige (Aus-)Gründen einer Körperschaft erscheint häufig als nicht praktikabel, so dass von dem Vorhaben Abstand genommen wird. Insoweit wäre der Gesetzgeber gefordert, durch eine Reform des Gemeinnützigkeitsrecht Abhilfe zu schaffen. Dabei dürfte eine Verbesserung der gemeinnützigkeitsrechtlichen Stellung einer GbR ein erstrebenswertes Ziel sein.[488]

C.4.8.6.4 Zur Kooperation in Form einer GmbH

Während für kurzfristige Kooperationen die GbR in vielen Fällen die beste Kooperationsform sein dürfte, bietet sich die Gründung einer Kapitalgesellschaft insbesondere für längerfristige Kooperationsvorhaben an. Dabei wird die Wahl häufig auf die (g)GmbH fallen. Dabei sind unterschiedliche Gestaltungen im Steuerlichen denkbar:

- Die Kooperations-GmbH beschränkt sich auf die Verwaltung von Vermögen.
- Die Kooperations-GmbH kann selbst steuerbegünstigt sein, sofern sie gemeinnützige Zwecke verfolgt.
- Die GmbH ist als gewerbliche Gesellschaft steuerpflichtig tätig.

In jeder dieser unterschiedlichen Konstellationen ist die Beteiligung steuerlich anders zu behandeln. Insbesondere bestehen Unterschiede hinsichtlich der Aufbringung des Stammkapitals und im Hinblick auf die steuerliche Behandlung von Gewinnabführungen an die Gesellschafter. Was letztere anlangt, gelten die Ausführungen zur GbR entsprechend.

Als Anschaffung einer Beteiligung ist die finanzielle oder sachliche Ausstattung der GmbH für die Mutterorganisation eine Vermögensumschichtung. Ob dies gemeinnützigkeitsrechtlich unbedenklich ist, entscheidet sich danach, welche Mittel verwendet werden. Zeitnah zu verwendende Mittel können eingesetzt werden, wenn die GmbH sie zeitnah für ihre steuerbegünstigten Zwecke einsetzt. Da dies auch für die Anschaffung von nutzungsgebundenem Anlagevermögen gilt, kann das Stammkapital der GmbH auch durch Ausgliederung eines Zweckbetriebs finanziert werden, wenn dieser unmittelbar für die steuerbegünstigten Zwecke der neuen GmbH eingesetzt wird.[489] Für die Ausstattung einer nicht gemeinnützigen GmbH dürfen dagegen keine zweckgebundenen Mittel eingesetzt werden.[490]

[487] Aus betriebswirtschaftlichen Gründen kann es im Hinblick auf eine gegebene Vorsteuerabzugsmöglichkeit mitunter attraktiver sein, die vollständige Befreiung nicht in Anspruch zu nehmen.

[488] Siehe schon Stock: Wahl der Rechtsform im gemeinnützigen Nonprofit-Bereich, NZG 2001, S. 440.

[489] OFD Frankfurt, Schreiben vom 9.9.2003, Az. S 0174 A - 16 - St II 1.03.

[490] Verwendet werden dürfen dagegen beispielsweise freie Rücklagen, ungebundene Zuwendungen von Todes wegen, Zuwendungen und Spenden zur allgemeinen Vermögensausstattung und –Stärkung.

C.4.8.6.5 Die Gebote der Ausschließlichkeit und Selbstlosigkeit im Rahmen von Kooperationen

Im Hinblick auf das Gebot der **Ausschließlichkeit** kann eine Kooperation Schwierigkeiten bergen, wenn ihre Tätigkeit im steuerpflichtigen Bereich liegt. Dann darf die Tätigkeit ein **bestimmtes (relatives) Geschäftsvolumen nicht übersteigen**, da der ideelle Zweck immer das Hauptaugenmerk darstellen muss.

Im Hinblick auf das Gebot der **Selbstlosigkeit** können Verluste problematisch werden. Denn steuerschädlich ist der Einsatz zweckgebundener Mittel für nicht durch die Satzung vorgegebene Zwecke. Aufgrund der unbeschränkten Haftung im Rahmen personengesellschaftlicher Konstruktionen kann dies insbesondere problematisch sein, wenn im Rahmen einer unvorhergesehenen Haftung (etwa des Verlustausgleichs) auf gebundene Mittel zurückgegriffen wird. Dies kann eine Mittelfehlverwendung begründen. Darüber hinaus gilt im Rahmen der Gemeinnützigkeit ein umfassendes Angemessenheitsgebot. Keine Personen, insbesondere nicht die Gesellschafterinnen, dürfen durch Ausgaben oder Bevorteilungen, die dem Zweck der Körperschaft fremd sind, begünstigt werden. Es müssen daher insbesondere Preisgestaltung, Gehaltszahlungen und Zuschnitt des Empfängerkreises stets **angemessen** ausfallen.

C.4.8.6.6 Dachverbände und Spitzenorganisationen

Wie gesehen, ist Unmittelbarkeit im Sinne des § 57 AO die Verwirklichung der steuerbegünstigten satzungsmäßigen Zwecke durch die Körperschaft selbst. § 57 Absatz 2 AO durchbricht diesen Grundsatz aber zugunsten der Dach- und Spitzenverbände, die ihre gemeinnützigen Mitgliedskörperschaften fördern oder betreuen, gemeinnützige Zwecke also nicht unmittelbar selbst verfolgen und nur die Selbstverwirklichung ihrer Mitglieder unterstützen.[491] Dies kann etwa die Zurverfügungstellung einer digitalen Lösung durch einen Dach- oder Spitzenverband sein, wenn die Satzung Entsprechendes erlaubt und Kapital zweckentsprechend zur Verfügung steht. Eine kostenentsprechende Umlage kann ggf. recht unproblematisch zur Kostendeckung herangezogen werden.

C.4.8.6.7 Kooperationen und Schutz der jeweiligen Beiträge/Betriebsgeheimnisse

Kooperationen zwischen Sozialunternehmen und Start-ups haben in der Vergangenheit mitunter zu Streitigkeiten über die Verwertung der jeweiligen Beiträge geführt. Vor diesem Hintergrund ist es wichtig, sich bereits in Vorfeld über alle denkbaren Schwierigkeiten möglichst umfassend ein Bild zu machen. Für jede einzelne sollte dann eine Lösungsmöglichkeit verhandelt und vertraglich fixiert werden. Wenn beispielsweise ein Start-up mit Geldern des Sozialunternehmens eine App herstellt, muss klar geregelt sein, ob das Start-up die App später ohne Weiteres unabhängig vom Sozialunternehmen einsetzen oder an Dritte verkaufen darf.

C.4.9 CHECKLISTE RECHTS-/ ORGANISATIONSFORM UND KOOPERATIONEN

Vor dem Hintergrund aller vorstehenden Ausführungen sind insbesondere folgende Fragen für eine zielgebende Prüfung im Einzelfall hilfreich. Die Fragen sind zur leichteren Orientierung nach Themengebieten sortiert, sollten aber in jedem Falle vollständig durchgegangen werden.

Satzung

- Deckt die Satzung die erstrebten Ziele (beispielsweise die Entwicklung einer angestrebten Lösung) ab bzw. kann eine ggf. notwendige Änderung der Satzung gemeinnützigkeitsspezifisch abgebildet werden?
- Ist im Falle angestrebter Gemeinnützigkeit die sorgfältige Ausgestaltung der Satzung (ggf. Übernahme der Mustersatzung bzw. vorherige Abstimmung mit der Finanzverwaltung) sichergestellt?

Kapital

- Wird für die erstrebte Lösung Kapital benötigt? Steht ggf. zweckentsprechendes Kapital[492] zur Verfügung und ist dessen ggf. gebundene Nutzung anforderungsspezifisch (im Falle gebundener Mittel bspw. „zeitnah“) sichergestellt?
- Sofern Anlaufverluste möglich sind: Ist deren zulässiger Ausgleich (zB. durch zweckgebundene Umlagen)[493] sichergestellt?[494]
- Kann die gewählte Rechtsform mit dem zur Verfügung stehenden Kapital errichtet werden und entspricht die Kapitalausstattung dem gewählten Zweck?

[491] Verfolgt ein Dach- oder Spitzenverband gemeinnützige Zwecke selbst unmittelbar, so bedarf es der Fiktion des § 57 Absatz 2 AO nicht. Die Suspendierung des Unmittelbarkeitserfordernisses wird durch eine Gleichstellung der Dach- und Spitzenverbände erreicht.

[492] ZB. dezidierte Projektrücklagen. Auch eine nachrangige Verwendung der Freien Rücklage kann in Betracht kommen.

[493] Eine ausdrückliche Widmung ist notwendig.

[494] Bei wirtschaftlichen Geschäftsbetrieb kommt auch die Darlehensaufnahme zum Verlustausgleich in Betracht (siehe Ziff. 7 zu § 55 AEAO). Bei neu gegründeten Betrieben werden Anlaufverluste 3 Jahre lang toleriert (BFH/NV 09, S. 1837; Ziff. 8 zu § 55 AEAO). Bei guter Begründung kann diese Frist im Einzelfall verlängert werden.

- Ist im Falle der Stiftungsgründung ein im Verhältnis zum angestrebten Stiftungszweck angemessenes Stiftungsvermögen vorhanden und ist insoweit die frühzeitige Abstimmung mit der Finanzverwaltung gesucht worden?

Einnahmen

- Sofern ein Entgelt erhoben wird: Ist damit die Kostendeckung sichergestellt bzw. kann ein Verlust mittelverwendungsrechtlich gerechtfertigt werden?
- Ist festgestellt, ob und ggf. in welcher Höhe das Entgelt einen umsatzsteuerbaren Umsatz begründet?
- Erlauben die de-minimis-Regelungen (etwa § 64 Abs. 3 AO für Erträge unter [derzeit] € 35.000 und nach dem Jahressteuergesetz 2020 voraussichtlich € 45.000) ggf. eine – teilweise oder zeitweise – Vernachlässigung steuerlicher Fragen?
- Erreicht der steuerpflichtige wirtschaftliche Geschäftsbetriebes einen Umfang, der Selbstlosigkeit/Ausschließlichkeit und damit den Status der Gemeinnützigkeit gefährden kann? Kann solchen Gefahren ggf. durch eine Auslagerung auf eine Kapitalgesellschaft (im Sinne der Umlagerung auf Vermögensverwaltung) begegnet werden?

Abstimmung Finanzverwaltung

- Ist (insbesondere bei möglicherweise problematischen oder komplexen Sachverhalten) die Abstimmung mit der Finanzverwaltung möglichst frühzeitig (in der Planungsphase) sichergestellt?
- Ist bei der angestrebten Beteiligung an einer steuerbegünstigten Kapitalgesellschaft deren Einordnung (als Vermögensverwaltung bzw. Zweckbetrieb) vorab mit der Finanzverwaltung abgestimmt?
- Ist die richtige und gemeinnützigkeitsrechtlich unschädliche Einordnung einer Mittelweitergabe nach § 58 AO gesichert?

Organisationsform

- Ist eine dem gewählten Kooperationsziel und den absehbaren steuerlichen Auswirkungen angemessene Organisationsform gewählt worden?
- Ist im Falle einer dem ideellen Bereich oder dem Zweckbetrieb zuzuordnenden Tätigkeit ggf. die Gründung einer gemeinnützigen Rechtsform geprüft worden?
- Im Falle der Gründung einer GbR und ihrer Erbringung entgeltlicher Leistungen: Sind gegebene Möglichkeiten zur Vermeidung des Anfalls von Gewerbesteuer geprüft?

Haftung

- Entspricht die gewählte Rechtsform dem aus der Tätigkeit erwachsenden Haftungsrisiko? (Der Einsatz eines größeren Kapitals verträgt sich beispielswese grundsätzlich nicht mit der unbeschränkten und persönlichen Haftung der Personengesellschafterinnen.)
- Sind die im Hinblick auf Tätigkeit und gewählte Organisationsform verbleibenden Haftungsrisiken hinreichend aufeinander abgestimmt?
- Sind verbleibende Haftungsrisiken noch reduzierbar durch eine Absprache unter den Gesellschafterinnen (Freistellung) bzw. individualvertraglich mit möglichen Haftungsgläubigern?
- Ist die Haftung (insbesondere im Insolvenzfalle) beschränkt (Kapitalgesellschaft) und/oder ist sichergestellt, dass es durch eine möglicherweise in Betracht kommende Haftung nicht zu Problemen einer Mittelfehlverwendung kommt?

Vertragliche Einzelfragen

- Ist bei der Ausgestaltung des Kündigungsrechts im Rahmen eines Gesellschaftsvertrages bedacht worden, dass das Recht zur außerordentlichen Kündigung rechtlich nicht beschränkt werden kann?
- Sind im Gesellschaftsvertrag die im Einzelfall als notwendig erachteten Regelungen zur Ausübung der Stimmrechte (qualifizierte Mehrheiten) geregelt worden?
- Sind bei der Gründung einer Gesellschaft ggf. in Betracht kommende Zuwendungsbedingungen (zB. keine Befreiung vom Selbstkontrahierungsverbot) hinreichend berücksichtigt?
- Sind bei Einschaltung einer Hilfsperson die oben (unter C.4.8.6.2) genannten Checklisten-Punkte bedacht worden?

Kooperationsspezifika

- Sind im Falle einer angestrebten Kooperation die gewollte Konstruktion und die einzelnen Beiträge der Kooperationspartnerinnen klar und eindeutig geregelt, so dass eine abweichende rechtliche Einordnung durch die Finanzverwaltung hinreichend ausgeschlossen ist?
- Ist im Falle einer Kooperation im steuerpflichtigen Bereich sichergestellt, dass der Umfang der Tätigkeit nicht einen Verstoß gegen das Ausschließlichkeitsgebot begründet?
- Ist der im Rahmen von Kooperationen möglicherweise anfallende Verlust derart unproblematisch, dass er ohne gemeinnützigkeitsrechtliche Konsequenzen (Mittelfehlverwendung) ausgleichbar ist?
- Ist bei Kooperationen dem – dem Prinzip der Selbstlosigkeit entspringenden – umfassenden Angemessenheitsgebot Rechnung getragen (auch Preisgestaltung, Gehälter, Empfängerkreis etc.)?
- Sind im Gesellschaftsvertrag – im Rahmen des rechtlich Möglichen – angemessene angepasste Regelungen zur Auflösung der Kooperation vorgesehen?

- Umfassen ggf. getroffene Kooperationsvereinbarungen hinreichende Auskunfts- und Nachweispflichten, etwa zu den von der Kooperationspartnerin übernommenen Tätigkeitspflichten, um den eigenen Pflichten gegenüber der Finanzverwaltung effektiv nachkommen zu können?
- Ist bei Kooperationen der Feststellungsbescheid der Partnerinnen nach § 60a AO zur Kontrolle vorgelegt worden?
- Ist eine solide Regelung hinsichtlich der Verwertung der durch die Kooperationspartner eingebrachten Beiträge und im Rahmen der Kooperation entstandenen Produkte für die Zeit während und nach der Kooperation getroffen worden? Sind dabei alle denkbaren Konstellationen des Interessengegensatzes der Kooperationspartner berücksichtigt?

Praxis-Hinweis:
Abschließend zu allem ist noch einmal hervorzuheben: Hier können nur allgemeine Hinweise gegeben werden, die die Beratung im Einzelfall nicht ersetzen. Nach den Voraussetzungen des § 89 Abs. 2 AO ist daher gerade in der Planungsphase Rechtssicherheit bei ungeklärten Fragen durch eine verbindliche Auskunft der Finanzverwaltung recht kurzfristig herstellbar. Die Finanzverwaltung, der insoweit eine Fürsorgepflicht obliegt, ist in vielen Fällen sehr kooperativ.

C.5 FINANZIERUNG

Da die Regelfinanzierung im sozialen Bereich (sozialrechtlich normierte Dienstleistungsfinanzierung/Leistungsentgelte) üblicherweise keinen ausreichenden Spielraum für Forschung & Entwicklung sowie Innovationen vorsieht, ist häufig ein Blick über den Tellerrand nötig, wenn (zusätzliche) Geldmittel für diesen Zweck benötigt werden.

In Frage kommen vor allem Eigenmittel, philanthropische Mittel, etwa aus dem **Fundraising, Fördermittel, Fremdkapital** mit Rückzahlungsverpflichtung (z.B. Social Venture Capital) sowie „mittelersetzende“ **Kooperationen** mit anderen Anbietern.[495]

C.5.1 EIGENMITTEL

Eigenmittel setzen sich meist aus kirchlichen Zuwendungen, Spenden und sonstigen Barmitteln wie zum Beispiel Bußgeldern und Mitgliedsbeiträgen zusammen. Bei einer größeren Eigenkapitalbasis sind diese Mittel ein guter Weg für die freie Investitions- und Innovationsfinanzierung sowie auch als Eigenanteil zur Ergänzung anderer Finanzierungswege.

C.5.2 PHILANTHROPISCHE MITTEL

Philanthropische Mittel, d.h. solche, die ohne Rückzahlungsverpflichtung zur Verfügung gestellt werden und eine möglichst hohe Flexibilität in der Verwendung erlauben, können eine gute Möglichkeit zur Innovationsfinanzierung bieten. Im Bereich der Fremdkapitaleinwerbung (mit Rückzahlungsverpflichtung) können für konkrete neuartige Geschäftsmodelle im Bereich der Digitalisierung auch Investitionen durch Sozialinvestoren in Frage kommen, für die es mehr auf die Wirkungsorientierung als auf etablierte Geschäftsmodelle und viele Sicherheiten ankommt (z.B. **Social Venture Capital, Social Impact Bonds**).

C.5.2.1 Fundraising

Fundraising kommt in unterschiedlichen Erscheinungsformen vor. Fundraising kann beispielsweise bereits eine einfache Spendenaktion sein, um eine zeitlich begrenzte Maßnahme zu ermöglichen; es kann aber auch die bewusste strategische und dauerhafte Ausrichtung eines diakonischen Trägers charakterisieren. Fundraisingmittel sind, je nach Zweckbin-

[495] Mehr Informationen zu ergänzenden Finanzierungsinstrumenten finden Sie auch im Diakonietext 01.2019 „Ergänzende Finanzierung diakonischer Unternehmen im Wettbewerb“ unter: https://www.diakonie.de/fileadmin/user_upload/Diakonie/PDFs/Diakonie-Texte_PDF/01_2019___Finanzierung_diakonischer_Unternehmen_Web.pdf (zuletzt abgerufen am 02. Oktober 2020).
Vorteile und Ausgestaltungsmöglichkeiten von Unternehmenskooperationen im diakonischen Kontext finden Sie im Diakonietext 03.2019 „GEMEINSAM. VERANTWORTLICH.Kooperationen zwischen diakonischen und gewerblichen Unternehmen aktiv gestalten“ unter: https://www.diakonie.de/fileadmin/user_upload/Diakonie/PDFs/Diakonie-Texte_PDF/03_2019_GEMEINSAM_VERANWORTLICH_Web2.pdf.

dung der Mittelgabe, sowohl für die Innovations- als auch die Investitionsfinanzierung einsetzbar. Sie helfen zudem, die Eigenmittelbasis und damit die Liquidität des Trägers zu verbessern.

Neben den überkommenen Finanzierungsmöglichkeiten erfreut sich auch das **Crowdfunding** als eine Unterform des Fundraisings immer stärkerer Beliebtheit, um Mittel für eine steuerbegünstigte Körperschaft einzuwerben. Die Beteiligung einer größeren Anzahl von Personen kann so – auch nicht notwendigerweise steuerbegünstigte – Projekte stützen. Crowdfunding ist spendenbasiert und nicht-spendenbasiert möglich. Im letzteren Falle wird meist ein Anlagemodell, mindestens aber eine Gegenleistung angeboten. Crowdlending und Crowdinvesting besitzen also nicht den Charakter einer Spende. Es kann aber eine Spende vorliegen, wenn die steuerbegünstigte Körperschaft, ggf. als Förderkörperschaft, selbst oder über eine Treuhänderin eine Crowd-Plattform mit dem Ziel der Unterstützung eines steuerbegünstigten Zweckes betreibt und es an einer Gegenleistung fehlt.[496]

Das Kleinanlegerschutzgesetz vom 03. Juli 2015[497] brachte diverse Gesetzesänderungen mit sich, die auch von steuerbegünstigten Körperschaften zu berücksichtigen sind. Auch Crowdfunding-Projekte können dabei betroffen sein. Allerdings sieht das Vermögensanlagegesetz – in § 2b (Befreiungen für soziale Projekte)[498] und 2c (Befreiungen für gemeinnützige Projekte und Religionsgemeinschaften)[499] – teilweise Befreiungen für steuerbegünstigte Körperschaften vor.

C.5.2.2 Fördermittel

Unter dem Oberbegriff Fördermittel sind Mittel als Darlehen oder Eigenkapitalhilfe aus Förderprogrammen der Kommunen, Länder, dem Bund oder der EU zusammengefasst. Es kann sich um zinsgünstige Darlehen, rückzahlbare oder verlorene Zuschüsse und sogar um Beteiligungen handeln. Innovationen und Projekte können sowohl durch die öffentliche Hand, als auch von öffentlichen und privaten Stiftungen und Soziallotterien bezuschusst werden. Aktuell sind häufig gerade auch Projektmittel für die Digitalisierung vorgesehen.

Ärgerlich ist, dass gemeinnützige Unternehmungen sich mitunter nicht die gleichen Förderungen erschließen können wie nichtgemeinnützige Unternehmen. Denn vielfach ist die Leistung von der Erbringung eines Eigenanteils abhängig, dessen Ansparung die Fähigkeiten des gemeinnützigen Unternehmens zur Rücklagenbildung übersteigt. Sofern dann nicht anderweit freie Mittel nutzbar werden, scheitert das Vorhaben womöglich bereits aus diesem Grund. Zudem sind bestimmte Förderungen auf gewinnorientierte Unternehmungen beschränkt. Hier kann im Rahmen der Rechtsformwahl mitunter der Vorzug einer nichtgemeinnützigen Organisationsform gebühren.[500]

C.5.3 FREMDKAPITAL

Auch **Social Venture Capital**[501] kann eine vielversprechende Möglichkeit zur Startfinanzierung neuer Geschäftsmodelle mit Digitalisierungsfokus sein. Es handelt sich um einen Ableger des **Venture Capital**, also des Risiko- oder Wagniskapitals, das in der Startup-Szene verbreitet ist und vor einigen Jahrzehnten aus dem angelsächsischen Wirtschaftsraum auf den deutschen Markt übertragen wurde. Diverse **Intermediärgesellschaften** sind spezialisiert auf die Finanzierung von marktfähigen Innovationen im sozialen Bereich und vergeben Kapital von wirkungsorientierten Privatinvestor*innen als Startfinanzierung. Aber Achtung: Wird eine Fremdkapitalfinanzierung (und keine philanthropische Bezuschussung) genutzt, ist bei – im diakonischen Zusammenhang üblicherweise – gemeinnützigen Unternehmen auf die Vereinbarkeit der Rückzahlungskonditionen mit den gemeinnützigkeitsrechtlichen Vorgaben zu achten.[502]

Die Renditeerwartungen der Investoren zeichnen sich durch zwei Aspekte aus und weichen so vom klassischen Risikokapitalmodell ab: Ein direkter angemessener finanzieller Ertrag (monetäre Rendite) wird ergänzt um Ergebnis- und Wirkungsziele (soziale Rendite) des finanzierten Vorhabens beziehungsweise des Sozialunternehmens. Als Ausgestaltung üblich sind entweder die **Direktbeteiligung** in Form des Erwerbs von Unternehmensanteilen (Exitvariante) oder die Fremdfinanzierung mit **Nachrangabrede** (Fremdkapitalvariante), zum Beispiel in der Ausgestaltung als eigenkapitalähnliches Mezzaninkapital oder als einfaches Nachrangdarlehen durch private Investoren oder Fonds.

Interessant ist diese Finanzierungsform insbesondere für junge soziale Unternehmen in der Gründungsphase (Startups) und in der Wachstumsphase, wenn diese nicht über bankübliche Sicherheiten und nicht über eine gesicherte Gewinnerwartung verfügen, die es ihnen ermöglicht, bankübliche Kredite zu bekommen. Social Venture Capital wird vorzugsweise für neue Geschäftsmodelle genutzt, also zur Innovationsfinanzierung und deren Skalierung. Voraussetzung

[496] Siehe BMF, DStR 2018, S. 133.
[497] BGBl 15, S. 1114; zur Gesetzesbegründung siehe BT-Drs 18/3994; 18/4708.
[498] Insbesondere: Vertrieb muss frei von Provisionen erfolgen; Erhöhung der Schwelle für die Prospektpflicht auf € 2,5 Millionen Euro; Deckelung des Sollzinssatzes; Jahresabschluss des Emittenten muss nicht von einem Abschlussprüfer geprüft werden.
[499] Insbesondere: Anbieter muss kein VIB erstellen; Vertrieb muss frei von Provisionen erfolgen; Erhöhung der Schwelle für die Prospektpflicht auf € 2,5 Millionen; Deckelung des Sollzinssatzes; Jahresabschluss des Emittenten muss nicht von einem Abschlussprüfer geprüft werden; vollständige Ausnahme von den besonderen Rechnungslegungspflichten, wenn Vermögensanlagen desselben Emittenten € 250.000 nicht überschreiten.
[500] Siehe zur Rechtsformwahl oben C.4.8.
[501] Social Venture Capital (SVC) bzw. soziales Wagniskapital bezeichnet äußerbörsliches Beteiligungskapital (Darlehensvergabe oder Beteiligung), das von institutionellen oder privaten Investoren zur Innovations- oder Projektfinanzierung an risikobehaftete Sozialunternehmen mit wenig Besicherung zur Verfügung gestellt wird. Diese Unterform von Venture Capital ist speziell auf Unternehmen ausgerichtet, die neben einer finanziellen Rendite (geringer als bei herkömmlichem Venture Capital, i.d.R. ca. 7-8%) auch eine soziale Rendite (Wirkungsorientierung) generieren.
[502] Eine weitere Möglichkeit bietet ggf. auch die gesellschaftsrechtliche Ausgestaltung in Form der Ausgliederung eines gewerblichen Zweigs, für den die Aufnahme von Mezzaninkapital weniger Vorgaben unterliegt. Eine vorangehende steuerrechtliche Beratung wird hierzu aber ggf. dringend empfohlen.

ist dafür ein ausgearbeitetes Geschäftskonzept, das die langfristige Marktfähigkeit einer Geschäftsidee nachweist. Im Gegenzug ist in der Regel keine bankentechnische Absicherung nötig. Der Social-Venture-Capital-Investor nimmt meistens auch einen Sitz in einem Begleitgremium (sofern vorhanden oder einzurichten) ein beziehungsweise begleitet das Engagement beratend und erwartet in regelmäßigen Abständen eine umfassende wirkungsorientierte Berichterstattung.

Auch **Social Impact Bonds** könnten eine Überlegung wert sein. Social Impact Bonds als Multi-Stakeholder-Partnerschaft zwischen Sozialunternehmen, Staat und privaten Investor*innen bieten den Vorteil, dass nicht das Sozialunternehmen die Kosten für das innovative Projekt tragen muss, sondern im Erfolgsfall der Staat und im Verlustfall die Investoren die Refinanzierung übernehmen. Private Investor*innen – in Deutschland bisher vor allem Stiftungen – übernehmen die Rolle der Vorfinanzierung und im Erfolgsfall zahlt der Staat den Vorfinanzierenden die Investition inklusive einer Verzinsung („pay-for-success“) zurück. Social Impact Bonds sind speziell auf die Dienstleistungs- beziehungsweise Innovationsfinanzierung ausgelegt. Allerdings gibt es in Deutschland bisher erst wenige Beispiele für Social Impact Bonds. Zu bedenken ist, dass bei dieser Finanzierungsart **hohe Anforderungen** an die Wirkungsorientierung und die Anbahnung der Kooperation zwischen den verschiedenen Stakeholdern bestehen. Interessant können Social Impact Bonds vor allem für den Fall sein, dass sie eine innovative (in unserem Kontext digital basierte) Dienstleistungsidee im Sinn haben, die bisher noch nicht regelfinanziert ist, da sie sie in klare Wirkziele fassen können und bereits in gutem Kontakt zu ihren Leistungsträgern und ggf. innovationswilligen Vorfinanzierer*innen stehen.

C.5.4 KOOPERATIONEN

Kooperationen mit Social Start-ups aus dem Digitalbereich sind im diakonischen Kontext bislang nicht üblich. Per se ausgeschlossen sind sie keinesfalls. Die digitalen Startups sind auf das Digitale spezialisiert und die wohlfahrtlichen Einrichtungen auf die Erbringung sozialer Dienstleistungen. Raum für Kooperation besteht also genug. Aufgrund der häufig **unterschiedlichen Unternehmensphilosophien** wird eine für beide Seiten durchweg vorteilhafte Kooperation indes recht selten sein. Die soziale Dienstleisterin sollte vor allem darauf achten, sich nicht in **Pfadabhängigkeiten** zu begeben.

Sponsoring, verkürzt die Unternehmens-PR mithilfe der Unterstützung eines „guten Zwecks“,[503] erfreut sich nach wie vor einiger Beliebtheit und kann mitunter auch als (teilweises) Finanzierungsmodell im Bereich der Digitalisierung dienen. Auf Seiten der empfangenden Körperschaft sind die Mittel entweder dem ideellen Bereich (mäzenatisches Sponsoring), dem Bereich der Vermögensverwaltung oder dem wirtschaftlichen Geschäftsbetrieb zuzuordnen.

[503] Zum umsatzsteuerlichen Nachteil der Sponsorin kann es in Fällen des angenommenen Leistungsaustauschs kommen. Insoweit ist das BMF-Schreiben vom 25. Juli 2014 – IV D 2 – S, DStR 2014, S. 1555 – zu beachten.

IMPRESSUM

Herausgeber:
Evangelisches Werk für Diakonie und Entwicklung e.V.
Diakonie Deutschland
Caroline-Michaelis-Straße 1
10115 Berlin

Verfasser:
Dr. Daniel Burchardt

Redaktion:
Prof. Dr. Michael Veddern, Marvelle Meko Talla

Layout:
Isabell Wirtz

Stand:
Oktober 2020

Gefördert vom:

Bundesministerium
für Familie, Senioren, Frauen
und Jugend

TEIL D ANHANG

Die nachfolgenden Dokumente sind **ausschließlich als Orientierungshilfe und Inspirationsquelle** gedacht. **Sie können und sollen eine individuelle Rechtsberatung für den jeweiligen Anwendungsfall nicht ersetzen**. Den jeweiligen Besonderheiten eines konkreten Falles kann nicht allein durch abstrakte Musterformulierungen entsprochen werden.

D.1 APPS:

D.1.1: DATENSCHUTZ-ERKLÄRUNG FÜR APPS

Die folgende Datenschutzerklärung für Apps kann als Basisversion bei geringem Funktionsumfang im Sinne eines Ausgangspunktes für einen individuellen Entwurf dienen. Letztlich sollten **sämtliche Verarbeitungsvorgänge im Datenschutzhinweis abgebildet** sein.[504] Insbesondere bei Einsatz von Cookies ist darauf zu achten, dass idR. ein verlinkter Datenschutzhinweis nicht ausreicht, sondern bereits **beim Öffnen** hierüber innerhalb eines Cookie-Banners zu informieren ist und ggf. Einwilligungen einzuholen sind.[505] Neben den jeweiligen Spezifitäten der App muss bei der Anpassung auch berücksichtigt werden, dass sich die technischen Eigenheiten der verschiedenen Betriebssysteme (bspw. Android oder iOS und Windows Phone) unterscheiden. Es ist daher möglich, dass auch für jedes Betriebssystem zusätzliche Anpassungen notwendig sind.

Hinsichtlich der Platzierung der Anbieterkennzeichnung und Datenschutzerklärung können den Anforderungen der § 5 TMG, § 18 MStV insofern kaum erfüllt werden, als dass innerhalb der App ständig Impressum und Datenschutzerklärung abrufbar wären. Über einen Menüpunkt „Datenschutzerklärung“ kann immerhin ein Zugriff mit zwei Klicks ermöglicht werden. Die Darstellung auf der Startseite der App muss indes erfolgen. Auch sind die Pflichtangaben zusätzlich auf der Angebotsseite des App-Stores bereitzustellen (Apple und Google bieten diese Möglichkeit) bzw. auf der Website, von der die App heruntergeladen werden kann, oder vor dem Start der App.

Aufgrund der Unübersichtlichkeit längerer Texte auf kleinen Anzeigegeräten empfiehlt es sich, die Erklärung in einzelne Kapitel zu unterteilen, die getrennt geöffnet werden können (layered approach).[506] Auch können ergänzend Icons eingesetzt werden.

Aufgrund der neueren Rechtsprechung des EuGH erscheint die Klausel in § 3 Abs. 1 der nachfolgenden Datenschutzer-

[504] Siehe oben B.1.5.3 und B.2.2.4.3.1
[505] Siehe oben B.2.2.3.2
[506] Siehe oben B.2.2.4.3.1

klärung als problematisch. Die Rechtsprechung zur Gemeinsamen Verantwortlichkeit kann dahin gelesen werden, dass eine pauschale Freizeichnung für in Anspruch genommene Dienste Dritter nicht möglich ist. Ggf. ist daher besonders darauf zu achten, welche Daten etwa die App-Store-Betreiberin den Nutzer*innen abverlangt und darauf entsprechend einzugehen.

Hinsichtlich der Erfüllung Ihrer Informationspflichten gegenüber den Nutzer*innen beachten Sie bitte zusätzlich die Arbeitshilfe zur Umsetzung von Informationspflichten[507] des Datenschutzbeauftragten der EKD.

[507] https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-umsetzung-von-informationspflichten/“ (zuletzt abgerufen am 08. Oktober 2020).

VERWENDUNG UNSERER MOBILEN APP

§ 1 Information über die Erhebung personenbezogener Daten

(1) Wir möchten Sie im Folgenden darüber informieren, wie personenbezogene Daten bei Nutzung unserer mobilen App erhoben werden. Personenbezogene Daten sind alle Daten, die auf Sie persönlich rückführbar sind, wie z. B. Name, Adresse, E-Mail-Adressen etc., aber auch Daten über das Nutzerverhalten selbst.

(2) Wir arbeiten in diakonischer Trägerschaft. Aus diesem Grund gelten anstelle der europäischen Datenschutz-Grundverordnung (DS-GVO) und der datenschutzrechtlichen Bestimmungen von Bund und Ländern ausschließlich die Bestimmungen des kirchlichen Datenschutzes (Art. 91 EU DS-GVO iVm. Art. 140 GG, Art. 137 Abs. 3 WRV, § 2 Abs. 1 S. 1 DSG-EKD). Konkret sind wir damit an die Vorgaben des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) gebunden. Diese Gesetze stehen im Einklang mit der EU DS-GVO, das heißt sie bauen auf deren Vorgaben auf und bieten Ihnen mindestens dasselbe hohe Schutzniveau.

Verantwortliche Stelle gemäß Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DS-GVO) bzw. § 17 Abs. 1 Nr. 1 DSG-EKD ist [Einfügen: Name, Adresse, Telefon] (siehe auch unser Impressum). Sie erreichen unseren Datenschutzbeauftragten unter [Einfügen: Name, Adresse, Telefon].

(3) Sollten Sie mit uns per E-Mail oder über unser Kontaktformular Kontakt aufnehmen, werden Ihre E-Mail-Adresse und die weiteren von Ihnen angegebenen Kontaktdaten wie auch Ihr Name gespeichert, um Ihre Anliegen beantworten zu können. Wir löschen die in diesem Zusammenhang anfallenden Daten, sobald deren Speicherung nicht mehr erforderlich ist. Soweit gesetzliche Aufbewahrungspflichten bestehen, schränken wir ihre Verarbeitung ein.

[Optional:] (4) Soweit wir für einzelne Funktionen der App auf beauftragte Dienstleister zurückgreifen, informieren wir Sie untenstehend im Detail über die jeweiligen Vorgänge. Wir benennen dabei auch die Kriterien zur Speicherdauer.

§ 2 Ihre Rechte

(1) Hinsichtlich der Sie betreffenden personenbezogenen Rechte haben Sie uns gegenüber folgende:

- das Recht auf Auskunft,
- das Recht auf Berichtigung oder Löschung,
- das Recht auf Einschränkung der Verarbeitung,
- das Recht auf Widerspruch gegen die Verarbeitung,
- das Recht auf Datenübertragbarkeit.

(2) Davon unabhängig haben Sie jederzeit das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über unsere Verarbeitung Ihrer personenbezogenen Daten zu beschweren. Die für uns zuständige Aufsichtsbehörde ist [Einfügen: Name, Adresse, Telefon].

§ 3 Erhebung personenbezogener Daten bei Nutzung unserer mobilen App

(1)[508] Wenn Sie unsere App herunterladen, werden die dazu erforderlichen Informationen an den App-Store übertragen. Dabei handelt es sich insbesondere um den Nutzernamen, die E-Mail-Adresse, die Kundennummer des Accounts, den Zeitpunkt des Downloads und die individuelle Gerätekennziffer. Wir haben auf diese Datenerhebung keinerlei Einfluss und sind daher dafür auch nicht verantwortlich. Insoweit können Sie sich an den Betreiber Ihres App-Stores wenden. Wir verarbeiten diese Daten auch nur, soweit es für den Vorgang des Herunterladens notwendig ist.

[Optional:] Alternativ können Sie die App zudem kostenlos über unsere Website direkt auf Ihr mobiles Endgerät laden. Über die Website werden dafür die Daten verarbeitet, über die wir in der Datenschutzerklärung unserer Website [Einfügen Link] informieren.

[508] Siehe zu diesem Absatz nochmals den Hinweis in der Einleitung.

(2) Bei Nutzung der mobilen App erheben wir die nachfolgend beschriebenen personenbezogenen Daten, um Ihnen die Funktionen unserer mobilen App anzubieten und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO bzw. § 6 Ziff. 3 und 4 iVm. Ziff. 8 DSG-EKD):

- IP-Adresse,
- Datum und Uhrzeit der Anfrage,
- Zeitzonendifferenz zur Greenwich Mean Time (GMT),
- Inhalt der Anforderung (konkrete Seite),
- Zugriffsstatus/HTTP-Statuscode,
- jeweils übertragene Datenmenge,
- Betriebssystem und dessen Oberfläche.

(3) Zusätzlich benötigen wir [ggf. Einfügen: z.B. Gerätekennzeichnung, IMEI, IMSI, MSISDN etc.]

(4) Unsere mobile App setzt keine Cookies ein.

[Optional im Falle der Nutzung von Cookies:] Bei Ihrer Nutzung unserer App werden zusätzlich auch Cookies auf Ihrem Gerät gespeichert. Cookies sind kleine Textdateien, die im Gerätespeicher Ihres mobilen Endgerätes abgelegt und der von Ihnen verwendeten mobilen App zugeordnet gespeichert werden. Durch diese Cookies können der sie setzenden Stelle, hier also uns, bestimmte Informationen zufließen. Bitte seien Sie dessen gewiss, dass die Cookies keine Programme ausführen oder Viren auf Ihr mobiles Endgerät übertragen können. Sie dienen vielmehr dazu, unsere App insgesamt nutzerfreundlicher und effektiver zu machen.

a) Folgende Arten von Cookies nutzt unsere App

- Transiente Cookies (dazu b)
- Persistente Cookies (dazu c).

b) Transiente Cookies werden automatisiert gelöscht, sobald Sie sich ausloggen oder unsere mobile App schließen. Zu ihnen zählen vor allem die Session-Cookies, die eine sogenannte Session-ID speichern. Mit dieser lassen sich die verschiedenen technischen Anfragen der von Ihnen genutzten App zuordnen. Sie erlaubt es, Ihr mobiles Endgerät wiederzuerkennen.

c) Persistente Cookies werden dagegen automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann.

(5) Die Einstellungen Ihres mobilen Betriebssystems und der App können Sie nach Ihren Wünschen konfigurieren und z. B. die Annahme von Third-Party-Cookies oder allen Cookies ablehnen. Wir weisen Sie darauf hin, dass Sie eventuell nicht alle Funktionen unserer mobilen App nutzen können.

[Optional:] Bei der Nutzung verwenden wir statt Cookies eine in ihrer Funktion vergleichbare Technik.

[Optionale Alternative für Apps ohne Datenerhebung:] Nach dem Laden unserer App auf Ihr mobiles Endgerät kann sie ohne Zugriff auf das Internet verwendet werden. Bei der Nutzung werden keinerlei personenbezogene Daten erhoben. [Achtung: Die obenstehende Datenschutzerklärung sollte aber dennoch erfolgen, sofern die Kontaktaufnahme außerhalb der Kernanwendungen möglich und absehbar ist.]

D.2 ONLINE-PLATTFORMEN UND ALLGEMEIN VERWENDBARE VORLAGEN[509]

D.2.1: DATENSCHUTZERKLÄRUNG FÜR WEBSITES (ALLGEMEIN)[510]

Bitte überprüfen Sie zusätzlich die Vorschläge des deutlich ausführlicheren Muster D.2.2: (Datenschutzerklärung für Websites der Online-Beratung) und beziehen Sie diese in die nachfolgende Erklärung mit ein, soweit angezeigt.

[509] Bitte beachten Sie auch die einführenden Hinweise zum Muster-Datenschutzhinweis zu Apps entsprechend (siehe D.1.1).

[510] Vergleiche zusätzlich jedenfalls die Hinweise des Datenschutzbeauftragten der EKD: https://datenschutz.ekd.de/wp-content/uploads/2018/09/Handreichung-DS-Erkl%C3%A4rung.pdf (zuletzt abgerufen am 08. Oktober 2020).

§ 1 Information über die Erhebung personenbezogener Daten

(1) Wir möchten Sie im Folgenden darüber informieren, wie personenbezogene Daten bei Nutzung unserer Website erhoben werden. Personenbezogene Daten sind alle Daten, die auf Sie persönlich rückführbar sind, wie z. B. Name, Adresse, E-Mail-Adressen etc. aber auch Daten über das Nutzerverhalten selbst.

(2) Wir arbeiten in diakonischer Trägerschaft. Aus diesem Grund gelten anstelle der europäischen Datenschutz-Grundverordnung (DS-GVO) und der datenschutzrechtlichen Bestimmungen von Bund und Ländern ausschließlich die Bestimmungen des kirchlichen Datenschutzes (Art. 91 EU DS-GVO i.V.m. Art. 140 GG, Art. 137 Abs. 3 WRV, § 2 Abs. 1 S. 1 DSG-EKD). Konkret sind wir damit an die Vorgaben des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) gebunden. Diese Gesetze stehen im Einklang mit der EU DS-GVO, das heißt sie bauen auf deren Vorgaben auf und bieten Ihnen mindestens dasselbe hohe Schutzniveau.

Verantwortliche Stelle gemäß Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DS-GVO) bzw. § 17 Abs. 1 Nr. 1 DSG-EKD ist [Einfügen: Name, Adresse, Telefon] (siehe auch unser Impressum). Sie erreichen unseren Datenschutzbeauftragten unter [Einfügen: Name, Adresse, Telefon].

(3) Sollten Sie mit uns per E-Mail oder über unser Kontaktformular Kontakt aufnehmen, werden Ihre E-Mail-Adresse und die weiteren von Ihnen angegebenen Kontaktdaten wie auch Ihr Name gespeichert, um Ihre Anliegen beantworten zu können. Wir löschen die in diesem Zusammenhang anfallenden Daten, sobald deren Speicherung nicht mehr erforderlich ist. Soweit gesetzliche Aufbewahrungspflichten bestehen, schränken wir ihre Verarbeitung ein.

[Optional:] (4) Soweit wir für einzelne Funktionen der Website auf beauftragte Dienstleister zurückgreifen, informieren wir Sie untenstehend im Detail über die jeweiligen Vorgänge. Wir benennen dabei auch die Kriterien zur Speicherdauer.

§ 2 Ihre Rechte

(1) Hinsichtlich der Sie betreffenden personenbezogenen Rechte haben Sie uns gegenüber folgende:

- das Recht auf Auskunft,
- das Recht auf Berichtigung oder Löschung,
- das Recht auf Einschränkung der Verarbeitung,
- das Recht auf Widerspruch gegen die Verarbeitung,
- das Recht auf Datenübertragbarkeit.

(2) Davon unabhängig haben Sie jederzeit das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über unsere Verarbeitung Ihrer personenbezogenen Daten zu beschweren. Die für uns zuständige Aufsichtsbehörde ist [Einfügen: Name, Adresse, Telefon].

§ 3 Erhebung personenbezogener Daten bei Besuch unserer Website

(1) Wenn Sie unsere Website nur zu Ihrer Information nutzen, sich also nicht registrieren oder uns anderweitig Informationen übermitteln, erheben wir nur die personenbezogenen Daten, die Ihr Browser an unseren Server übermittelt. Um Ihnen die Möglichkeit zu geben, unsere Website zu betrachten, erheben wir dabei die folgenden Daten, die für uns technisch erforderlich sind, um Ihnen unsere Website anzuzeigen und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO bzw. § 6 Ziff. 3 und 4 iVm. Ziff. 8 DSG-EKD):

- IP-Adresse,
- Datum und Uhrzeit der Anfrage,
- Zeitzonendifferenz zur Greenwich Mean Time (GMT),
- Inhalt der Anforderung (konkrete Seite),
- Zugriffsstatus/HTTP-Statuscode,
- jeweils übertragene Datenmenge,
- Website, von der die Anforderung kommt,
- Browser, Sprache und Version der Browsersoftware,
- Betriebssystem und dessen Oberfläche.

(2) Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung unserer Website Cookies auf Ihrem Rechner gespeichert. Cookies sind kleine Textdateien, die im Gerätespeicher Ihres mobilen Endgerätes abgelegt und der von Ihnen verwendeten mobilen App zugeordnet gespeichert werden. Durch diese Cookies können der sie setzenden Stelle, hier also uns, bestimmte Informationen zufließen. Bitte seien Sie dessen gewiss, dass die Cookies keine Programme ausführen oder Viren auf Ihr Endgerät übertragen können. Sie dienen vielmehr dazu, unsere Website insgesamt nutzerfreundlicher und effektiver zu machen.

(3) Einsatz von Cookies:

a) Um folgende Arten und Einsatz handelt es sich:

- Transiente Cookies (dazu b)
- Persistente Cookies (dazu c).

b) Transiente Cookies werden automatisiert gelöscht, sobald Sie Ihren Browser schließen. Zu ihnen zählen vor allem die Session-Cookies, die eine sogenannte Session-ID speichern. Mit dieser lassen sich die verschiedenen technischen Anfragen des von Ihnen genutzten Browsers zuordnen. Sie erlaubt es, Ihren Rechner wiederzuerkennen.

c) Persistente Cookies werden dagegen automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann. Die Cookies können Sie jederzeit in den Sicherheitseinstellungen Ihres Browsers löschen.

d) Sie haben auch die Möglichkeit, Ihre Browser-Einstellung entsprechend Ihren Wünschen zu konfigurieren und so z.B. die Annahme von Third-Party-Cookies oder aller Cookies abzulehnen. [Optional:] Es ist allerdings möglich, dass Sie dann eventuell nicht alle Funktionen unserer Website nutzen können.

[Optional:] e) Um Sie im Falle von Folgebesuchen identifizieren zu können, setzen wir ebenfalls Cookies ein, sofern Sie über einen Account bei uns verfügen. Verfügen Sie dagegen über keinen Account, müssten Sie sich für jeden Besuch erneut einloggen.

[Optional:] f) Flash-Cookies werden nicht durch Ihren Browser erfasst, sondern durch Ihr Flash-Plug-in – sofern Sie dieses installiert haben. Sollten Sie die Verarbeitung der Flash-Cookies ablehnen wollen, müssen Sie ein entsprechendes Add-On installieren, z. B. „Better Privacy“ für Mozilla Firefox (https://addons.mozilla.org/de/firefox/addon/betterprivacy/) oder das Adobe-Flash-Killer-Cookie für Google Chrome. Weiterhin nutzen wir HTML5 storage objects, die auf Ihrem Endgerät abgelegt werden. Die insoweit erforderlichen Daten werden unabhängig von Ihrem verwendeten Browser gespeichert und haben kein automatisches Ablaufdatum. Sie können die Nutzung dieser Daten verhindern, indem Sie den privaten Modus Ihres Browsers einsetzen. Zudem empfiehlt sich die regelmäßige manuelle Löschung von Cookies.

D.2.2: DATENSCHUTZ-ERKLÄRUNG FÜR WEBSITES DER ONLINE-BERATUNG

In diesem Text sind Sicherheitsfeatures benannt, die ein anspruchsvolles Datenschutzniveau zu garantieren helfen. Soweit diese Features durch die betreffende Beratungsstelle nicht oder anders eingehalten werden, ist der Text entsprechend anzupassen. Auch sind die weiteren Angaben anhand der Bedingungen vor Ort zu überprüfen und ggf. entsprechend anzupassen.

Wer ist die [Einfügen: Name Online-Beratung]?

Die [Einfügen: Name Online-Beratung] ist [Einfügen: Beschreibung]. Sie ist in diakonischer Trägerschaft. Aus diesem Grund gelten für sie anstelle der europäischen Datenschutz-Grundverordnung (DS-GVO) und der datenschutzrechtlichen Bestimmungen von Bund und Ländern ausschließlich die Bestimmungen des kirchlichen Datenschutzes (Art. 91 EU DS-GVO iVm. Art. 140 GG, Art. 137 Abs. 3 WRV, § 2 Abs. 1 S. 1 DSG-EKD). Konkret ist sie damit an die Vorgaben des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) gebunden. Diese Gesetze stehen im Einklang mit der EU DS-GVO, das heißt sie bauen auf deren Vorgaben auf und bieten Ihnen mindestens dasselbe hohe Schutzniveau.

Wie gewährleistet die [Einfügen: Name Online-Beratung] Datenschutz und Anonymität?

Garantierte Anonymität und Datenschutz sind die obersten Prinzipien der [Einfügen: Name Online-Beratung]. Personenbezogene Daten von Nutzer*innen der [Einfügen: Name Online-Beratung] werden nicht verarbeitet, statistische Daten werden ohne Personenbezug registriert und selbst diese Daten werden am Jahresende nach Erstellung der Jahresstatistik vernichtet. [Optional:] Telefonnummern werden auch nicht gespeichert oder im Einzelverbindungsnachweis (EVN) der Anrufenden aufgeführt. Denn nach § 99 Abs. 2 des Telekommunikationsgesetzes (TKG) dürfen Telefonate zu Anschlüssen von Personen, Behörden oder Organisationen, die der anonymen Beratung im sozialen oder kirchlichen Bereich dienen, im Einzelverbindungsnachweis nicht aufgeführt werden.

Unser Internetangebot ist datenschutzrechtlich umfassend gesichert. Da sich der Versand von verschlüsselten Mails als zu kompliziert erwiesen hat, verbleibt bei unserem Mailkonzept der gesamte Kontakt auf dem Server der [Einfügen: Name Online-Beratung].

Ratsuchende können sich auf dem Server der [Einfügen: Name Online-Beratung] anonym einen Account anlegen, ohne ihre E-Mail-Adresse angeben zu müssen. Die gesamte Kommunikation wird verschlüsselt, wodurch auch die Integrität des Transfers garantiert wird. Das SSL-Zertifikat kann im Browser angezeigt werden und garantiert die Authentizität der [Einfügen: Name Online-Beratung]. Durch eine Firewall werden die Daten vor Zugriff von außen gesichert. Vom Ratsuchenden kann bei Bedarf ein Anonymisierungsdienst genutzt werden wie z.B. JAP, ein Dienst der Technischen Universität Dresden. Diese Technik ermöglicht es, sämtliche Datenspuren (IP-Adresse) zu verwischen und so die Privatsphäre besser zu schützen. Die [Einfügen: Name Online-Beratung] ist für die Inhalte dieser Anonymisierungsdienste nicht verantwortlich.

Darüber hinaus hat die [Einfügen: Name Online-Beratung] verbindliche Sicherheitsrichtlinien für alle beteiligten [Einfügen: Name Online-Beratung]-Stellen und Mitarbeiterinnen und Mitarbeiter verabschiedet. Mailkontakte werden nur in einem klar definierten Zeitrahmen aufbewahrt, inaktive Kontakte nach standardisierten Zeiträumen gelöscht.

[Anzupassen:] Das Onlineportal der [Einfügen: Name Online-Beratung] wird regelmäßig durch ein Audit zur IT-Sicherheit und zum Datenschutz geprüft. Die Prüfung erfolgt durch ein externes Sicherheitsunternehmen und einen TÜV zertifizierten Datenschutzauditor. Das Audit erfolgt auf der Basis der DIN ISO/IEC 27001 und dem BSI Standard 200. Es erfüllt die Vorgaben des § 26 KDG und des §27 DSG-EKD.

Wenn die [Einfügen: Name Online-Beratung] keine personenbezogenen Daten führt, weshalb benötigt sie dann überhaupt eine Datenschutzerklärung?

Diese Frage stellen Sie sich vielleicht, wenn Sie an diesem Punkt unserer Datenschutzerklärung angelangt sind. In Bezug auf die Verarbeitung personenbezogener Daten muss unterschieden werden zwischen der Beratungs-Tätigkeit und anderen, organisatorischen Tätigkeiten der [Einfügen: Name Online-Beratung]. Wenn Sie als Ratsuchender ein Beratungs-Gespräch per [Auswahl Telefon, E-Mail oder Chat] mit unseren Mitarbeiterinnen und Mitarbeitern führen, verarbeiten wir – wie zuvor erläutert – keinerlei personenbezogene Daten von Ihnen. Sie bleiben anonym. Garantiert.

Wenn Sie aber außerhalb eines solchen streng vertraulichen Beratungs-Gespräches mit uns Verbindung aufnehmen, zB. weil Sie Fragen zu unserer Öffentlichkeitsarbeit haben, sich als ehrenamtliche Mitarbeiterin oder ehrenamtlicher Mitarbeiter bewerben oder eine Spende tätigen wollen, verarbeiten wir selbstverständlich die Daten, die Sie dabei angeben. Wir müssen der Natur der Sache nach z.B. im Rahmen einer Anfrage Ihre E-Mail-Adresse und Ihren Namen verarbeiten, um Ihnen antworten zu können. Genauso müssen wir im Rahmen einer Spende die erforderlichen Daten verarbeiten, um diese ordnungsgemäß verbuchen und Ihnen auf Wunsch eine Spendenquittung ausstellen zu können.

Informationspflichten gemäß § 17 DSG-EKD

Im Internetauftritt der [Einfügen: Name Online-Beratung] werden Ihre Daten verantwortungsbewusst und rechtskonform entsprechend den Bestimmungen des DSG-EKD verarbeitet. Im Folgenden klären wir Sie gemäß § 17 DSG-EKD umfassend darüber auf, ob und wie wir Ihre personenbezogenen Daten verarbeiten, wenn Sie unsere Webseiten besuchen.

Verantwortlicher (§ 17 Abs. 1 Nr. 1 DSG-EKD)

Wer ist verantwortlich für die Datenverarbeitung auf dieser Webseite?

Verantwortlich für die Verarbeitung personenbezogener Daten auf dieser Webseite ist:

[Einfügen: Verantwortliche mit sämtlichen üblichen Kontaktdaten]

Datenschutzbeauftragter (§ 17 Abs. 1 Nr. 2 DSG-EKD)

Wer ist unser Datenschutzbeauftragter?

Als Datenschutzbeauftragter gemäß § 36 DSG-EKD wurde bestellt:

[Einfügen: Datenschutzbeauftragte mit sämtlichen üblichen Kontaktdaten]

Umfang, Zweck und Rechtsgrundlage der Datenverarbeitung (§ 17 Abs. 1 Nr. 3 DSG-EKD)

Wie erfassen und verarbeiten wir Ihre Daten? Um welche Daten handelt es sich?
[Anzupassen:] **Besuch unserer Webseiten**

Sofern innerhalb unseres Internetauftrittes die Möglichkeit zur Eingabe persönlicher Daten besteht, so erfolgt die Angabe dieser Daten seitens des Besuchers ausdrücklich auf freiwilliger Basis.

Wenn Sie unsere Webseiten besuchen, werden aber einige Daten in Form sogenannter „Server-Log-Files“ automatisch erhoben, die Ihr Browser dann an uns übermittelt. Sie enthalten folgende Informationen:

- Browsertyp und Browserversion,
- verwendetes Betriebssystem,
- Referrer URL (Webseite, von der das System des Nutzers auf die aufgerufene Webseite gelangt),
- Hostname/IP-Adresse des zugreifenden Rechners,
- Datum und Uhrzeit der Serveranfrage.

Diese Daten sind für uns nicht bestimmten Personen zuordenbar. Auch eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen. Selbstverständlich werden auch keine Nutzerprofile erstellt. Eine Weitergabe an Dritte, auch in Auszügen, findet nicht statt.

Wir behalten uns aber vor, die protokollierten Daten nachträglich zu prüfen, wenn uns konkrete Anhaltspunkte für eine rechtswidrige Nutzung der Webseite bekannt werden. Die Daten werden spätestens nach sieben Tagen wieder gelöscht, soweit keine weitere Aufbewahrung zu Beweiszwecken erforderlich ist. Andernfalls sind die Daten bis zur endgültigen Klärung eines Vorfalls ganz oder teilweise von der Löschung ausgenommen. Die Erfassung der Daten zur Bereitstellung der Webseiten und die Speicherung der Daten in Logfiles ist für den Betrieb unserer Internetseiten zwingend erforderlich. Es besteht folglich seitens des Nutzers keine Widerspruchsmöglichkeit.

Rechtsgrundlage für diese Datenverarbeitung ist § 6 Nr. 8 DSG-EKD. Unser berechtigtes Interesse an der Datenverarbeitung liegt hier in der korrekten, ansprechenden Darstellung und in der Verbesserung, Stabilität, Funktionalität und Sicherheit unseres Internetauftritts. Außerdem haben wir ein berechtigtes Interesse an der Ahndung einer rechtswidrigen Nutzung unseres Internetauftrittes.

[Anzupassen:][511] Verwendung von Cookies

Unsere Webseiten verwenden Cookies. Bei Cookies handelt es sich um Textdateien, die im Internetbrowser bzw. vom Internetbrowser auf dem Computersystem des Nutzers gespeichert werden. Ruft ein Nutzer eine Webseite auf, so kann ein Cookie auf dem Betriebssystem des Nutzers gespeichert werden. Dieses Cookie enthält eine charakteristische Zeichenfolge, die eine eindeutige Identifizierung des Browsers beim erneuten Aufrufen der Webseite ermöglicht.

Wir setzen Cookies ein, um unsere Webseite nutzerfreundlicher zu gestalten. Einige Elemente unserer Internetseiten erfordern es, dass der aufrufende Browser auch nach einem Seitenwechsel identifiziert werden kann. In den Cookies werden dabei folgende Daten gespeichert und übermittelt:

- Spracheinstellungen,
- Log-In-Informationen.

Der Zweck der Verwendung technisch notwendiger Cookies ist es, die Nutzung von Webseiten für die Nutzer zu vereinfachen. Einige Funktionen unserer Internetseiten können ohne den Einsatz von Cookies nicht angeboten werden. Für diese ist es erforderlich, dass der Browser auch nach einem Seitenwechsel wiedererkannt wird. Für folgende Anwendungen benötigen wir Cookies:

- Übernahme von Spracheinstellungen
- Log-In

Die durch technisch notwendige Cookies erhobenen Nutzerdaten werden nicht zur Erstellung von Nutzerprofilen verwendet und nicht mit anderen Datenquellen zusammengeführt. Eine Weitergabe an Dritte, auch in Auszügen, findet nicht statt.

Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten unter Verwendung von Cookies ist § 6 Nr. 4 DSG-EKD. Unser berechtigtes Interesse liegt hier in den genannten Zwecken, d.h. in der nutzerfreundlichen Gestaltung und vereinfachten Nutzung unserer Webseiten für unsere Besucher.

Cookies werden auf dem Rechner des Nutzers gespeichert und von diesem an unsere Webseiten übermittelt. Daher haben Sie als Nutzer auch die volle Kontrolle über die Verwendung von Cookies. Durch eine Änderung der Einstellungen in Ihrem Internetbrowser können Sie die Übertragung von Cookies deaktivieren oder einschränken. Bereits gespeicherte Cookies können jederzeit gelöscht werden. Dies kann auch automatisiert erfolgen. Werden Cookies für unsere Webseiten deaktiviert, können möglicherweise nicht mehr alle Funktionen der Webseiten vollumfänglich genutzt werden.

Verarbeitung von Daten bei Kontaktaufnahme mit den Webseitenbetreibern

Bei Fragen zur Öffentlichkeitsarbeit wenden Sie sich bitte an [Einfügen: ggf. Pressestelle].

Weitere Kontaktinformationen finden Sie unter der Rubrik „Presse“.

Bei Fragen zur Arbeit der [Einfügen: Name Online-Beratung] und bei allgemeinen Rückmeldungen wenden Sie sich bitte an [Einfügen: E-Mail-Adresse].

Wenn Sie uns ein Feedback zu unserer Arbeit geben möchten, können Sie das gerne über die Mailadresse [Einfügen: E-Mail-Adresse] tun.

Sollten Sie mit uns zu einem der gerade genannten Zwecke Kontakt aufnehmen, werden die von Ihnen mitgeteilten personenbezogenen Daten (z.B. Ihr Name, Ihre E-Mail-Adresse und sonstige Daten, die Sie übermitteln) von uns gespeichert, um Ihre Fragen zu beantworten bzw. Ihr Anliegen zu bearbeiten. Rechtsgrundlage für diese Datenverarbeitung ist ebenfalls § 6 Nr. 4 DSG-EKD. Unser berechtigtes Interesse liegt hier darin, jedes Ihrer Anliegen möglichst zeitnah, umfassend und zu Ihrer Zufriedenheit zu bearbeiten.

Die gerade beschriebene Datenerfassung erfolgt ausdrücklich nur bei einer Kontaktaufnahme über eine der vorgenannten E-Mail-Adressen! Wenn Sie ein Beratungs-Gespräch per Telefon, E-Mail oder Chat wünschen, gehen Sie bitte wie in der jeweiligen Rubrik der Webseite angegeben vor und nutzen Sie die dort aufgeführten Kontaktdaten. Im Rahmen eines Beratungsgesprächs bleiben Sie vollständig anonym.

[511] Bei Verwendung weiterer Cookies kann optional entsprechend auf Formulierungen der obigen Datenschutzerklärung für Apps zurückgegriffen werden.

[Optional:] Verarbeitung von Daten im Rahmen einer Bewerbung als ehrenamtliche Mitarbeiterin/ehrenamtlicher Mitarbeiter

Wenn Sie als ehrenamtliche Mitarbeiterin oder ehrenamtlicher Mitarbeiter bei der [Einfügen: Name Online-Beratung] tätig werden wollen, bewerben Sie sich bitte über [Einfügen: Kontakt].

Die [Einfügen: Name Online-Beratung] wird alle Daten, die Sie in Ihrer Bewerbung angeben, zum Zwecke der Bewerbungsabwicklung verarbeiten. Es gelten die allgemeinen Aufbewahrungs- und Löschfristen. Wir speichern Ihre personenbezogenen Daten grundsätzlich solange, wie dies für die Entscheidung über Ihre Bewerbung erforderlich ist und darüber hinaus nur, soweit ein anderer Rechtsgrund für eine weitergehende Speicherung besteht.

Die Rechtsgrundlage für diese Datenverarbeitung ergibt sich aus § 6 Nr. 3 und Nr. 4 DSG-EKD. Sollte Ihre Bewerbung Erfolg haben, werden Ihre Daten anschließend in unsere Datenbank ehrenamtlicher Mitarbeiter übertragen.

[Optional:] Verarbeitung von Daten im Rahmen von Spenden an die [Einfügen: Name Online-Beratung]

Der Anspruch der [Einfügen: Name Online-Beratung], an 365 Tagen im Jahr rund um die Uhr kompetent zu beraten, erfordert einen großen personellen und organisatorischen Einsatz und professionelle Strukturen. Die meist ehrenamtlichen Mitarbeiterinnen und Mitarbeiter werden in zahlreichen Schulungen und Fortbildungen zu kompetenten Beraterinnen und Beratern ausgebildet, Büroräume und technische Ausstattung sind notwendig. Das dazu erforderliche Geld kann nicht ausschließlich von den Trägern aufgebracht werden. Deshalb braucht die [Einfügen: Name Online-Beratung] Unterstützung.

Zweck der Verarbeitung der Daten, die Sie im Rahmen einer Spende angegeben haben, ist die reibungslose Abwicklung der Spende und auf Wunsch auch die Ausstellung einer Spendenquittung. Diese Datenverarbeitung liegt im berechtigten Interesse der [Einfügen: Name Online-Beratung], sich als eine notwendige Organisation zu erhalten. Zudem ist sie für die Wahrnehmung der Aufgabe der [Einfügen: Name Online-Beratung], die im kirchlichen und öffentlichen Interesse liegt, erforderlich. Damit ist die Datenverarbeitung gemäß § 6 Nr. 4 DSG-EKD i.V.m. Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO gerechtfertigt.

Verarbeitung von Daten im Rahmen eines Beratungsgesprächs

Wenn Sie sich entschließen, als Ratsuchende/r die [Einfügen: Name Online-Beratung] zu kontaktieren, so finden Sie im Folgenden einige Informationen zur Verarbeitung personenbezogener Daten im Rahmen eines Beratungsgesprächs [Auswahl: am Telefon, per E-Mail oder per Chat]. Detaillierte Informationen finden Sie in unseren Rubriken “Mailseelsorge“, “Chatseelsorge“ und “FAQ“.

Alle Mitarbeiterinnen und Mitarbeiter der [Einfügen: Name Online-Beratung] verpflichten sich, über alles, was ihnen anvertraut wird, Stillschweigen zu bewahren. Unsere wichtigsten Grundsätze sind Anonymität, Verschwiegenheit, Kompetenz, weltanschauliche Offenheit und Gebührenfreiheit. Unser Angebot umfasst Begegnung und Begleitung; es ersetzt keine Therapie.

Rechtlich betrachtet schließen wir einen Beratungs-Vertrag mit Ihnen, sobald Sie unser Beratungs-Angebot nutzen. Damit unterliegen wir den dafür relevanten Gesetzen und Richtlinien.

[Optional:] Telefonische Beratung:

Bei einem Beratungsgespräch am Telefon werden keine personenbezogenen Daten von Ihnen erfasst; wir garantieren Ihnen vollständige Anonymität. Wie in der Präambel dieser Datenschutzerklärung bereits erläutert, werden gemäß den gesetzlichen Vorgaben weder Telefonnummern gespeichert noch Anrufe im Einzelverbindungsnachweis des Anrufers aufgeführt. Es werden lediglich statistische Daten ohne Personenbezug registriert; diese Daten werden am Jahresende nach Erstellung der Jahresstatistik vernichtet. Sie können die [Einfügen: Name Online-Beratung] jederzeit kostenfrei unter einer der beiden auf unserer Webseite angegebenen Telefonnummern erreichen.

[Optional:] Online-Seelsorge:

Vielleicht fällt Ihnen das Schreiben leichter. Sie können über [Einfügen: Web-Adresse] zwischen Mail und Chat wählen. Ein Seelsorger oder eine Seelsorgerin wird Ihnen in einem schriftlichen Kontakt zur Seite stehen. Wenn Sie auf unserer Webseite den Link „Mailberatung“ oder „Chatberatung“ anklicken, werden Sie zum zentralen Webportal [Einfügen: Portal] weitergeleitet.

[Optional:] Vor Ort / Offene Türen-Netzwerk

Die Beratungsstellen „Vor Ort“ bieten ein niedrigschwelliges Beratungsangebot für Menschen, die sich [Einfügen: Beratungsindikation] befinden. In einem zweiten Schritt leisten die Mitarbeiter eine weiterführende Beratung; ggf. verweisen sie auch an geeignete Fachdienste. Die Beratung findet persönlich vor Ort statt, auf Wunsch auch anonym. Entscheiden Sie sich, das Beratungsangebot „Vor Ort“ wahrzunehmen, so schließen Sie rechtlich gesehen einen Beratungsvertrag. Die jeweils verantwortlichen Träger der Einrichtung sind für die Einhaltung der Datenschutzbestimmungen verantwortlich. Gleiches gilt für die Stellen des Offene Türen-Netzwerks.

Registrierung

Um die Möglichkeit der Mail- oder Chatseelsorge nutzen zu können, müssen Sie sich registrieren und anmelden. Wir erbitten dabei weder Ihren Namen noch Ihre Adresse, Sie bleiben also auch hier vollständig anonym, sofern Ihre E-Mail-Adresse keine Identifikation zulässt. Zu keinem Zeitpunkt werden persönliche Daten von Ihnen an unsere Mitarbeiter übermittelt. Sie entscheiden, welche Informationen Sie unseren Seelsorgerinnen und Seelsorgern mitteilen möchten. Lediglich eine funktionierende Mailadresse, über die wir Sie erreichen können, und ein Benutzername, um Sie ansprechen zu können, sind für die Nutzung erforderlich. Sie können darüber hinaus im Rahmen Ihrer Registrierung auch Angaben zu Ihrem Alter und Geschlecht machen, die uns dabei helfen, Statistiken zu erstellen und besser zu verstehen, wer unser Angebot im Internet wahrnimmt. Die Angabe dieser Daten ist aber absolut freiwillig. Die [Auswahl: Mailseelsorge/Chatseelsorge] der [Einfügen: Name Online-Beratung] ist selbstverständlich [Optional: – ebenso wie die Seelsorge am Telefon –] kostenlos. (Ausgenommen davon sind die Kosten, die Sie für die Bereitstellung Ihres Internetzugangs benötigen).

Wenn Sie gegen unsere Empfehlungen selber personenbezogen Daten von sich preisgeben, verarbeiten wir diese Daten, ohne Ihre Rechte zu verletzen, da Sie diese Informationen freiwillig selber von sich preisgegeben haben. Die Rechtsgrundlage ergibt sich in diesen Fällen aus § 6 Nr. 8 DSG-EKD.

Datenverarbeitung

Wenn Sie uns Texte in [ggf. Auswahl: Chat bzw. Mail] hinterlassen, werden neben diesen Angaben auch der Zeitpunkt ihrer Erstellung und der zuvor von Ihnen gewählte Benutzername gespeichert. Dies dient dazu, eine persönliche Kommunikation mit Ihnen zu führen. Die Daten werden für ein halbes Jahr gespeichert und helfen uns darüber hinaus, statistische Auswertungen ohne Personenbezug zu erstellen.

Löschung Ihres Accounts

Als Nutzer haben Sie jederzeit die Möglichkeit, die Registrierung aufzulösen. Wenn Sie Ihren Account löschen möchten, haben Sie dazu die Möglichkeit unter „Mein Account“. Das entsprechende Feld finden Sie oben links in der Anzeige.

[Optional und anzupassen:] Mail-Beratung

Die Mail-Beratung ermöglicht es Ihnen, auch über einen längeren Zeitraum mit einer Person in Kontakt zu bleiben. Wie beim Briefe schreiben können Sie sich Zeit nehmen, Ihre Gedanken zu sortieren. In der Regel können Sie innerhalb von 72 Stunden mit einer ersten Antwort auf Ihre Mail rechnen. In Einzelfällen kann die Beantwortung länger dauern. Sollte dies so sein, bitten wir um Ihr Verständnis.

Ablauf:
Ihre Mail wird einem unserer ehrenamtlichen Berater*innen zugewiesen, der oder die Ihr/e Ansprechpartner/in bleibt, auch wenn Sie sich häufiger schreiben. Eine zeitliche Begrenzung für den gemeinsamen Mailwechsel gibt es nicht. Falls Sie einen Mailverkehr beenden möchten, können Sie das einfach innerhalb ihres persönlichen Bereichs tun. Sie haben jederzeit die

Möglichkeit, einen neuen Mailverkehr zu beginnen. Dann werden Sie erneut einem/einer Gesprächspartner/in zugewiesen. Ein Anspruch auf den/die gleiche/n Gesprächspartner/in besteht nicht.

[Optional und anzupassen:] Chat-Beratung

Die Chat-Beratung bietet Ihnen die Möglichkeit, unmittelbar in ein schriftliches Gespräch zu kommen. Die direkte Reaktion ähnelt dem Gespräch von Angesicht zu Angesicht. Damit Sie die volle Aufmerksamkeit unserer Seelsorger/innen bekommen und ungestört chatten können, machen wir Termine aus.

Ablauf:
Sind Sie im geschützten Bereich eingeloggt, finden Sie unter der Rubrik „Zur Anmeldung“ eine Übersicht aller freien Chat-Termine. Hier können Sie einen Termin auswählen und anschließend auf „Termin belegen“ klicken. Bitte loggen Sie sich kurz vor dem vereinbarten Termin ein. Sobald ihr Termin beginnt, können Sie unter dem Reiter „Chat“ Ihren Termin anklicken und direkt ins Gespräch kommen. Sollte der Chat trotz Reservierung besetzt sein, kann das verschiedene Gründe haben. Bitte achten Sie auf entsprechende Hinweise Ihrer Kontaktperson unterhalb des Terminbuttons. Falls Sie einen gebuchten Termin nicht wahrnehmen können, sagen Sie ihn bitte ab. So kann die Zeit für andere Ratsuchende genutzt werden. Dazu melden Sie sich mit Ihrem Benutzernamen und Passwort an und klicken in der Terminliste im geschützten Bereich auf den Button „Termin absagen“ hinter Ihrem Termin. Danach loggen Sie sich aus.

Manchmal werden Termine spontan frei, dann können Sie auch ohne reservierten Termin chatten. Der Termin erscheint dann oben in der Liste kommender Termine. Sie können dann unmittelbar in den Chat eintreten und das Gespräch beginnen. Für diesen Vorgang müssen Sie ebenfalls eingeloggt sein.

Empfänger / Kategorien von Empfängern der personenbezogenen Daten (§ 17 Abs. 1 Nr. 4 DSG-EKD)

Empfänger aller mit der Nutzung unserer Webseiten [Einfügen: Webseiten] verbundenen Daten ist ausschließlich die [Einfügen: Name Online-Beratung].

Ihre Daten werden streng vertraulich behandelt und selbstverständlich nicht an Dritte weitergegeben oder in irgendeiner Weise kommerziell verwendet.

Wir haben alle Mitarbeiter auf das Datengeheimnis gemäß § 26 DSG-EKD hingewiesen und auf die Einhaltung der einschlägigen Datenschutzvorschriften verpflichtet. Zur sicheren Einhaltung der Datenschutzvorschriften werden Mitarbeiter/innen des Dachverbandes regelmäßig von unserer Datenschutzbeauftragten geschult.

Dauer der Speicherung und Löschung personenbezogener Daten (§§ 17 Abs. 2 Nr. 1, 21 DSG-EKD)

Wir halten uns an die Grundsatz der Datenminimierung. Wir speichern Ihre personenbezogenen Daten daher nur so lange, wie dies zur Erreichung der genannten Zwecke erforderlich ist oder wie es die vom Gesetzgeber vorgesehenen vielfältigen Speicher- bzw. Löschfristen vorsehen. Nach Wegfall des jeweiligen Zweckes bzw. Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig und entsprechend den gesetzlichen Vorschriften gesperrt oder gelöscht.

Die einschlägigen datenschutzrechtlichen Vorgaben zur Datenlöschung werden in § 21 Abs. 1 DSG-EKD gemacht. Danach sind wir verpflichtet, Ihre personenbezogenen Daten zu löschen und Sie haben das Recht, eine solche Löschung von uns zu verlangen, wenn einer der folgenden Gründe zutrifft:

1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig bzw. ihre Kenntnis ist für den Verantwortlichen zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben nicht mehr erforderlich.

2. Sie widerrufen Ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

3. Sie legen Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.

4. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet bzw. ihre Speicherung ist unzulässig.

5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

6. Sie verlangen die Löschung personenbezogener Daten, die bei elektronischen Angeboten erhoben wurden, die Minderjährigen direkt gemacht worden sind. Diese Verpflichtung zur Löschung bzw. das Recht auf Löschung besteht jedoch gemäß § 21 Abs. 3 DSG-EKD ausnahmsweise nicht, soweit die Datenverarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach kirchlichem oder staatlichem Recht, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- für im kirchlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, soweit das zuvor genannte Recht auf Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung von Rechtsansprüchen sowie zur Ausübung oder Verteidigung von Rechten.

Ihre Rechte als betroffene Person (§ 17 Abs. 2 Nr. 2 DSG-EKD)

Sie haben als von der Verarbeitung personenbezogener Daten betroffene Person folgende Rechte gegenüber der [Einfügen: Name Online-Beratung]:

Recht auf Auskunft gemäß § 19 DSG-EKD

Sofern personenbezogene Daten verarbeitet werden, können Sie gemäß § 19 Abs. 1 DSG-EKD jederzeit unentgeltlich Auskunft über diese personenbezogenen Daten und über folgende Informationen verlangen:

1. die Verarbeitungszwecke;

2. die Kategorien personenbezogener Daten, die verarbeitet werden;

3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;

4. falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

5. das Bestehen eines Rechts auf Berichtigung oder Löschung der Sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

6. das Bestehen eines Beschwerderechts bei der Datenschutzaufsicht;

7. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

8. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Recht auf Berichtigung gemäß § 20 DSG-EKD

Sie haben das Recht, von uns unverzüglich die Berichtigung Sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung haben Sie das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Recht auf Löschung gemäß § 21 DSG-EKD

Details zum Recht auf Löschung finden sie oben unter Punkt 5 dieser Datenschutzerklärung.

Recht auf Einschränkung der Verarbeitung gemäß § 22 DSG-EKD

Sie haben gemäß § 22 Abs. 1 DSG-EKD das Recht, von uns die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

1. die Richtigkeit der personenbezogenen Daten wird von Ihnen bestritten, und zwar für eine Dauer, die es uns ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;

2. die Verarbeitung ist unrechtmäßig. Sie lehnen die Löschung der personenbezogenen Daten ab und verlangen stattdessen die Einschränkung der Nutzung der personenbezogenen Daten;

3. wir benötigen die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, Sie benötigen sie jedoch zur Geltendmachung von Rechtsansprüchen oder zur Ausübung oder Verteidigung von Rechten, oder

4. Sie haben Widerspruch gegen die Verarbeitung eingelegt und es steht noch nicht fest, ob unsere berechtigten Gründe gegenüber Ihren überwiegen.

Wurde die Verarbeitung gemäß den oben genannten Voraussetzungen eingeschränkt, so werden diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung von Rechtsansprüchen oder zur Ausübung oder Verteidigung von Rechten oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen kirchlichen Interesses verarbeitet.

Recht auf Widerspruch gegen die Verarbeitung gem. § 23 KDG, § 25 DSG-EKD

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von § 6 Nr. 1, 3, 4, 8 DSG-EKD erfolgt, Widerspruch einzulegen. Wir verarbeiten die personenbezogenen Daten nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung von Rechtsansprüchen oder der Ausübung oder Verteidigung von Rechten.

Recht auf Datenübertragbarkeit gem. § 22 KDG, § 24 DSG-EKD

Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und Sie haben das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch uns zu übermitteln, sofern

1) die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und

2) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Bei der Ausübung des Rechts auf Datenübertragbarkeit haben Sie das Recht zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen zu einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Die Ausübung des Rechts auf Datenübertragbarkeit lässt das Recht auf Löschung („Recht auf Vergessen werden“) unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Recht auf Widerruf einer ggf. erteilten Einwilligung zur Verarbeitung personenbezogener Daten gemäß § 11 Abs. 3 DSG-EKD

Sofern die Verarbeitung der personenbezogenen Daten auf einer von Ihnen erteilten Einwilligung beruht, haben Sie jederzeit das Recht, die Einwilligung zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde (§ 17 Abs. 2 Nr. 3 DSG-EKD)

Die [Einfügen: Name Online-Beratung] ist eine Organisation in kirchlicher Trägerschaft. Neben den gerade aufgezählten Rechten haben Sie deshalb – unbeschadet eines anderweitigen Rechtsbehelfs – das Recht auf Beschwerde bei der Datenschutzaufsicht der Evangelischen Kirche in Deutschland. Die zuständige Stelle ist:

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

Michael Jacob, Böttcherstr. 7, 30419 Hannover, Tel.: 0511 76 81 28-0

Fax: 0511 76 81 28-20, E-Mail: michael.jacob@datenschutz.ekd.de

Sicherheit

Schutz Ihrer personenbezogenen Daten

Wir haben technische und organisatorische Maßnahmen i.S.d. § 27 DSG-EKD getroffen, um Ihre zur Verfügung gestellten Daten vor zufälliger oder vorsätzlicher Manipulation, Verlust, Zerstörung, Zugriff unberechtigter Personen oder unberechtigter Offenlegung zu schützen. Wir wenden äußerste Sorgfalt und modernste Sicherheitsstandards an, um einen maximalen Schutz Ihrer personenbezogenen Daten zu gewährleisten. Unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung ständig verbessert.

SSL-Verschlüsselung

Diese Webseite nutzt aus Gründen der Sicherheit und zum Schutz der Übertragung vertraulicher Inhalte eine dem aktuellen Stand der Technik entsprechende SSL-Verschlüsselung. Eine verschlüsselte Verbindung erkennen Sie daran, dass die Adresszeile des Browsers von „http://“ auf „https://“ wechselt und an dem Schloss-Symbol in Ihrer Browserzeile. Wenn die SSL-Verschlüsselung aktiviert ist, können die Daten, die Sie an uns übermitteln, nicht von Dritten mitgelesen werden.

Hosting

Alle Daten, die über unseren Mail- und Chatdienst erhoben werden, werden seitens des Dienstleisters [Einfügen: Dienstleister] auf einem Server in Deutschland gespeichert.

E-Mails an veröffentlichte Mailadressen der [Einfügen: Name Online-Beratung] **(mit Endung** [Einfügen: Endung]**)**

Der E-Mail-Verkehr erfolgt über das ungesicherte Internet. Wir weisen darauf hin, dass das Internet viele Angriffsgefahren birgt und eine absolut sichere Übertragung nicht gewährleistet werden kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.

[Optional:] **Links**

Unsere Webseite enthält Links zu Internetseiten Dritter, mit uns teilweise nicht verbundener Anbieter. Wir haben keinen Einfluss auf deren Inhalte und darauf, dass deren Betreiber die Datenschutzbestimmungen einhalten. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen, sofern wir uns die Inhalte nicht zu eigen gemacht haben, also sie

wie eigene Inhalte und/oder Dienste erscheinen lassen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Zweck und Umfang der Datenerhebung, der weiteren Verarbeitung und Nutzung der Daten durch den jeweiligen Dritten sowie Ihre diesbezüglichen Rechte und Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre entnehmen Sie bitte den Datenschutzhinweisen des Dritten.
Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Wir sind grundsätzlich nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen, sofern wir uns die Inhalte nicht zu eigen gemacht haben, also sie wie eigene Inhalte erscheinen lassen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Unser Internetauftritt [Einfügen Internetauftritt] verzichtet auf die Einbindung von Videos, Karten oder Social Media von Drittanbietern. Verlinkungen auf entsprechende Angebote sind keine Einbindungen.

Bereitstellung vorgeschrieben oder erforderlich

Die Bereitstellung Ihrer personenbezogenen Daten erfolgt freiwillig. Sofern Sie den Zugriff unterbinden, kann es hierdurch zu Funktionseinschränkungen auf der Website kommen.

D.2.3: VERPFLICHTUNGS-ERKLÄRUNG (MUSTER) FÜR MITARBEITENDE VON BERATUNGSSTELLEN

Nachfolgend findet sich ein Muster einer Verpflichtungserklärung für Mitarbeiterinnen und Mitarbeiter von Beratungsstellen. Hierbei ist auf Folgendes hinzuweisen:

- Es handelt sich um ein Muster, das jede Beratungsstelle (im Rahmen des rechtlich Erlaubten) an ihre jeweiligen Bedürfnisse anpassen kann. Dies gilt insbesondere für die Regelungen zur Wahrung der Anonymität der Mitarbeiter der Beratungsstellen, welche örtlich oder regional unterschiedlich gehandhabt wird.
- Auch eine bereits unterzeichnete Verpflichtungserklärung kann durch individuelle Ausnahmeregelungen für bestimmte Mitarbeiter*innen oder bei bestimmten Situationen ergänzt werden: Eine Ausnahmeregelung für eine/n bestimmte/n Mitarbeiter/in könnte z.B. vorsehen, dass dieser/diese die Entscheidung über die Verständigung der Polizei generell allein treffen darf. Eine Ausnahmeregelung für eine bestimmte Situation könnte etwa darin liegen, dass ein/e Mitarbeiter/in in einem bestimmten Fall von der Amtsverschwiegenheit vor Gericht entbunden wird. Solche Ausnahmeregelungen sollten im Interesse der/des jeweiligen Mitarbeiters/Mitarbeiterin schriftlich festgehalten werden.
- Neben der Mustererklärung sollte – individuell für jede Beratungsstelle– eine weitere Vereinbarung abgeschlossen werden, welche die übrigen Bedingungen der Mitarbeit in der jeweiligen Beratungsstelle regelt: Insbesondere die Zahl der monatlichen Dienste sowie ggf. Verpflichtungen der Mitarbeiter/innen zur Teilnahme an Fortbildungen und Supervisionen.
- Die Verpflichtung auf das Fernmeldegeheimnis sollte dann in Erwägung gezogen werden, wenn Telekommunikationsdienste angeboten werden. Dies kann insbesondere in der Beratung der Fall sein, wenn die Lösungen Dienste der Internettelefonie, E-Mail-Service oder des Text-Chattings umfassen sollte.

VERPFLICHTUNGSERKLÄRUNG FÜR MITARBEITERINNEN UND MITARBEITER VON BERATUNGSSTELLEN

1. Pflicht zur Geheimhaltung. Hiermit verpflichte ich mich, über alles, was mir im Zusammenhang mit der Ausübung meiner Tätigkeit bei der [Einsetzen: Beratungsstelle] von Klient*innen anvertraut oder über Klient*innen bekannt wird, Stillschweigen zu bewahren. Das bedeutet im Einzelnen:

- Innerhalb der [Einsetzen: Beratungsstelle] sowie ggf. im Rahmen der Supervision dürfen mitgeteilte Sachverhalte nur geschildert werden, soweit es zur Bearbeitung dieser Fälle unerlässlich ist.
- Außerhalb der [Einsetzen: Beratungsstelle] besteht die Pflicht zur strikten Geheimhaltung über alle mitgeteilten Sachverhalte gegenüber allen Personen, auch gegenüber vertrauten Personen, z.B. dem Lebenspartner.

2. Schriftliche Aufzeichnungen. Ich verpflichte mich, im Rahmen meiner Tätigkeit schriftliche Aufzeichnungen oder Aufzeichnungen am Computer nur in dem Ausmaß anzufertigen, wie es für die Bearbeitung eines Falles unbedingt notwendig ist. Der Klarname des/der Anrufenden darf nicht in den Aufzeichnungen vermerkt werden; ggf. ist ein Pseudonym zu verwenden. Ich verpflichte mich, schriftliche Aufzeichnungen oder Computerdaten (E-Mails, Chatverläufe usw.) nur nach Rücksprache mit der Leitung und deren ausdrücklicher Genehmigung mit nach Hause oder an andere Orte außerhalb der [Einsetzen: Beratungsstelle] mitzunehmen bzw. dorthin elektronisch zu übertragen.

3. Wahrung der eigenen Anonymität. Ich verpflichte mich, auch über meine eigene Mitarbeit in der [Einsetzen: Beratungsstelle] sowie über die anderen Mitarbeiter/innen und über die [Einsetzen: Beratungsstelle] Verschwiegenheit zu wahren und meine und deren persönliche Daten (Name, Adresse, Telefon usw.) geheim zu halten. Ich werde persönliche Begegnungen mit Anrufer/innen nicht vornehmen, es sei denn, dies wurde ausnahmsweise von der Leitung im Einzelfall genehmigt.

4. Personenbezogene Daten. Unabhängig meiner obigen Verpflichtung zur Geheimhaltung verpflichte ich mich, sämtliche personenbezogene Daten, also alle Informationen, die sich auf einen benannten oder identifizierbaren Menschen beziehen, vertraulich zu behandeln und ausschließlich auf Weisung von [Einsetzen: Beratungsstelle] zu verarbeiten. Sie dürfen also nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung meiner Tätigkeit für [Einsetzen: Beratungsstelle] fort.

5. [Optional:] Ich bin zudem darüber belehrt worden, dass durch im Rahmen der Beratung [Einsetzen: Beratungsstelle] geschäftsmäßig Telekommunikationsdienste erbracht werden und dass ich deshalb gemäß § 206 StGB und ggf. § 88 TKG strafbewehrt zur Wahrung des Fernmeldegeheimnisses verpflichtet bin. Ich bin mir darüber bewusst, dass diese Verpflichtung auch nach Beendigung meiner Tätigkeit fortbesteht. Mir ist klar, dass dem Fernmeldegeheimnis sowohl die Inhalte der Telekommunikation als auch deren Umstände unterliegen, insbesondere ob eine bestimmte Person an einer Telekommunikation beteiligt ist oder war. Das Geheimnis erstreckt sich auch auf die Umstände erfolgloser Verbindungsversuche.

6. Keine Beratung in rechtlichen und medizinischen Fragen. Ich verpflichte mich, Anrufende im Rahmen der Tätigkeit nicht über rechtliche oder medizinische Fragen zu beraten, selbst wenn ich darüber Kenntnisse habe. Anrufende, die solche Fragen haben, sind an einen Rechtsanwalt, Arzt, Psychotherapeuten oder Heilpraktiker zu verweisen. Dabei darf kein bestimmter Dienstleister empfohlen werden. Liegt in der [Einsetzen: Beratungsstelle] eine Liste solcher Dienstleister*innen aus, kann hieraus Auskunft gegeben werden.

7. Kenntnis von strafbaren Handlungen, Notsituationen, Suizid usw. Sollte ich im Rahmen meiner Tätigkeit mit Aussagen über Situationen konfrontiert werden, die mir nahelegen, die Polizei einzuschalten, werde ich hierüber unverzüglich die Leitung der [Einsetzen: Beratungsstelle] verständigen. Grundsätzlich soll nur gemeinsam mit der Leitung über die Einleitung weiterer Schritte entschieden werden, insbesondere darüber, ob die Polizei verständigt wird, welche eine Leitungsverfolgung beantragen kann.

8. Kenntnis der geltenden Datenschutzbestimmungen des Kirchendatenschutzrechts. Die Regelungen des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-DSG) und des kirchlichen Datenschutzgesetzes der katholischen Kirche (KDG) und der sog. Durchführungsverordnung zum KDG (Anhang 1 zu dieser Verpflichtungserklärung) sind mir bekannt und zu Beginn meiner Tätigkeit für die [Einsetzen: Beratungsstelle] ausgehändigt worden. Ich verpflichte mich hiermit, diese einzuhalten.

9. Aussagen gegenüber der Polizei und Gerichten. Wenn ich wegen Sachverhalten, die ich im Rahmen der Tätigkeit erfahren habe, als Zeuge von der Polizei, von der Staatsanwaltschaft oder vor Gericht vernommen werden soll, werde ich hierüber rechtzeitig vorher die Leitung der [Einsetzen: Beratungsstelle] verständigen. Dies gilt auch für Anrufe der Polizei bei der [Einsetzen: Beratungsstelle]. Mir ist bekannt, dass ich gegenüber der Polizei nicht zur Aussage verpflichtet bin und einer Vorladung zur Polizei keine Folge zu leisten brauche. Sofern keine Ausnahmen bestehen, bin ich bei allen Vernehmungen verpflichtet, mich auf meine ggf. bestehende Schweigepflicht und auf meine evtl. Amtsverschwiegenheit (§ 54 StPO) als Mitarbeiter/in der [Einsetzen: Beratungsstelle] zu berufen (eine Berufung auf ein „Nicht-Wissen“ habe ich zu unterlassen).

10. Folgen eines Pflichtverstoßes. Ich bin mir darüber bewusst, dass eine Verletzung meiner Pflichten, insbesondere eine Verletzung meiner Geheimhaltungspflicht und Vertraulichkeitsverpflichtung, zur sofortigen Auflösung meines Tätigkeitsverhältnisses mit der [Einsetzen: Beratungsstelle] führen und weitere rechtliche Konsequenzen, ggf. auch Schadensersatzansprüche und sogar strafrechtliche Konsequenzen nach sich ziehen kann.

11. Fortdauer der Verpflichtung nach Ausscheiden. Diese Verpflichtung gilt in allen Punkten auch für die Zeit nach meinem Ausscheiden aus dem Dienst der [Einsetzen: Beratungsstelle].

12. Ich bestätige, dass ich heute über die Bedeutung meiner Verpflichtung zur Geheimhaltung und zur Verschwiegenheit über personenbezogene Daten belehrt wurde. Ein Exemplar dieses Formulars sowie ein Merkblatt mit Erläuterungen habe ich erhalten.

Ort, Datum Unterschrift

D.2.4: MERKBLATT ZUR WAHRUNG DER VERTRAULICHKEIT IN DER SOZIALEN ARBEIT

Wie Sie wissen, ist Vertrauen die Basis unserer gemeinsamen Arbeit. Unsere Klienten müssen teilweise bereit sein, uns intimste Informationen zuteilwerden zu lassen, damit sie von unserer Hilfe und Unterstützung Gebrauch machen können. Sie müssen sich daher absolut sicher sein können, dass wir dieses Vertrauen nicht enttäuschen, dass also die uns anvertrauten Informationen vertraulich behandelt werden. An die wesentlichen Aspekte dieser Vertraulichkeit in der sozialen Arbeit möchten wir mit diesem Merkblatt erinnern. Sollten Sie nach Lektüre der Hinweise noch Fragen haben, wenden Sie sich bitte an [Einsetzen: Ansprechpartner, Telefonnummer].

Datenschutzrechtliche Vertraulichkeitsverpflichtung

In aller Regel stellen Informationen, die Sie von oder über unsere Klient*innen erhalten, personenbezogene Daten im Sinne des Datenschutzrechts dar. Daraus folgt, dass Sie alle Vorschriften des insoweit geltenden Datenschutzrechts einzuhalten haben. Ihre heutige förmliche Verpflichtung dient dazu, Ihnen die Bedeutung der Einhaltung des Datenschutzes zu verdeutlichen.

Der Datenschutz und Ihre diesbezügliche Vertraulichkeitspflicht schützt das Persönlichkeitsrecht derjenigen Menschen, auf die sich die Daten beziehen. Dieses soll den Berechtigten, den sogenannten „betroffenen Personen“ garantieren, dass sie grundsätzlich selbst über die Verwendung ihrer Daten entscheiden können. Diese so genannten „betroffenen Personen“ können unsere Kunden sein, Ihre Kollegen – oder auch Sie als unser/e Mitarbeiter/in. Grundsätzlich ist daher jede Verarbeitung personenbezogener Daten verboten. Dazu gibt es natürlich Ausnahmen, zum Beispiel die Einwilligung der betroffenen Person in die Verarbeitung oder eine gesetzliche Erlaubnis der Verarbeitung. Für uns gilt das Datenschutzgesetz der EKD. Auch dann, wenn die Verarbeitung für die Durchführung eines Vertrages notwendig ist, ist sie grundsätzlich erlaubt. Die Erlaubnis zur Verarbeitung muss aber nicht nur [Einsetzen: Beratungsstelle] zustehen, sondern auch müssen Sie nach der internen Aufgabenverteilung die Befugnis zur Verarbeitung besitzen. Sollten insoweit Unklarheiten bestehen, sprechen Sie bitte Ihre Vorgesetze an.

Beim Datenschutz geht es um alle personenbezogene Daten. Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen. Dazu gehört etwa der Name, die Adresse und der Gesundheitszustand, aber auch Daten wie die Kontonummer, Partei- oder Vereinszugehörigkeit, schlicht alles, was Informationen über einen Menschen vermittelt. Personenbezogene Daten sind auch dann geschützt, wenn zu Ihnen kein Name genannt wird. Es kann nämlich sein, dass sie anders auf eine bestimmte Person zurückgeführt werden können. Nur dann, wenn es sich um klar anonyme Daten handelt, Daten, die also schlechthin nicht mit einer Person in Verbindung gebracht werden können, handelt es sich nicht um personenbezogene Daten im datenschutzrechtlichen Sinne. Beachten Sie bitte, dass Sie auch dann, wenn sie davon ausgehen, dass es sich um Daten handelt, die keinem bestimmten Menschen zugeordnet werden können, diese nicht ohne Zustimmung Ihrer Vorgesetzten und der betrieblichen Datenschutzbeauftragten an Dritte weitergeben dürfen. Auch sonst müssen Sie sich im Rahmen Ihres Umgangs mit personenbezogenen Daten immer an die Weisungen Ihrer Vorgesetzten bzw. der betrieblichen Datenschutzbeauftragten halten. Bitte wenden Sie sich in Zweifelsfällen immer an diese Personen.

Das Datenschutzrecht gilt nicht nur für Computer-Daten, sondern auch für solche nichtautomatisiert verarbeiteten Daten, die in einer systematisierten, also geordneten Ablage abgelegt werden. So kann auch ein unsortierter Stapel handschriftlicher Notizen dem Datenschutzrecht unterfallen, wenn er nur nachvollziehbar archiviert wurde. Aber auch wenn ein solcher Stapel nicht archiviert, sondern weggeworfen werden soll, verliert er den Schutz nicht. So würde ein Stapel mit lesbaren Mitarbeiter- oder Klientenunterlagen in der Mülltonne einen Datenschutzbruch darstellen, der zur Ahndung und Bestrafung führen könnte. Auch das Offen-Herumliegenlassen kann einen Datenschutzbruch darstellen, wenn Unbefugte Kenntnis nehmen können.

Sie dürfen personenbezogene Daten immer nur für den Zweck verarbeiten, zu dem sie erhoben wurden. Eine Zweckänderung bräuchte eine Grundlage. Folgen Sie insoweit bitte den Weisungen Ihrer Vorgesetzten. Sie sollten daher personenbezogene Daten insbesondere nicht aus eigenem Antrieb an Dritte weitergeben oder für sich selbst verarbeiten.

Sie müssen personenbezogene Daten geschützt halten, so dass Unbefugte keine Kenntnis von ihnen nehmen und dass sie auch nicht versehentlich verloren gehen können. Werden personenbezogene Daten über das Internet übertragen muss das verschlüsselt erfolgen. Sie dürfen niemals per normaler E-Mail versendet werden. Das ist nur möglich, wenn sowohl Ihr Mailprogramm als auch das des Empfängers mit einer E-Mail-Verschlüsselung ausgestattet ist. Hierzu werden Sie von uns informiert.

Aber auch im Falle der Verschlüsselung ist immer zu überprüfen, ob die empfangende Person zum Empfang der Daten auch berechtigt ist. Achten Sie auch darauf, dass die richtige Empfängerin im Adressfeld steht. Aufgrund ähnlicher Namen liegen

Verwechselungen mitunter nahe. Geht eine Nachricht an mehrere Empfänger, bedarf die Übermittlung der E-Mail-Adressen grundsätzlich einer Erlaubnis. Die Verwendung eines offenen E-Mail-Verteilers ist datenschutzrechtlich häufig unzulässig ist, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben. Ein derartiger Verstoß kann sehr schnell und fahrlässig geschehen, wenn die E-Mail-Adressen nicht in das „BCC-Feld“ eingegeben werden. Trägt man sie nämlich in das „AN-Feld“ oder das „CC-Feld“ ein und nicht in das „BCC-Feld“ (Blind Carbon Copy), sehen sowohl die unmittelbaren Empfänger („AN-Feld“) als auch die Empfänger der Kopien („CC-Feld“) dieser E-Mail, an wen die E-Mail sonst noch geschickt wurde.

Unter keinen Umständen dürfen Sie vertrauliche Daten an Ihren privaten E-Mail-Account weiterleiten oder woanders als auf unseren Servern speichern – vor allem nicht in der „Cloud“. Insbesondere eine automatische Weiterleitung an Ihre private E-Mail-Adresse ist unzulässig.

Es sind regelmäßig Sicherungskopien (Backups) anzufertigen. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten dürfen keinesfalls einfach weggeworfen oder weggegeben werden. Papier ist vor der Entsorgung ordnungsgemäß zu schreddern, Datenträger sind durch die EDV-Abteilung sicher zu löschen. Bitte geben Sie Ihr Passwort zur Nutzung unserer Systeme nicht an Dritte Personen, auch nicht an Kollegen, weiter.

Da betroffene Personen unter anderen auch ein Recht auf Auskunft darüber haben, welche auf sie bezogenen Daten wir verarbeiten, fertigen Sie bitte sämtliche Aufzeichnungen niemals beleidigend an. Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, leiten Sie ihn bitte sofort an die betriebliche Datenschutzbeauftragte [Einsetzen: Ansprechpartner, Telefonnummer] weiter. Sie dürfen solcherlei nur dann selbstständig bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. Bitte holen Sie in Zweifelsfällen Rat bei der betrieblichen Datenschutzbeauftragten ein. Beachten Sie bitte auch, dass selbst Behörden und Polizei nicht ohne Weiteres Daten von uns erhalten können. Sollten Sie von der Polizei oder einer anderen Behörde kontaktiert werden, informieren Sie bitte sofort Ihren Vorgesetzten und die betriebliche Datenschutzbeauftragte.

Bitte beachten Sie: Ihre Vertraulichkeitsverpflichtung gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt umfassend, also gegenüber allen Personen, denen keine dienstliche Zuständigkeit für die jeweilige Sache zukommt. Daher gilt es auch gegenüber den anderen Kollegen, Ihrer Familie und der Presse.

Auskunftsrechte der Klient*innen

Ihre Klient*innen haben gemäß § 19 DSG-EKD bzw. Art. 15 DS-GVO einen Anspruch auf Auskunft über den Inhalt ihrer Akte. Dabei kann es im Einzelfall erforderlich sein, den nachfragenden Klient*innen den Akteninhalt mündlich zu erläutern – etwa wenn dort Feststellungen und Wertungen enthalten sind, die „schwer zu verdauen“ sind. Bitte berücksichtigen Sie dies bereits bei der Vornahme von Eintragungen, bleiben Sie immer sachlich und korrekt.

Sicherheit der Kommunikation

Personenbezogene Daten dürfen nicht per normaler (unverschlüsselter) E-Mail versendet werden.

Möglich ist, dass Klienten oder Dritte Sie bitten, per E-Mail mit Ihnen zu kommunizieren. Geben Sie Ihre E-Mail-Adresse daher nicht von vornherein heraus. Weisen Sie darauf hin, dass unverschlüsselte E-Mails von Unbefugten mitgelesen werden können und dass daraus den Betroffenen schwere Nachteile erwachsen können. Verweisen Sie stattdessen auf sichere Kommunikationswege wie Post, Fax oder Telefon. Sofern möglich, antworten Sie nicht per unverschlüsselter E-Mail.

Erhalten Sie im Rahmen Ihrer Tätigkeit von Behörden oder anderen Einrichtungen vertrauliche E-Mails auf unverschlüsseltem Wege, so verwahren Sie sich demgegenüber bei dem Absender und informieren im Wiederholungsfalle die Datenschutzbeauftragte der Gegenstelle oder unsere Datenschutzbeauftragte [Einfügen: Name, Adresse, Telefon]. Leiten Sie unverschlüsselte E-Mails keinesfalls weiter.

Sichere Aktenentsorgung

Sämtliche Informationen zu Klient*innen müssen sicher vernichtet werden, falls sie nicht in die Akte gehören. Notizen, Briefe oÄ. darf keinesfalls ungeschreddert in den Müll oder das Recycling gehen. Ein derart schwerwiegender Vertrauensbruch kann im Einzelfall sogar strafbar sein. Benutzen Sie daher immer den Aktenvernichter.

Spezielle Vertraulichkeitspflichten

Gleichwohl können Ihre Verpflichtungen hierüber aber noch hinausgehen. So ist es möglich, dass Sie sich als [Auswahl: Ehe-, Familien-, Erziehungs-, Jugend-, Sucht-, Schwangerschaftskonfliktberaterin, Sozialarbeiterin, Sozialpädagogin] nach § 203 Abs. 1 Nr. [4, 4 a, 5] StGB sogar strafbar machen, sollten Sie Ihnen durch Klient*innen anvertraute Geheimnisse an Dritte gelangen lassen. Dabei stellt schon der Umstand, dass jemand überhaupt entsprechender Beratung sucht oder sich in solcher Beratung befindet, ein Geheimnis in diesem Sinne dar, das geheim bleiben muss. Würden Sie als Beraterin etwa den Namen, die Adresse oder ein anderes identifizierendes persönliches Datum der Klient*innen weitergeben, würden Sie bereits das Geheimnis offenbaren, dass diese Person bei Ihnen in Beratung ist bzw. war.

Aus diesem Grunde müssen Sie unbedingt verhindern, dass Dritte irgendwas über eine Beratung erfahren, dass Rückschlüsse auf eine bestimmte Person zulässt. Dritte in diesem Sinne auch Ihre Freunde und Verwandte sowie gegenüber den in den Fall nicht inhaltlich eingebundenen Kolleg*innen. Auch Kolleg*innen dürfen Informationen über Ihre Klient*innen also nur erhalten, wenn sie diese Information zur Ausübung ihrer dienstlichen Tätigkeit unbedingt benötigen (zB. während einer Urlaubsvertretung). Sollten Sie sich im Rahmen der kollegialen Hilfe Unterstützung zu einem Fall einholen wollen, müssen Sie diesen anonym darstellen. Es ist insbesondere zu vermeiden, dass Dritte Einsicht in Patientenakten erlangen; dies beispielsweise dadurch, dass die Akten im Büro, im HomeOffice oder an öffentlichen Orten (etwa für Sitznachbarn in Bus oder Bahn) für Dritte einsehbar sind – egal, ob dies beabsichtigt oder unbeabsichtigt erfolgt. Akten sollten daher einen gut gesicherten Bereich nur in dem Fall verlassen, dass dies notwendig ist. Im Büro sollten Besucher keine Einsicht nehmen können. Sollten Sie also Ihren Arbeitsplatz verlassen, auch wenn dies zum Beispiel nur kurz für einen Gang in die Teeküche zum WC erfolgen sollte, sollte entweder Ihr Büro oder der Schrank mit den Klient*innen-Akten verschlossen sein bzw. der Rechner mit einer durch ein Passwort ausreichend geschützten Sperre versehen werden. Sollte keine Kollegin in ihrem Büro zurückbleiben, sollte dies wie auch dessen Fenster bei Ihrer Abwesenheit (auch bei kurzzeitiger Abwesenheit) immer abgeschlossen sein. Beachten Sie aber, dass Sie sich auch durch Unterlassen strafbar machen können, wenn eine nicht in den Fall inhaltlich eingebundene Kollegin die Akten liest. Bei längerer Abwesenheit sind alle Akten einzuschließen.

Bitte beachten Sie, dass Sie die Verpflichtung zur Vertraulichkeit auch gegenüber Freunden und Verwandten der Klient*innen zu wahren haben. Allein die Klient*innen entscheiden, welche Information an diese weitergegeben werden dürfen. Davon besteht eine Ausnahme nur bei solchen Klient*innen, denen die natürliche Einsichts- und Urteilsfähigkeit fehlt, die also nicht verstehen können, welche Bedeutung und Auswirkung eine Einwilligung zur Informationsweitergabe hat. In diesen Fällen entscheiden die Personensorgeberechtigten. Eine Ausnahme von dieser Ausnahme gilt dann, wenn eine nicht einwilligungsfähige Person direkt Kontakt mit der Beratungsstelle aufnimmt. Dann wird ihre Einwilligungsfähigkeit grundsätzlich angenommen.

Ausnahmen bei Kindeswohlgefährdung

Eingeschränkt ist Ihre Verschwiegenheitspflicht dann, wenn Ihnen in Ihrer Tätigkeit als [Auswahl: Ehe-, Familien-, Erziehungs-, Jugend-, Sucht-, Schwangerschaftskonfliktberaterin, Sozialarbeiterin, Sozialpädagogin] gewichtige Anhaltspunkte dafür bekannt werden, dass das Wohl eines Kindes oder Jugendlichen gefährdet ist – etwa durch Vernachlässigung, sexuellen Missbrauch oder sonstige Gewalt. § 4 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) erlaubt Ihnen hier ein gestuftes Vorgehen: Soweit es überhaupt möglich ist und als sinnvoll erscheint, sollen Sie das Problem mit dem Kind bzw. den Eltern besprechen. Dabei kann unterstützende Beratung durch das Jugendamt, auf die ein Rechtsanspruch besteht, eingefordert werden, wozu aber nur pseudonymisierte Daten weitergeben werden dürfen – also keine Klarnamen. Erscheint der kooperative Ansatz aber nicht als ausreichend oder gar als aussichtslos und halten Sie ein Einschreiten des Jugendamtes für erforderlich, dann dürfen Sie das Jugendamt entsprechend informieren und die dazu erforderlichen Daten an das Jugendamt weitergeben (keinesfalls aber ungeprüft Ihre komplette Akte). Zuvor müssen Sie Kind und Eltern auf Ihre Absicht, das Jugendamt einzuschalten, informieren, sollte dadurch der wirksame Schutz des Kindes oder Jugendlichen nicht in Frage gestellt werden.

Ungeachtet der Möglichkeit zur Einschaltung des Jugendamtes stehen wir Ihnen natürlich ebenfalls jederzeit zur Seite. Wir raten Ihnen dringend, sich in solchen Fällen jederzeit an unsere Ansprechpartner für Fälle von Kindeswohlgefährdung [Einfügen: Name, Telefon] zu wenden. Diese Hilfe steht Ihnen sowohl für eine Unterstützung ohne Nennung der Namen der Betroffenen als auch für eine fachkundige Mitbearbeitung des Falls zur Verfügung.
Zeugnisverweigerungsrecht [Variante für Schwangerschaftskonflikt- und Betäubungsmittelberaterin in anerkannten Beratungsstellen]

Als [Auswahl: Schwangerschaftskonfliktberaterin, Beraterin für Fragen der Betäubungsmittelabhängigkeit] in einer anerkannten Beratungsstelle haben Sie entsprechend Ihrer strafrechtlichen Verschwiegenheitsverpflichtung ein Zeugnisverweigerungsrecht über alles, was Ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist (§ 53 Abs. 1 Nr. [3 a, 3 b] StPO, § 383 Abs. 1 Nr. 6 ZPO). Sie werden als Berufsgeheimnisträgerin auf dieses Recht von öffentlichen Stellen der Strafverfolgung nicht gesondert hingewiesen – Sie müssen es also selbst kennen und beachten, weil Sie sich ansonsten strafbar machen, wenn Sie Fragen des Gerichts oder der Polizei beantworten.

Zeugnisverweigerungsrecht [Variante für andere Tätigkeiten]

Zwar sind Sie gemäß § 203 StGB grundsätzlich zur Verschwiegenheit verpflichtet. Hierzu existieren allerdings Ausnahmen. Als Zeuge im Zivil- oder Verwaltungsprozess haben Sie ein Zeugnisverweigerungsrecht über alles, für das Ihre Verschwiegenheitspflicht gilt (§ 383 Abs. 1 Nr. 6 ZPO). Im Strafprozess ist das anders: Nach § 53 StPO haben nur Betäubungsmittel- und Schwangerschaftsberater*innen ein automatisches Zeugnisverweigerungsrecht. Für alle nicht dort genannten Berufsgruppen – also auch Sie – gilt ein Zeugnisverweigerungsrecht nur ausnahmsweise. Ihre Pflicht zur (wahrheitsgemäßen) Aussage geht also in der Regel Ihrer Verschwiegenheitspflicht vor. Aus verfassungsrechtlichen Gründen können Sie in besonderen Fällen dennoch ein Aussageverweigerungsrecht haben; dann beispielsweise, wenn es um intime Klient*innen-Informationen geht, aber nur leichte strafrechtliche Vorwürfe erhoben werden. Stehen also der Schutzwert der Information und der mögliche Strafanspruch außer Verhältnis, dürfen Sie keine Aussage machen. In solchen Fällen sprechen Sie bitte rechtzeitig mit uns bzw. einer Rechtsanwältin/einem Rechtsanwalt Ihres Vertrauens. Im Notfall weisen Sie das Gericht bitte ausdrücklich auf Ihre Eigenschaft als Berufsgeheimnisträgerin hin und fragen Sie ausdrücklich, ob Sie in Anbetracht der Sachlage tatsächlich zu einer Aussage verpflichtete sind. Bitten Sie darum, dass Ihr Hinweis und die Antwort des Gerichts protokolliert wird, sofern es trotz Ihrer Nachfrage bei Ihrer Aussagepflicht bleibt. In kritischen Fällen können Sie die Beiordnung eines Zeugenbeistands nach § 68 Abs. 2 stopp beantragen; dies sollte möglichst rechtzeitig vor der Vernehmung erfolgen.

In jedem Fall gilt: Vor der Polizei sind Sie nicht zum Erscheinen bzw. zur Aussage verpflichtet, sondern nur vor Staatsanwaltschaft und Gericht (§§ 48 Abs. 1, 161 a Abs. 1 StPO). Sie werden als Berufsgeheimnisträgerin auf Ihr Recht zur Zeugnisverweigerung nicht hingewiesen – Sie müssen es selbst kennen und beachten, weil Sie sich ansonsten strafbar machen, wenn Sie Fragen des Gerichts oder der Polizei beantworten.

[Optional:] Das Fernmelde- oder Telekommunikationsgeheimnis

Durch das Fernmeldegeheimnis werden nicht nur Telefonate und Faxe, sondern auch moderne Kommunikationsformen wie beispielsweise Internettelefonie, E-Mail und Chats geschützt. So gefasst handelt sich also um ein umfassendes Telekommunikationsgeheimnis, das grundrechtlich in Art. 10 GG verbürgt ist. In § 88 TKG ist es der Sache nach geregelt, in § 206 StGB im Hinblick auf die Strafbarkeit seiner Verletzung hin geregelt. So ist der Inhalt der Kommunikation geschützt (Was wurde besprochen?; Was steht in der Nachricht?; Welche Daten wurden übermittelt? etc), aber auch „die näheren Umstände der Kommunikation“ (Wann kommunizierte wer mit wem? Wer hat wann versucht, wen zu erreichen? Welche Website wurde besucht? etc.).

Auch Sie sind gesetzlich gemäß § 88 TKG und § 206 StGB verpflichtet, das Telekommunikationsgeheimnis einzuhalten. Ihre heutige förmliche Verpflichtung dient dazu, Ihnen die Bedeutung der Einhaltung des Telekommunikationsgeheimnisses zu verdeutlichen.

Ihre Pflicht zur Wahrung des Fernmeldegeheimnisses

Alle Informationen, die dem Telekommunikationsgeheimnis unterliegen, müssen Sie absolut vertraulich behandeln. Weder dürfen Sie die entsprechenden Informationen weitergeben noch sie für außerdienstliche Zwecke nutzen. So dürfen Sie Nachweise oder Logfiles der einzelnen Verbindungen, E-Mail-Postfächer und Ähnliches nur dann einsehen, wenn dies ausnahmsweise erlaubt ist. Bitte sprechen Sie im Zweifel Ihre Vorgesetzte an. Von dieser erhalten Sie alle weiteren Anweisungen.

Auch wenn eine Erlaubnis besteht, reicht diese immer nur so weit, wie die Kenntnis, Speicherung oder sonstige Nutzung bzw. Verarbeitung der Daten für den jeweiligen erlaubten Zweck unbedingt erforderlich ist. Jede über dieses Maß hinausgehende Nutzung bzw. Verarbeitung ist unzulässig. Eine Ausnahme kann sich dann ergeben, wenn Sie davon Kenntnis erlangen, dass eine schwere, in § 138 StGB genannte Straftat geplant wird.

Auskunftsverlangen

Sollte die Polizei oder eine andere Stelle Sie um bestimmte Informationen bitten, leiten Sie die Anfrage bitte sofort an [Einfügen: Ansprechpartner, Telefon, usw.] weiter. Soweit es nicht zu Ihrem dienstlichen Aufgabengebiet gehört, dürfen Sie selbst keine Auskünfte erteilen.

Folgen von Verstößen

Verstöße gegen das Telekommunikationsgeheimnis können unter Umständen nach § 206 StGB mit bis zu fünf Jahren Haft bestraft werden. Auch kann die Verhängung eines Bußgelds ausgelöst sein.
Zudem kann selbst die unbeabsichtigte Verletzung des Telekommunikationsgeheimnisses zu schwerem Schaden führen, so zB. wenn unsere Klient*innen das in uns gesetzte Vertrauen verlieren. Es ist auch möglich, dass wir und Sie persönlich zu Schadensersatzzahlungen verpflichtet werden. Je nach Schwere Ihres Fehlverhaltens können schließlich auch arbeitsrechtliche Maßnahmen wie Abmahnung oder Kündigung drohen.

Ihre Pflicht zur Wahrung des Telekommunikationsgeheimnisses gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt umfassend, also gegenüber allen Personen, denen keine dienstliche Zuständigkeit für die jeweilige Sache zukommt. Daher gilt es auch gegenüber den anderen Kollegen, Ihrer Familie und der Presse.
Wortlaut der Gesetze

[Es ist – soweit für die jeweiligen Mitarbeiter von Relevanz – der Wortlaut der §§ 45, 48 DSG-EKD, §§ 203, 206 StGB, §§ 161 a Abs. 1, 53, 48 Abs. 1 StPO, § 383 Abs. 1 Nr. 6 ZPO, § 4 KKG, § 88 TKG einzufügen.]

D.2.5: NUTZUNGS-BEDINGUNGEN ONLINE-BERATUNG (FÜR NUTZER*INNEN)[512]

Eine spezifizierte Einwilligungserklärung der Nutzer*innen (die nach Aufklärung über alle relevanten Punkte aufgeklärt erfolgt) ist erforderlich. Auch der Datenschutzhinweis muss zusätzlich erfolgen.

[512] Kann ggf. angepasst auch im Bereich einer App eingesetzt werden.

AGB/NUTZUNGSBEDINGUNGEN FÜR [EINFÜGEN]

Bei der Nutzung des Online-Beratungsangebots gelten (ggf. unter Einbeziehung weiterer bereichsspezifischer Bedingungen) die nachfolgenden allgemeinen Bedingungen:

1. Gegenstand der Online-Beratung

Die Online-Beratung richtet sich an alle interessierten Personen. Sie ist kostenlos [ggf. anzupassen] verfügbar und erfordert lediglich die Registrierung des/der Interessierten.

1.1 Plattform [Optional]
Das [einzusetzen] (im Folgenden: Plattformbetreiberin) stellen den Mitgliedseinrichtungen des [einzusetzen] (im Folgenden: beratende Stelle) diese Plattform technisch zur Verfügung. [Bei Nichtnutzung des Einschubs ist die Bezeichnung der Verwenderin zu korrigieren]

1.2. Ablauf der Online-Beratung [Optional (sofern nicht bereits andernorts bereits beschrieben)]
[Sofern nicht bereits prominenter auf der Website beschrieben, sollte der grobe Ablauf der Beratung an dieser Stelle einmal wiedergegeben werden. Zum Beispiel sollte verdeutlicht werden, wie die ratsuchende Person eine Frage stellen kann (inklusive der Anmeldeschritte und der Absendung der Anfrage) und wie die Beantwortung dann erfolgt.]

[Optional:] Es besteht die Möglichkeit der verschlüsselten Dokumentenübertragung. Es sind hierbei so wenig persönliche Daten wie möglich (d. h. möglichst keine Geburtsurkunden, Aufenthaltstitel etc.) zu übertragen.

[Optional (wenn bei bloßer Erstberatung):] Das Beratungsangebot soll eine Möglichkeit der schnellen ersten Hilfe sein und ersetzt keine Therapie oder Behandlung. Die Beratung kann wichtige Anhaltspunkte für die Lösung einer Problemsituation geben, darin gegebene Hinweise und Tipps sind als erste Empfehlungen zu verstehen und ersetzen nicht den persönlichen Besuch bei einer Beratungsstelle, einem Therapeuten oder Fachmediziner, wenn Sie ernste Probleme haben.

[Optional:] In akuten Krisensituationen weisen wir Sie an dieser Stelle auf den direkten Kontakt zu psychosozialen Diensten oder das kostenlose Beratungsangebot der TelefonSeelsorge unter den Nummern 08001110111 und 08001110222 hin. Sollten Sie das Gefühl haben, dass Sie oder ein anderer Mensch in akuter Gefahr schweben (z.B. nach übermäßigem Alkoholkonsum), rufen Sie bitte den Rettungswagen (112) oder die Polizei (110). Dort wird Ihnen sofort geholfen.

2. Registrierung und Datenschutz [anzupassen]

Die Inanspruchnahme der Beratung ist grundsätzlich ohne Bekanntgabe personenbezogener Informationen möglich. Es ist aber die vorherige Registrierung erforderlich. Zur Anonymisierung geben Sie sich bitte bei der Anfrage einen Nicknamen an. Diese Daten werden ausschließlich für die Korrespondenz und Durchführung der Online-Beratung durch den/die jeweilige/n Berater*in mit Ihnen verwendet. Eine Weitergabe der Daten an Dritte erfolgt ohne Ihre ausdrückliche Einwilligung nicht. Sofern innerhalb der Onlineangebote die Möglichkeit zur Eingabe persönlicher oder geschäftlicher Daten (E-Mailadresse, Namen, Anschriften usw.) besteht, so erfolgt die Eingabe dieser Daten seitens der Nutzer*innen auf ausdrücklich freiwilliger Basis. Bitte beachten Sie auch die Datenschutzerklärung [Verlinkung einfügen], die Auskunft über die im Rahmen ihrer Nutzung systembedingt gespeicherten Daten gibt. Es gelten zudem für die Datenverarbeitung personenbezogener Daten die Bestimmungen des EKD-Datenschutzgesetzes, in der jeweils gültigen Fassung (DSG-EKD vom 15. November 2017)

3. Vertraulichkeit

Die Berater*innen beantworten Ihre Fragen in den Beratungsangeboten kostenfrei [ggf. anzupassen]. Sie unterliegen dabei der gesetzlichen Schweigepflicht und können sich auf das Zeugnisverweigerungsrecht berufen. Alle von Ihnen gemachten Angaben werden vertraulich behandelt. Allein zu Schulungszwecken werden Nachrichten vereinzelt im Beisein einer zu schulenden dritten Person beantwortet. Darüber hinaus werden die Beraterinnen und Berater fachlich-supervisorisch begleitet. So werden einzelne Fälle unter Maßgabe der Anonymisierung in Supervisionsgesprächen besprochen.

4. Qualifikation

Die Gewährleistung der angemessenen Qualifikation der Berater*innen obliegt der jeweiligen ausführenden Stelle. Falls Sie mit der jeweiligen Begleitung nicht einverstanden sein sollten oder technische Probleme die Begleitung beeinträchtigen, senden Sie uns bitte eine E-Mail an [einzusetzen].

5. Rücksicht [optional]

[Sofern ein Forum für die Nutzer*innen vorgehalten wird:] Die Nutzer*innen haben die Möglichkeit, sich im Rahmen eines Forums in Echtzeit auszutauschen. Für den Inhalt, Form und Richtigkeit der darin veröffentlichten Beiträge übernehmen Plattformbetreiberin und beratende Stelle keinerlei Haftung. Die Nutzer*innen verpflichten sich, keine strafbaren, jugendgefährdenden, pornografischen gewaltverherrlichenden oder sonst widerrechtlichen Inhalte einzustellen. Insbesondere zählen dazu auch solche Inhalte, die das Persönlichkeitsrecht Anderer verletzen. Sollten der Plattformbetreiberin oder der beratenden Stelle derartige Beiträge auffallen, so werden diese und (beim Anschein der Wiederholungsgefahr) gegebenenfalls auch deren Verfasser-Accounts ohne vorherige Ankündigung gelöscht. Alle Nutzer*innen werden um eine faire Diskussion und um eine akzeptable Wortwahl gebeten. Die Plattformbetreiberin und die beratende Stelle behalten sich vor, einzelnen Nutzer*innen zeitweise oder gänzlich die Schreibberechtigung zu entziehen oder ihre Beiträge zu löschen, wenn deren Verhalten die Grenzen der sachlichen Diskussion verlässt und diese durch ihr Verhalten für Konflikte mit anderen Forumsmitgliedern sorgen, das Forum gezielt mit Postings bombardieren (Spamming) oder das Forum dazu nutzen, gegen bestimmte Personen oder Sachen zu agitieren bzw es sonst missbräuchlich nutzen.

6. Löschung der Daten [anzupassen]

Aus technischen bzw. fachlich-supervisorischen Gründen werden die Texte aus [einzusetzen, zB. dem Messenger] mit dem verwendeten Nicknamen des/der Interessierten, dem Datum und der Uhrzeit in einer Protokolldatei bis [einzusetzen] gespeichert.

Sie können Ihren Account mitsamt der mit diesem verknüpften Inhalte jederzeit löschen. [Optional:] Account-Daten werden nach dem Löschen der App für [einzusetzen] Monate zu Dokumentationszwecken vorgehalten und danach automatisiert und vollständig gelöscht.

7. Haftung [anzupassen, wenn keine Vermittlung über Plattform erfolgt]

Die jeweiligen Beratungsstellen sind für die grundsätzliche Wahrung des Geheimhaltungsinteresses der beratenen Personen und die Einhaltung der für die Beratung geltenden gesetzlichen Bestimmungen und Bedingungen verantwortlich. Aus einer möglichen Pflichtverletzung der beratenden Stelle sich ggf. ergebende Haftungsansprüche unterliegen den Bedingungen der beratenden Stelle. Eine Haftung der Plattformbetreiberin ist hierbei ausgeschlossen.

Eine Haftung dafür, ob und wie Sie die sich aus der Beratung ergebenden Hinweise und Perspektiven umsetzen, kann nicht übernommen werden. Auch eine Haftung für technische Störungen, die zu einer Nichtverfügbarkeit der Beratung führen, kann nicht übernommen werden.

Darüber hinaus übernehmen wir keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der von Dritten bereitgestellten oder verlinkten Informationen. Alle Angebote sind freibleibend und unverbindlich.

8. Vorbehalt bei schwer missbräuchlichem Verhalten

Für den Fall des schweren Verstoßes gegen die Nutzungsbedingungen sowie bei missbräuchlichen Zugriffen bzw. Zugriffsversuchen behalten wir uns die Sperrung des Accounts vor. Zudem behalten wir uns vor, bei missbräuchlichen Zugriffen bzw. Zugriffsversuchen auf die eingesetzte technische Infrastruktur, insbesondere auf die Server, unter Zuhilfenahme einzelner Datensätze die Identifikation der verantwortlichen Person über zur Verfügung stehende personenbezogene Daten zu veranlassen.

9. Urheber- und Kennzeichnungsrecht

Die Inhalte auf diesen Webseiten sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das gilt für die gesamte Webseite, ihre einzelnen Teile, Grafiken, Layouts, Logos, Fotos, Filme, Software, Texte und sonstigen Inhalte.

Alle innerhalb des Internetangebots genannten und gegebenenfalls durch Dritte geschützte Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen Eigentümer*innen. Die bloße Nennung der geschützten Marken, Zeichen etc. ermöglicht nicht die Vermutung, dass die verwendeten Namen nicht durch Rechte Dritter geschützt seien.

10. Anwendbares Recht

Auf alle in den Nutzungsbedingungen angesprochenen Rechtsbeziehungen zu den Nutzer*innen findet ausschließlich deutsches Recht Anwendung.

D.2.6: NUTZUNGS-BEDINGUNGEN ONLINE-BERATUNG (FÜR HAUPT- UND EHRENAMTLICHE MITARBEITENDE)[513]

Dieser Entwurf ist ggf. gegen die Nutzungsbedingung für Nutzer*innen abzugleichen. Eine spezifizierte Einwilligungserklärung der Nutzer*innen (die nach Aufklärung über alle relevanten Punkte aufgeklärt erfolgt) ist erforderlich. Auch der Datenschutzhinweis muss zusätzlich erfolgen.

[513] Quelle der Textvorlage: Rechtsanwalt Jacob Metzler, Berlin. Die Nutzungsbedingungen dürfen bei Nennung der Quelle kostenlos vervielfältigt, bearbeitet, verbreitet und öffentlich zugänglich gemacht werden, sofern dies unentgeltlich erfolgt.

1. GELTUNGSBEREICH UND ALLGEMEINES

1.1 Für die Nutzung der von der [einfügen Betreiberin] (nachfolgend: Betreiberin) über die Website [einfügen Website] betriebenen Anwendung [einfügen Anwendung] (nachfolgend: Anwendung) gelten ausschließlich die nachfolgenden Allgemeinen Geschäftsbedingungen (AGB). Entgegenstehende Geschäftsbedingungen der registrierten Nutzer*innen von [einfügen Anwendung] (nachfolgend Nutzer*in oder Nutzer*innen) finden ausdrücklich keine Anwendung, es sei denn, die Betreiberin stimmt ihrer Geltung ausdrücklich schriftlich zu.

1.2 Die Betreiberin behält sich das Recht vor, diese AGB mit Wirkung für die Zukunft zu ändern. Dies ist insbesondere der Fall, wenn die Änderungen ohne wirtschaftliche Nachteile für die Nutzer*innen sind, z.B. bei Veränderungen im Anmeldeprozess oder Anpassung der AGB unter Beachtung abgeänderter oder neuer Dienste oder Funktionalitäten.

1.3 Im Fall der Änderung teilt die Betreiberin den Nutzer*innen die Änderungen der AGB per E-Mail mit und weist sie darauf hin, dass die Änderungen als akzeptiert gelten, wenn sie nicht binnen vier Wochen nach Erhalt der E-Mail widersprechen.

1.4 Die Anwendung bietet ihren Nutzer*innen Funktionen für die Beratungs-Arbeit (zur Kommunikation, Dokumentation, Statistik, Verwaltung) und die Möglichkeit, eigene Texte, Bilder und sonstige eigene Inhalte in Foren zu veröffentlichen. Die Nutzer*innen können ihre Profile und ihre Inhalte selbständig veröffentlichen, für die bereitgestellten Inhalte sind sie allein verantwortlich.

1.5 Alle Nutzer*innen verpflichtet sich, die Grundsätze von [einfügen Anwendung] zu beachten und insbesondere keine Inhalte einzustellen, die unwahr oder verleumderisch sind oder sonstige Straftatbestände erfüllen oder die Rechte Dritter verletzen. Im Übrigen sind die im Internet üblichen allgemeinen Umgangsformen zu wahren.

2. REGISTRIERUNG

2.1 Nutzer*innen, die die Anwendung nutzen möchten, müssen sich vor der Nutzung registrieren. Hierzu müssen sie die im Anmeldeformular abgefragten Daten bereitstellen, die sie anschließend für die Dauer ihrer Registrierung auf dem aktuellen Stand zu halten verpflichtet sind. Ehrenamtliche Nutzer*innen, die über keine eigene Emailadresse verfügen, erteilen ihrer Einsatzleitung schriftlich die Zustimmung, sie zu registrieren und unterschreiben die Nutzungsbedingungen sowie die Datenschutzerklärung in ausgedruckter Form. Beide Dokumente werden in der betreffenden Leitstelle sicher aufbewahrt.

2.2 Die erfolgte Registrierung wird den Nutzer*innen bzw. – in dem Fall, dass sie nicht über eine eigene Emailadresse verfügen – der Einsatzleitung per E-Mail bestätigt.

2.3 Die Nutzer*innen müssen alle bei der Anmeldung als Pflichtfelder gekennzeichneten Felder vollständig ausfüllen. Pseudonyme sind dabei nicht erlaubt, ebenso wenig die Angabe einer nicht existenten E-Mail-Adresse oder einer E-Mail-Adresse, die einer dritten Person gehört. Ändern sich nach der Anmeldung die angegebenen Daten, besteht die Verpflichtung, die Angaben im Mitgliedskonto Nutzer*innenseitig umgehend zu korrigieren. Eine Mehrfachregistrierung ist nicht gestattet.

2.4 Ein Rechtsanspruch auf Registrierung besteht nicht. Die Betreiberin behält sich vor, eine Registrierung ohne die Angabe von Gründen zu verweigern. Alle Daten der Nutzer*in, die in der Anwendung gespeichert wurden, werden in diesem Fall binnen 5 Werktagen gelöscht, sofern kein gesetzlicher oder vertraglicher Grund zur Speicherung besteht.

2.5 Die Betreiberin behält sich das Recht vor, Nutzer*innenkonten bei nicht vollständig durchgeführter Anmeldungen nach einer angemessenen Zeit (höchstens 5 Tage) zu löschen.

3. PASSWORT UND PFLICHTEN DER NUTZER*INNEN

3.1 Mit der Registrierung erhält Nutzer*in ein individuelles Passwort. Der Zugang zu den Dienstleistungen der Anwendung ist nur mit diesem Passwort möglich.

3.2 Bei Verlust des Passworts oder bei der begründeten Vermutung, dass eine dritte Person Kenntnis von dem Passwort erlangt, sind Nutzer*innen verpflichtet, unverzüglich das Passwort zu ändern und die Einsatzleitung zu informieren.

3.3 Nutzer*in hat alle eingestellten Texte auf inhaltliche Korrektheit zu überprüfen.

3.4 Nutzer*in darf keine Inhalte bzw. Beiträge einstellen, die Viren, Umgehungsvorrichtungen oder unaufgeforderte Massensendungen (so genannte „Spam“) enthalten, oder die kommerzielle bzw. gewerbliche Zwecke verfolgen. Nutzer*innen haben

bestehende Urheber- und Schutzrechte Dritter und strafrechtliche Bestimmungen zu beachten.
3.5 Folgende Inhalte sind per se nicht zulässig und dürfen von Nutzer*in nicht eingestellt werden:

- pornografische Inhalte
- rechtswidrige/strafbare Inhalte
- verleumderische und sittenwidrige Inhalte
- gewalttätiges Gedankengut
- Inhalte mit Bezug auf Drogenmissbrauch
- Gedankengut mit radikaler politischer oder religiöser Auffassung.

3.6 Werden sittenwidrige oder unzulässige Inhalte eingestellt, ist die Betreiberin berechtigt, diese zu löschen und Nutzer*in das weitere Posten in der Anwendung zu untersagen.

3.7 Es ist nicht gestattet, mehr als einen Nutzer*innenzugang für die Anwendung zu halten, auch nicht bei Einsatz verschiedener E-Mail-Adressen.

3.8 Es ist ferner nicht gestattet, Maschinen, Algorithmen oder andere automatische Funktionen zu nutzen, um Seitenaufrufe oder Inhalte zu generieren.

3.9 Die Betreiberin behält sich vor, Verstöße gegen geltendes Recht den zuständigen Landes- bzw. Bundesbehörden zu melden. Weiterhin behält sich die Betreiberin Schadensersatzansprüche bei Verstößen gegen die AGB vor.

4. EINGERÄUMTE RECHTE DURCH DIE NUTZER*INNEN

4.1 Nutzer*in überträgt der Betreiberin ein vergütungsfreies, unbefristetes, umfassendes Nutzungsrecht, insbesondere zur Vervielfältigung, Verbreitung, Bearbeitung an allen Werken oder Werkteilen, die die Nutzer*innen in der Anwendnung veröffentlichen, einschließlich des Rechts, diese Inhalte in Printmedien, online, auf CD-ROM etc. zu publizieren. Nutzer*in bleibt vorbehalten, einzelnen Nutzungen zu widersprechen.

4.2 Mit dem Einstellen von Texten, Bilder, Bildfolgen und Kennzeichen erklärt Nutzer*in, dass sie die über entsprechende Rechte an den bereitgestellten Texten, Bildern, Bildfolgen und Kennzeichen verfügt.

4.3 Die eingeräumten Rechte erlöschen mit der Löschung der Registrierung oder der Herausnahme der Informationen seitens Nutzer*in.

5. LÖSCHUNG DER REGISTRIERUNG

Nutzer*in kann ihre Registrierung jederzeit löschen lassen. Mit der Löschung der Registrierung entfällt die Teilnahmeberechtigung. Die Betreiberin ist berechtigt, eine bestehende Registrierung ohne Angabe von Gründen zu löschen, und wird dies insbesondere dann tun, wenn Nutzer*in bei der Anmeldung falsche Angaben gemacht hat oder gegen die Nutzungsbedingungen verstößt. Eine Löschung der Registrierung wird Nutzer*in seitens der Betreiberin schriftlich, per Telefax oder elektronischer Post (E-Mail) mitgeteilt. Im Fall der Löschung der Registrierung bestehen keine Ansprüche gegenüber der Betreiberin, insbesondere nicht auf Löschung von Nutzer*innen-Beiträgen in der Anwendung.

6. HAFTUNG

6.1 Die Betreiberin haftet nur in Fällen, in denen ihr selbst, einer gesetzlichen Vertreterin oder einem Erfüllungsgehilfen Vorsatz oder grobe Fahrlässigkeit zur Last fällt.

6.2 Für Schäden, die aus der Nutzung bereitgestellter Informationen entstehen, haftet allein Nutzer*in als Bereitsteller*in dieser Informationen.

6.3 Die jeweiligen Nutzer*innen haften grundsätzlich für sämtliche Aktivitäten, die unter Verwendung ihres Nutzer*innenkontos vorgenommen werden. Haben Nutzer*innen den Missbrauch ihres Kontos nicht zu vertreten, weil eine Verletzung der

bestehenden Sorgfaltspflichten nicht vorliegt, so haften sie nicht.

7. HAFTUNGSFREISTELLUNG

7.1 Nutzer*in stellt die Betreiberin von sämtlichen Ansprüchen frei, die andere Nutzer*innen oder Dritte der Betreiberin gegenüber geltend machen wegen Verletzung ihrer Rechte durch von Nutzer*in eingestellte Inhalte oder wegen deren sonstiger pflichtwidriger Nutzung der Anwendung. Nutzer*in trägt die hierfür entstandenen Kosten der notwendigen Rechtsverteidigung der Betreiberin einschließlich sämtlicher Gerichts- und Anwaltskosten in gesetzlicher Höhe.

7.2 Dies gilt nicht, wenn die Rechtsverletzung von Nutzer*in nicht zu vertreten ist. Nutzer*in ist verpflichtet, der Betreiberin für den Fall einer Inanspruchnahme durch Dritte unverzüglich, wahrheitsgemäß und vollständig alle Informationen zur Verfügung zu stellen, die für die Prüfung der Ansprüche und eine Verteidigung erforderlich sind.

8. GEWÄHRLEISTUNG

8.1 Die Betreiberin kann keine Gewährleistung für technische Mängel, insbesondere für die ständige und ununterbrochene Verfügbarkeit der Datenbank und ihrer Inhalte oder für die vollständige und fehlerfreie Wiedergabe der von Usern bereitgestellten Beiträge übernehmen.

8.2 Die Leistungen der Anwendung werden von der Betreiberin ohne jegliche rechtliche Verpflichtungen zur Aufrechterhaltung des Betriebs angeboten.

9. [Optional:] EXTERNE LINKS UND VIREN

9.2 Unsere Webseite enthält Links zu Internetseiten Dritter, mit uns teilweise nicht verbundener Anbieter. Wir haben keinen Einfluss auf deren Inhalte und darauf, dass deren Betreiber die Datenschutzbestimmungen einhalten. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen, sofern wir uns die Inhalte nicht zu eigen gemacht haben, also sie wie eigene Inhalte und/oder Dienste erscheinen lassen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Zweck und Umfang der Datenerhebung, der weiteren Verarbeitung und Nutzung der Daten durch den jeweiligen Dritten sowie Ihre diesbezüglichen Rechte und Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre entnehmen Sie bitte den Datenschutzhinweisen des Dritten. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

9.2 Wir sind grundsätzlich nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen, sofern wir uns die Inhalte nicht zu eigen gemacht haben, also sie wie eigene Inhalte erscheinen lassen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

9.3 Nutzer*in haftet dafür, dass die von ihm/ihr übermittelten Dateien virenfrei sind. Die Betreiberin behält sich das Recht vor, Ersatzansprüche wegen virenbedingter Schäden gegenüber den jeweiligen Nutzer*innen geltend zu machen.

10. DATENSCHUTZ

10.1 Die Nutzer*in sind über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung der für die Registrierung für die Anwendung und des Handelns vermittels dieser erforderlichen personenbezogenen Daten durch den Betreiber informiert (siehe Datenschutzerklärung).

10.2 Nutzer*in ist bekannt, dass zur Optimierung von [einfügen Anwendung] alle aufgerufenen Seiten sowie die Dauer jedes Aufrufs gespeichert werden. Ferner ist der Nutzer*in bekannt, dass persönliche Informationen wie etwa die E-Mail-Adresse in den Räumen angezeigt werden, in denen eine Registrierung erfolgt.

10.3 Nutzer*in verpflichtet sich, vorbehaltlich einer ausdrücklichen Genehmigung durch die Betreiberin keine ihr durch die Anwendung bekannt gewordenen Daten anderer Nutzer*innen in irgendeiner Form zu verwenden. Insbesondere ist es verboten, solche Informationen für Werbung, unerbetene E-Mails, andere unerwünschte Kontaktaufnahmen oder für andere unzulässige Zwecke zu verwenden.

D.2.7: AUFTRAGS-DATENVERARBEITUNGS-VERTRAG

Das folgende Muster wurde freundlicher Weise von der Agaplesion AG zur Verfügung gestellt.

Zusätzlich zu den von dem Beauftragten für Datenschutz der EKD bereitgestellten Hinweisen und Arbeitshilfen zur Erstellung eines Auftragsdatenverarbeitungsvertrages (AVV)[514] kann folgendes Muster zur Orientierung von Verantwortlichen verwendet werden, die einem diakonischen Werk angehören und somit den Bestimmungen des DSG-EKD unterliegen.

Sofern die kirchlichen Datenschutzbestimmungen auf die Auftragsverarbeiterin keine Anwendung finden, kann auch ein Vertragsmuster zur Auftragsverarbeitung nach DS-GVO von den Vertragsparteien zur Sicherstellung gleichwertiger Bestimmungen genutzt werden. Der Auftragnehmer unterwirft sich der kirchlichen Datenschutzaufsicht (vgl. § 30 Abs. 5 DSG-EKD).

Bitte erstellen Sie AVV **immer in Abstimmung mit ihrer zuständigen Datenschutzbeauftragten**! Sie wird Sie hinsichtlich der Notwendigkeit eines solchen Vertrages, der richtigen Vertragsvorlage sowie den auszufüllenden Punkten beraten. Auch Änderungen des Vertragstextes sollten Sie nur in Abstimmung mit Ihrem Datenschutzbeauftragten vornehmen.

Gelb markiert sind Informationen zur Bearbeitung. Dabei gibt es zum einen Hinweise – wie diese hier – die bei der Bearbeitung zu löschen sind, bzw. Beispieltexte, die bei der Bearbeitung unterstützen sollen und durch individuellen Text zu ersetzen sind.

Falls der DV als Anlage oder Nachtrag zu einem Hauptvertrag geschlossen wird, kann an dieser Stelle auf ihn verwiesen werden.

[514] https://datenschutz.ekd.de/infothek-items/av-vertrag/

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG NACH § 30 DATENSCHUTZGESETZ DER EVANGELISCHEN KIRCHE IN DEUTSCHLAND (DSG-EKD)

zwischen [einfügen Partei]
nachfolgend Auftraggeber genannt -

und [einfügen Partei]
nachfolgend Auftragnehmer genannt -

Präambel

Bei dem Auftraggeber handelt es sich um eine Einrichtung der Evangelischen Kirche in Deutschland. Der Auftraggeber unterliegt damit den Bestimmungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD).
Im Rahmen des zwischen Auftraggeber und Auftragnehmer bestehenden Hauptvertrags erhebt, verarbeitet oder nutzt der Auftragnehmer personenbezogene Daten des Auftraggebers beziehungsweise nimmt die Prüfung oder Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen des Auftraggebers in der Art vor, dass dabei ein Zugriff des Auftragnehmers auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann. Der Auftragnehmer verpflichtet sich, bei der Auftragsverarbeitung die Bestimmungen des DSG-EKD einzuhalten, die im Wesentlichen den Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) entsprechen. Diese Auftragsverarbeitung im Sinne von § 30 DSG-EKD wird durch die nachfolgende Vereinbarung entsprechend den gesetzlichen Vorschriften konkretisiert und geregelt. Es gelten die Begriffsbestimmungen des DSG-EKD.

Diese Vereinbarung wird mit ihrer Unterzeichnung wesentlicher Bestandteil des zugrundeliegenden Hauptvertrags. Gleiches gilt für alle Anlagen, auf welche diese Vereinbarung ausdrücklich Bezug nimmt. Andere zwischen den Parteien getroffene datenschutzrelevante Vereinbarungen, die ebenfalls für die hier geregelte Auftragsverarbeitung gelten, gehen dieser Vereinbarung nur dann vor, wenn sie die Regelungen dieser Vereinbarung weiter ausführen. Andere Vereinbarungen zwischen den Parteien, die den Kerngehalt der Bestimmungen dieser Vereinbarung verändern oder hinter dem hier vereinbarten Datenschutzniveau zurück bleiben, werden von dieser Vereinbarung verdrängt.

1. Gegenstand und Dauer der Auftragsverarbeitung

(1) Gegenstand und Dauer der Auftragsverarbeitung richten sich grundsätzlich nach den Regelungen des zugrundeliegenden Hauptvertrages. Gegenstand und Dauer der Auftragsverarbeitung werden zudem in Anlage 1 geregelt.

(2) Der Auftraggeber hat das Recht zur fristlosen Kündigung aus wichtigem Grund, wenn der Auftragnehmer datenschutzrechtliche Vorschriften oder ihm nach dieser Vereinbarung obliegende Pflichten erheblich verletzt. Eine erhebliche Pflichtverletzung liegt insbesondere dann vor, wenn die Pflichtverletzung zur Folge hat, dass der Auftraggeber seinen gesetzlichen Verpflichtungen als datenschutzrechtlich verantwortliche Stelle nicht nachkommen kann oder der Auftragnehmer einer Weisung des Auftraggebers nicht nachkommen kann oder will.

2. Umfang, Art und Zweck der Auftragsverarbeitung, Art der Daten und Kreis der Betroffenen

Die Verarbeitung und Nutzung der personenbezogenen Daten des Auftraggebers durch den Auftragnehmer und gegebenenfalls von dessen Unterauftragnehmern findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verarbeitung oder Nutzung in anderen Staaten bedarf der vorherigen Zustimmung des Auftraggebers und setzt die Gewährleistung eines angemessenen Datenschutzniveaus voraus. Umfang, Art und Zweck der Verarbeitung sind der Anlage 1 zu entnehmen. Gleiches gilt für Art der Daten und dem Kreis der Betroffenen.

3. Stand der Technik

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird diejenigen technischen und organisatorischen Maßnahmen (TOM) nach § 27 DSG-EKD treffen, die im Rahmen dieser Auftragsverarbeitung erforderlich sind, um die Ausführung der datenschutzrechtlichen Vorschriften zu gewährleisten. Dies bedeutet, dass in Abstimmung mit dem Auftraggeber solche technischen und organisatorischen Maßnahmen zu treffen sind, die in einem angemessenen Verhältnis zum Schutzbedürfnis der im Rahmen dieses Auftragsverhältnisses verarbeiteten personenbezogenen Daten stehen.

(2) Es sind insbesondere Maßnahmen zu den in § 27 Abs. 1 DSG-EKD genannten Punkten zu treffen:

- die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3) Der Stand der Technik wird durch eine Beschreibung der technischen und organisatorischen Maßnahmen dargestellt, welche im Rahmen dieses Vertragsverhältnisses als verbindlich festgelegt werden. Es wird auf Anlage 2 verwiesen. Alternativ kann dieser Vereinbarung auch ein durch den Auftragnehmer vorgelegtes und vom Auftraggeber akzeptiertes Sicherheitskonzept als Anlage 2 beigefügt werden, sofern dieses die Vorgaben von § 27 DSG-EKD angemessen umsetzt.

(4) Der Auftragnehmer hat dem Auftraggeber vor Beginn der Auftragsverarbeitung nachzuweisen, dass er die durch § 27 DSG-EKD geforderten Maßnahmen bei sich angemessen umgesetzt hat. Der Nachweis kann durch einschlägige Zertifikate, die der Auftragnehmer erhalten hat, belegt werden. Solche Zertifikate müssen durch unabhängige Institutionen (z. B. durch Wirtschaftsprüfer oder TÜV) auf der Basis relevanter Standards (z. B. ISO 27001 oder BSI-Grundschutz) erteilt worden sein.

(5) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(6) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer darf daher von mit dem Auftraggeber vereinbarten Maßnahmen abweichen und diese durch alternative mindestens gleichwertige oder höherwertige Maßnahmen ersetzen. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber vorab zur Beurteilung mitzuteilen.

(7) Verarbeitet der Auftragnehmer auch andere Daten als solche des Auftraggebers,garantiert der Auftragnehmer, dass diese Daten durch technische und organisatorische Maßnahmen von den Daten des Auftraggebers getrennt sind und bleiben.

4. Berichtigung, Löschung und Sperrung von Daten

(1) Die Berichtigung, Löschung und Sperrung personenbezogener Daten erfolgt durch den Auftragnehmer nur dann, wenn er dazu entsprechende Weisungen des Auftraggebers erhalten hat.

(2) Sollte sich ein Betroffener unmittelbar an den Auftragnehmer wegen der Berichtigung, Löschung oder Sperrung seiner Daten wenden, so wird der Auftragnehmer dieses Begehren unverzüglich an den Auftraggeber weiterleiten, der dann bezüglich des weiteren Vorgehens entscheidet.

(3) Ist der Auftraggeber gegenüber einer betroffenen Person verpflichtet, dieser Auskünfte zur Auftragsverarbeitung zu erteilen, wird der Auftragnehmer auf eigene Kosten dem Auftraggeber bei der Ermittlung der zu diesem Zweck benötigten Informationen unterstützen.

(4) Beim Auftragnehmer im Rahmen der Auftragsverarbeitung anfallendes Test- und Ausschussmaterial ist dagegen unverzüglich durch den Auftragnehmer zu vernichten. Bis zur Vernichtung ist dieses Material gesichert aufzubewahren. Die Vernichtung hat mit einem Verfahren, das dem Stand der Technik entspricht, zu erfolgen.

(5) Soweit der Auftragnehmer im Rahmen der Prüfung oder Wartung von automatisierten Verfahren und Datenverarbeitungsanlagen des Auftraggebers defekte oder nicht mehr benötigte Datenspeicher ausbaut, sind diese beim Auftragnehmer gesichert aufzubewahren, bis sie einer Reparatur, Entsorgung oder weiteren Verwendung zugeführt werden. Vor einer

Weitergabe der Komponenten an Dritte hat der Auftragnehmer sicherzustellen, dass alle darauf gespeicherten Daten des Auftraggebers physisch gelöscht sind. Diese Verfahrensweise ist auch einzuhalten, wenn der Auftragnehmer im Rahmen der Auftragsverarbeitung von ihm genutzte Datenspeicher ausbaut, soweit diese Daten des Auftraggebers enthalten.

5. Pflichten des Auftraggebers

(1) Der Auftraggeber ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweiligen einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus § 32 DSG-EKD und §15a TMG resultierenden Informationspflichten zu möglichen oder eingetretenen Datenschutzvorfällen.

(4) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(5) Der Auftraggeber verpflichtet sich, alle nicht allgemein bekannten Angelegenheiten und insbesondere die Geschäfts- und Betriebsgeheimnisse des anderen Vertragspartners unbefristet streng vertraulich zu behandeln. Solche Informationen werden nur im Rahmen der Vertragsbeziehung und zur Erreichung des Vertragszwecks genutzt. Sie werden weder aufgezeichnet noch weitergegeben.

6. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, die Bestimmungen zur Auftragsverarbeitung nach § 30 DSG-EKD einzuhalten und unterstellt sich der Kontrolle durch die zuständige kirchliche Datenschutzaufsichtsbehörde. Bei nicht-kirchlichem Auftragnehmer übernimmt die Behörde insbesondere die Aufgaben nach §43 DSG-EKD sowie die Befugnisse §44 DSG-EKD unmittelbar gegenüber dem nicht-kirchlichen Auftragnehmer.

(2) Der Auftragnehmer stellt sicher, dass bei Durchführung der Tätigkeiten in seinem Verantwortungsbereich das DSG-EKD sowie sämtliche speziellen datenschutzrechtlichen Vorschriften, denen der Auftraggeber unterliegt, eingehalten werden. Hierzu verarbeitet der Auftragnehmer personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer speichert keine Daten des Auftraggebers auf Systemen außerhalb des eigenen Verfügungsbereichs.

(3) [Der nächste Absatz ist nicht erforderlich und kann gelöscht werden, wenn die Einrichtung Auftragnehmer ist.]
Die Verarbeitung von Daten in Privatwohnungen ist grundsätzlich zulässig. Ausnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers. Für den jeweiligen Einzelfall sind die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten festzulegen. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch der Auftraggeber oder die Beauftragte für den Datenschutz der EKD oder den Beauftragten für den Datenschutz der EKD vorher mit dem Auftragsverarbeiter abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(4) Nach § 30 Abs. 4 DSG-EKD darf der Auftragnehmer die personenbezogenen Daten des Auftraggebers nur im Rahmen dieser Vereinbarung und der dazu ergangenen Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

6.1 Stillschweigen

Der Auftragnehmer verpflichtet sich, alle nicht allgemein bekannten Angelegenheiten und insbesondere die Geschäfts- und Betriebsgeheimnisse des anderen Vertragspartners unbefristet streng vertraulich zu behandeln. Solche Informationen werden nur im Rahmen der Vertragsbeziehung und zur Erreichung des Vertragszwecks genutzt. Sie werden weder aufgezeichnet noch weitergegeben.

6.2 Beauftragter für den Datenschutz

Sofern der Auftragnehmer nach §§ 36 ff. DSG-EKD bzw. Art. 37 ff. DSGVO gesetzlich hierzu verpflichtet ist, hat er einen Betriebs-/Beauftragten für den Datenschutz zu bestellen. Auf Verlangen des Auftraggebers hat er diesem dessen Kontaktdaten zu nennen und die Bestellung unter Vorlage einer Kopie der Bestellungsurkunde nachzuweisen. Die Kontaktdaten sind in Anlage 4 aufzuführen.

6.3 Datengeheimnis

(1) Der Auftragnehmer hat bei der Auftragsverarbeitung ausschließlich Personen einzusetzen, die schriftlich auf das Datengeheimnis nach § 26 DSG-EKD bzw. Artt. 28, 29 DSGVO verpflichtet wurden und mit den für sie maßgeblichen Bestimmungen des Datenschutzes, der Bestimmungen dieser Vereinbarung und der aufgrund dessen erteilten Weisungen vertraut gemacht wurden. Entsprechende Nachweise hat er dem Auftraggeber auf dessen Verlangen vorzulegen.

(2) Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäftsgeheimnissen des Auftraggebers zu verpflichten und müssen auf § 23 GeschGehG hingewiesen werden. Weiterhin müssen die vom Auftragnehmer eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht. Eine gesetzliche Offenbarungspflicht des Auftragnehmers bleibt hiervon unberührt.

[Der Abschnitt 6.4 ist nicht erforderlich und kann gelöscht werden, wenn keine Daten eines Berufsgeheimnistärgers verarbeitet.]

6.4 Schweigepflicht von Berufsgeheimnisträgern

(1) Eine Kenntnisnahme von Informationen des Auftraggebers, die einem Berufsgeheimnis im Sinne von § 203 StGB (vgl. dazu Gesetzestext in Anlage 5) unterliegen, durch den Auftragnehmer (bzw. durch seine Mitarbeiter), stellen kein Offenbaren im Sinne der vorgenannten Vorschrift dar. Eine solche Offenbarung ist strafrechtlich irrrelevant, soweit dies für die Vorbereitung und Ausführung der beauftragten Tätigkeit durch den Auftragnehmer erforderlich ist. Für die Einrichtung und Wartung von IT-Anlagen und Systemen ist ein Offenbaren regelmäßig zur Aufgabenerfüllung erforderlich.

(2) Der Auftragnehmer verpflichtet sich seine Kenntnisnahme auf die erforderlichen Daten zu beschränken und die Verarbeitung der Daten ausschließlich zur Erfüllung vertraglich vereinbarter Pflichten vorzunehmen.

(3) Alle Mitarbeiter sind nicht nur auf das Datengeheimnis zu verpflichten, sondern auch über die Verschwiegenheit nach § 203 StGB schriftlich zu belehren.

(4) Dem Auftragnehmer ist bekannt, dass die einem Berufsgeheimnis unterliegenden Daten dem Zeugnisverweigerungsrecht gemäß § 53a StPO unterfallen. Die Ausübung des Zeugnisverweigerungsrechts obliegt dem Berufsgeheimnisträger. Der Auftragnehmer stimmt sich mit diesem ab.

(5) Dem Auftragnehmer ist bekannt, dass die sich in seinem Gewahrsam befindlichen und einem Berufsgeheimnis unterliegenden Daten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren

(6) Über Maßnahmen von Strafverfolgungsorganen wird der Auftragnehmer den Auftraggeber unaufgefordert und unverzüglich benachrichtigen, soweit hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist oder sein kann. Die Benachrichtigungspflicht des Auftraggebers besteht nicht, soweit dieser durch die Benachrichtigung gegen ein gesetzliches Verbot verstoßen würde.

6.5 Kontrollen durch den Auftragnehmer

(1) Der Auftragnehmer hat durch geeignete und regelmäßige Kontrollen sicherzustellen, dass bei der Auftragsverarbeitung nicht gegen Datenschutzvorschriften oder die Regelungen dieser Vereinbarung oder die zugehörigen Weisungen verstoßen wird. Entsprechende Kontrollen sind vom Auftragnehmer auch bei den von ihm im Rahmen der Auftragsverarbeitung eingesetzten Unterauftragnehmern vorzunehmen. Auf Verlangen hat der Auftragnehmer dem Auftraggeber die Durchführung dieser Kontrollen, die dabei erhaltenen Ergebnisse und getroffenen Maßnahmen nachzuweisen.

(2) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSG-EKD oder andere Vorschriften über den Daten-

schutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Eine materiell rechtliche Prüfung steht dem Auftragnehmer nicht zu.

6.6 Kontrollen beim Auftragnehmer durch Datenschutzaufsichtsbehörden

(1) Kontrollhandlungen und Maßnahmen der zuständigen Aufsichtsbehörde werden umgehend zwischen den Vertragsparteien kommuniziert. Der Auftragnehmer unterwirft sich den entsprechenden (landes-)rechtlichen bzw. kirchlichen Bestimmungen hinsichtlich der Kontrolle bzgl. der dieser Vereinbarung zugrundeliegenden Datenverarbeitung der Kontrolle durch die für den Auftraggeber zuständige Aufsichtsbehörde.

(2) Die Prüfungs-, Zutritts- und Auskunftsrechte, welche in 8. geregelt sind, stehen auch der oder dem Beauftragten für den Datenschutz der EKD zu.

(3) Über Kontrollen und Maßnahmen der oder des staatlichen Datenschutzbeauftragten oder der oder des Beauftragten für den Datenschutz der EKD wird der Auftragnehmer den Auftraggeber unaufgefordert unverzüglich in Kenntnis setzen, sofern hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist.

6.7 Verzeichnis von Verarbeitungstätigkeiten

Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten für die bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne von Art. 31 DSG-EKD. Auf Anforderung des Auftraggebers oder der zuständigen Aufsichtsbehörde stellt er diesen die notwendigen Angaben zur Verfügung.

6.8 Datenschutz-Folgenabschätzung

Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

6.9 Rechte und Eigentum an Datenträgern und Dokumenten

Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

6.10 Berichtung, Löschung, Sperrung

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6.11 Pfändung, Beschlagnahme

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

7. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. [Der nächste Halbsatz ist nicht erforderlich und kann gelöscht werden, wenn keine Daten eines Berufsgeheimnisträgers verarbeitet werden und Absatz 6.4 im Vertrag gelöscht wurde: und beinhaltet auch die Belehrung auf die Verschwiegenheit nach § 203 StGB.] Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Die Kontroll- und Überprüfungsrechte sind entsprechend dieser Vereinbarung auch mit dem Unterauftragnehmer zu vereinbaren und einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis zu erhalten. Bei einem Verstoß gegen die in diesem Absatz genannten Pflichten, insbesondere wenn Unterauftragnehmer ohne schriftliche Zustimmung des Auftraggebers eingesetzt werden, steht dem Auftraggeber ein außerordentliches Kündigungsrecht zu.

(2) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 3 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(3) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers.

(4) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen. Die mit den Unterauftragnehmern ausgehandelten Preise können geschwärzt werden. Der Auftragnehmer haftet für das Handeln von Unterauftragnehmern wie für eigenes Handeln.

(5) Keine zustimmungspflichten Dienstleistungen im Rahmen eines Unterauftragsverhältnisses sind Nebenleistungen Dritter, die der Auftragnehmer zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen beispielsweise Prüfer oder die Entsorgung von Datenträgern, Reinigungsdienste, Telekommunikationsleistungen oder Wartungs- und Benutzerdienste. Der Auftragnehmer beachtet auch in diesem Zusammenhang datenschutzrechtliche Vorgaben und führt entsprechende Kontrollmaßnahmen durch.

(6) Bei der Vergabe von Unterauftragsverhältnissen muss der Auftragnehmer sicherstellen, dass der Auftraggeber zur Durchführung von Kontrollen beim Unterauftragnehmer berechtigt ist. Der Auftraggeber ist berechtigt, diese Kontrollen auch durch Dritte vornehmen zu lassen.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, regelmäßig beim Auftragnehmer die Einhaltung der Bestimmungen dieser Vereinbarung und der aufgrund derer erteilten Weisungen sowie insbesondere die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen zu überprüfen. Der Auftraggeber führt vorgesehene Auftragskontrollen in Absprache mit dem Auftragnehmer durch. Im Einzelfall kann er auch fachkundige Prüfer für die Durchführung benennen. Er hat das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Diese sind rechtzeitig anzumelden und abzustimmen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle
erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Der Auftraggeber kann

- Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen und/oder
- nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Der Auftragnehmer ist zur Duldung und Mitwirkung bei den Kontrollen verpflichtet. Die Durchführung der Kontrollen ist rechtzeitig zwischen Auftraggeber und Auftragnehmer abzustimmen.

(3) Im Rahmen von Kontrollen hat der Auftragnehmer dem Auftraggeber Zutritt zu denjenigen Räumlichkeiten zu gewähren, in welchen die Auftragsverarbeitung stattfindet. Der Auftragnehmer hat dem Auftraggeber zudem die notwendigen Auskünfte zu erteilen und relevante Unterlagen vorzulegen.

9. Mitzuteilende Verstöße des Auftragnehmers

(1) Der Auftragnehmer und die bei ihm beschäftigten Personen haben den Auftraggeber bei Störungen des Verarbeitungsablaufs, bei Verdacht auf Datenschutzverletzungen oder Verstößen gegen die in dieser Vereinbarung getroffenen Festlegungen und anderen Unregelmäßigkeiten bei der Auftragsverarbeitung unverzüglich zu informieren. Dies gilt in besonderem Maße, wenn sensible Daten im Sinne des § 32 DSG-EKD (bzw. Art. 33 DSGVO) unrechtmäßig übermittelt worden sind oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

(2) Gleichermaßen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

10. Umfang der Weisungsbefugnisse des Auftraggebers

(1) Der Auftraggeber ist die verantwortliche Stelle im Sinne von § 4 Abs. 9 DSG-EKD und damit alleine zuständig für die Beurteilung der Zulässigkeit dieser Auftragsverarbeitung sowie für die Wahrung der Rechte der Betroffenen.

(2) Der Auftraggeber hat das Recht, dem Auftragnehmer hinsichtlich der Auftragsdatenverarbeitung Weisungen zu erteilen. Eine Weisung im Sinne dieser Vereinbarung ist eine einseitige Anordnung des Auftraggebers gegenüber dem Auftragnehmer, welche auf einen bestimmten Umgang mit personenbezogenen Daten bei der Auftragsverarbeitung gerichtet ist. Die Erteilung von Weisungen hat in Schrift- oder Textform zu erfolgen.

(3) Auskünfte an Dritte oder an Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

11. Beendigung der Auftragsverarbeitung

Auf Verlangen des Auftraggebers, spätestens jedoch nach der Beendigung der Auftragsverarbeitung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Ergebnisse der Auftragsverarbeitung und Datenbestände, dem Auftraggeber herauszugeben oder nach dessen vorheriger Zustimmung physisch zu löschen.

12. Löschung von Daten und Rückgabe von Datenträgern

(1) Der Auftragnehmer hat die vom Auftraggeber überlassenen Unterlagen einschließlich Schriftstücke, Disketten, CD-ROMs, sonstigen Speichereinheiten und Ähnliches als Unterlagen des Auftraggebers zu kennzeichnen, getrennt von seinen Unterlagen aufzubewahren und durch geeignete Maßnahmen in besonderer Weise gegen den Zugriff Unberechtigter zu schützen und gegen die nicht vertragsgemäße Nutzung, Vervielfältigung und Weitergabe zu sichern. Diese Verpflichtung schließt ein, dass die Unterlagen bei Abwesenheit des Bearbeiters verschlossen zu halten sind. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

(2) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung hat mit einem Verfahren, das dem Stand der Technik entspricht, zu erfolgen. Ein Protokoll der Löschung ist dem Auftraggeber auf dessen Verlangen auszuhändigen.

(3) Der Auftragnehmer garantiert dem Auftraggeber die ordnungsgemäße Vernichtung nicht benötigten Datenmaterials (Probeausdrucke, überzählige Listen etc.). Zu entsorgende Unterlagen sind nach DIN 66399 unleserlich zu machen.

13. Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSG-EKD oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich.
Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

14. Schlussbestimmungen

(1) Unabhängig von der Verpflichtung des Auftragnehmers, personenbezogene Daten gemäß den Vorschriften des DSG-EKD und sonstiger datenschutzrechtlicher Vorschriften, gemäß den Bestimmungen dieser Vereinbarung und der aufgrund dessen erteilten Weisungen zu verarbeiten, ist der Auftragnehmer zudem auch zur Vertraulichkeit im Hinblick auf Betriebs- und Geschäftsgeheimnisse des Auftraggebers verpflichtet. Diese Verpflichtung gilt für alle betrieblichen und geschäftlichen Angelegenheiten und sonstige Informationen, über die der Auftragnehmer im Rahmen der Auftragsverarbeitung Kenntnis erlangt und die ihrer Natur nach vertraulich zu behandeln sind. Der Auftragnehmer hat bezüglich dieser Informationen gegenüber unbefugten Dritten Stillschweigen zu bewahren. Etwaige weitergehende Regelungen, die im zugrundeliegenden Hauptvertrag getroffen wurden, bleiben unberührt. Die Verpflichtung zur Wahrung der Vertraulichkeit gilt über das Vertragsende hinaus.

(2) Es gilt deutsches Recht. Erfüllungsort und Gerichtsstand ist der Sitz des Auftraggebers.

(3) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Bestimmungen dieser Vereinbarung unvollständig, unwirksam oder undurchführbar sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. In diesem Fall ist die unvollständige, unwirksame oder undurchführbare Bestimmung durch eine Regelung zu ersetzen, die dem entspricht, was die Parteien gewollt hätten, wenn sie die Unvollständigkeit, Unwirksamkeit oder Undurchführbarkeit gekannt hätten.

Ort, Datum, Firma, Unterschrift (Auftraggeber)

Ort, Datum, Firma, Unterschrift (Auftraggeber)

ANLAGE 1 – AUFTRAGSSPEZIFISCHE VEREINBARUNGEN

[Alternative 1 (Falls der ADV als Anlage oder Nachtrag zu einem Hauptvertrag geschlossen wird, kann an dieser Stelle auf ihn verwiesen werden.):]

Bezüglich Gegenstand und Dauer der Auftragsverarbeitung wird auf [Bezeichnung des Hauptvertrages] vom [Datum] verwiesen.

[Alternative 2 (Wenn kein Hauptvertrag vorliegt oder dieser keine ausreichenden Regelungen enthält, sollten an dieser Stelle Gegenstand und Dauer der Auftragsverarbeitung festgelegt werden.):]

1. Gegenstand und Dauer der Auftragsverarbeitung

Gegenstand der Auftragsverarbeitung:

Dauer der Auftragsverarbeitung:

[Beispiele]

- „Diese Vereinbarung tritt mit Unterzeichnung in Kraft und wird auf unbestimmte Zeit geschlossen."
- „Diese Vereinbarung tritt zum …. in Kraft und wird auf unbestimmte Zeit geschlossen."
- „Diese Auftragsverarbeitung beginnt am …. und endet am …"

2. Umfang, Art und Zweck der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Umfang, Art und Zweck der Datenverarbeitung:

Art der Daten (Kategorie):

Kreis der Betroffenen (Kategorien):

ANLAGE 2 – SICHERHEIT DER VERARBEITUNG – STAND DER TECHNIK - TOM

[Anmerkung :Nachfolgend sind die durch den Auftragnehmer realisierten technischen und organisatorischen Sicherheitsmaßnahmen (TOM) konkret darzustellen. Die unten dargestellten Sicherheitsmaßnahmen sind nur beispielhaft zu verstehen.Alternativ kann auch ein durch den Auftragnehmer vorgelegtes und vom Auftraggeber akzeptiertes Sicherheitskonzept als Anlage 2 beigefügt werden, sofern dieses die Vorgaben von § 9 DSG-EKD angemessen umsetzt.]

1. Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

[z. B.: Zutrittskontrollsystem, Ausweisleser, Chipkarten, kontrollierte Schlüsselvergabe Vereinzelungsanlage, Personenkontrolle durch Pförtner, Einbruchmeldeanlage, Bewegungsmelder, Glasbruchmelder, Videoüberwachung, Außenhautsicherheit]

2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

[z. B.: Passwort-Richtlinie, Protokollierung der Passwortnutzung und Chipkartennutzung, regelmäßige Kontrolle der Protokolle, Firewall, Virenscanner, Verwendung von dem Stand Technik entsprechenden Verschlüsselungsverfahren.]

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

[z. B.: systemimmanente Sicherungsmechanismen, übergeordnetes Zugriffsschutzsystem Berechtigungsvergabe nach vorgegebenen Rollen und Profilen, Mehraugenprinzip, automatische Prüfung der Zugriffsberechtigung, Protokollierung der Zugriffe, regelmäßige Kontrolle der Protokolle, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren]

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

[z.B.: physische oder logische Trennung von Anwendungssystemen, Trennung nach Mandanten oder Buchungskreisen, Trennung über Zugriffsregelung, Trennung von Produktionsumgebung sowie Test- und Entwicklungsumgebung, Mehraugenprinzip]

5. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

[z.B.: Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, VPN, Regelungen zur Datenträgervernichtung, sicherer Transport von Datenträgern, Taschenkontrollen]

6. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

[z.B.: Protokollierung der Systemaktivitäten, Verarbeitungsprotokolle, regelmäßige Kontrolle der Protokolle]

7. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

[z.B. Erteilung von Weisungen, Festlegung und Abgrenzung der Kontrollen von Auftraggeber und Auftragnehmer, vertragliche Regelungen mit und Kontrollen bei Unterauftragnehmern]

8. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

[z.B. Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort von Datensicherungskopien, Auslagerung von Sicherungskopien, Notstromaggregate, unter- brechungsfreie Stromversorgung, Brandschutz, Katastrophenplan]

9. Pseudonymisierung

Maßnahmen, die gemäß § 27 Abs. 1 Nr. 1 DSG EKD, gewährleisten, dass verarbeitete Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

10 Evaluierung

Maßnahmen, zur Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (z.B. Datenschutz-Management; Incident-Response-Management; Datenschutzfreundliche Voreinstellungen (§ 27 Abs. 1 Nr. 4 DSG-EKD); Auftragskontrolle)

ANLAGE 3:

Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Name und Anschrift des Unterauftragnehmers	**Beschreibung der Teilleistungen**	**Ort der Leistungserbringung**

ANLAGE 4:

Bestellter betrieblicher Datenschutzbeauftragter:

Name und Anschrift des betrieblichen Datenschutzbeauftragten:

ANLAGE 5:

[Die Anlage 5 ist nicht erforderlich und kann gelöscht werden, wenn keine Daten des Berufsgeheimnistärgers verarbeitet werden und Absatz 6.4 im Vertrag gelöscht wurde.]

Schweigepflicht von Berufsgeheimnisträgern, § 203

(Verletzung von Privatgeheimnissen – Stand Juli 2020)

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) 1Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger oder Europäischer Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. 2Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

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

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

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis

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

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

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

D.2.8: VEREINBARUNG GEMEINSAM VERANT-WORTLICHE STELLE

VEREINBARUNG ÜBER DIE GEMEINSAME VERARBEITUNG PERSONENBEZOGENER DATEN GEMÄSS § 29 EKD-DATENSCHUTZGESETZ (DSG-EKD)

Zwischen [einfügen Partei]
vertreten durch [einfügen Vertreterin]

und [einfügen Partei]
vertreten durch [einfügen Vertreterin]

Präambel

Dieser Vertrag umfasst Leistungen, die beide Vertragsparteien (in Folge auch „Parteien“ genannt) zum Betrieb des Portals „[einfügen Name]“ (im Folgenden Portal genannt) erbringen. Beide Parteien betreiben dieses Portal gemeinsam.

Für jede Partei gilt das DSG-EKD (ggf. ein anderes Datenschutzgesetz [zB. das KDG] basierend auf der Rechtsgrundlage des Art. 140 GG, Art. 137 Abs. 3 WRV iVm. Art. 91 EU-DSGVO. Für die [einfügen Partei] gilt das Datenschutzgesetz der Evangelischen Kirche von Deutschland (im folgenden DSG-EKD genannt). Bei der Verwendung des Begriffs Mitarbeitende bezieht sich dies ausschließlich auf Mitarbeitende beider Vertragsparteien. Entsprechend den gesetzlichen Vorgaben des § 29 DSG-EKD konkretisiert diese Vereinbarung die gemeinsame Verantwortlichkeit beider Vertragsparteien.

§ 1

(1) Diese Vereinbarung regelt die Rechte und Pflichten der Parteien bei der gemeinsamen Verarbeitung personenbezogener Daten. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Beschäftigte der Parteien oder durch sie beauftragte Auftragsverarbeiter personenbezogene Daten für die Verantwortlichen verarbeiten. Die Parteien haben die Mittel und Zwecke der nachfolgend näher beschriebenen Verarbeitungstätigkeiten gemeinsam festgelegt. Die gemeinsame Verarbeitung bezieht sich ausschließlich auf den Betrieb des Portals.

(2) Im gemeinsam betriebenen Portal werden personenbezogene Daten verarbeitet. Die Verarbeitung erfolgt über einen Auftragsverarbeitungsvertrag (im Folgenden AV-Vertrag genannt) mit der [einfügen Firma] (im Folgenden Auftragsverarbeiter genannt). Beide Parteien sind hier als verantwortliche Stelle benannt und geben nach gegenseitiger Rücksprache konkret Weisungen an die Auftragsverarbeiterin (siehe Anlage AV-Vertrag).

Für den gesamten Betrieb des Portals gilt nach den Vorgaben des § 29 DSG-EKD folgende Vereinbarung:

§ 2

Beide Parteien betreiben das Portal als gemeinsam Verantwortliche. Alle Änderungen oder Weisungen erfolgen nur nach gemeinsamer Abstimmung. Die Weitergabe von Weisungen an den Auftragsverarbeiter erfolgt durch im AV-Vertrag festgelegte Personen. Jede Weisung erfolgt schriftlich und wird schriftlich bestätigt.

§ 3

Jede Partei gewährleistet die Einhaltung der gesetzlichen Bestimmungen, insbesondere die Rechtmäßigkeit der durch sie auch im Rahmen der gemeinsamen Verantwortlichkeit durchgeführten Datenverarbeitungen. Um die technische Sicherheit gem. § 27 DSG-EKD zu gewährleisten, wird das Portal alle zwei Jahre durch einen externen Datenschutzauditor auditiert. Beide Parteien verpflichten sich Risiken oder Mängel, die im Auditbericht dokumentiert sind, entsprechend den Vorgaben im Bericht abzustellen. Mängel, die mit einem hohen Risiko für die Betroffenen behaftet sind oder eine Datenschutzverletzung hervorrufen können, sind unverzüglich abzustellen. Unwesentliche, kleinere Mängel, die kein hohes Risiko für den Betroffenen darstellen, müssen spätestens bis zum nächsten Audit behoben sein (so auch die Vorgaben der DIN ISO/IEC 27001 und des Grundschutzes nach BSI 200).

§ 4

Die Parteien speichern über den Auftragsverarbeiter die personenbezogenen Daten in einem strukturierten gängigen und maschinenlesbaren Format. Beide Parteien tragen dafür Sorge, dass nur personenbezogene Daten verarbeitet werden, die für den rechtmäßigen Betrieb des Portals zwingend erforderlich sind und für die die Zwecke und Mittel der Verarbeitung durch das jeweilige kirchliche Datenschutzrecht vorgegeben sind. Im Übrigen beachten beide Vertragsparteien den Grundsatz der Datenminimierung im Sinne des § 5 Abs. 3 DSG-EKG.

§ 5

Beide Parteien gewährleisten gemeinsam, der betroffenen Person die gemäß § 17 DSG-EKD erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen. Die Parteien stellen die Informationen in einem gemeinsamen Dokument, welches beide Datenschutzgesetzte berücksichtigt, zur Verfügung. Im Portal ist eine gemeinsam erstellte Datenschutzerklärung vorhanden, die den Anforderungen des § 17 DSG-EKG erfüllt.

§ 6

Betroffene Personen können die ihnen aus den §§ 19-25 DSG-EKD zustehenden Rechte gegenüber beiden Vertragsparteien geltend machen. Gestellte Auskunftsbegehren werden über eine gemeinsam entwickelte Vorlage schriftlich erstellt und werden nach gemeinsamer Abstimmung dem Auskunftssuchenden fristgerecht und in schriftlicher Form zugestellt. Auskunftssuchende können ihr Auskunftsbegehren an beide Parteien richten oder über den bestellten Datenschutzbeauftragten anfordern.

§ 7

(1) Beide Parteien verpflichten sich, der Auskunftspflicht gemäß § 19 DSG-EKD nachzukommen. Beide Parteien verpflichten sich, den betroffenen Personen, die diesen gemäß § 19 DSG-EKD zustehenden Auskünfte auf Nachfrage zur Verfügung zu stellen.

(2) Nach Auskunftsersuchen des Betroffen wird über das Portal geprüft, ob und welche personenbezogenen Daten im Portal vorhanden sind. Dies erfolgt über eine Weisung im Rahmen des AV-Vertrages mit der Auftragsverarbeiterin. Diese führt eine Suchabfrage im Portal durch und sendet die Auskunftsinformationen an beide verantwortlichen Parteien. Diese geben die Daten an den Datenschutzbeauftragten. Dieser prüft, ob die Auskunft den Anforderungen des § 19 DSG-EKD erfüllt. Nach Prüfung des Datenschutzbeauftragten werden die Informationen den Betroffenen per Post oder verschlüsselt digital zugestellt. Der Gesamtprozess beträgt maximal 20 Tage.

§ 8

(1) Soweit sich eine betroffene Person an eine der Parteien in Wahrnehmung ihrer Betroffenenrechte wendet, insbesondere wegen Auskunft oder Berichtigung und Löschung ihrer personenbezogenen Daten, verpflichten sich die Parteien, dieses Ersuchen unverzüglich und unabhängig von der Pflicht zur Gewährleistung des Betroffenenrechtes an die andere Partei weiterzuleiten. Diese ist verpflichtet, der anfragenden Vertragspartei die zur Auskunftserteilung notwendigen Informationen aus ihrem Wirkbereich unverzüglich zur Verfügung zu stellen.

(2) Sollen personenbezogene Daten gelöscht werden, informieren sich die Parteien zuvor gegenseitig. Die jeweils andere Partei kann der Löschung aus berechtigtem Grund widersprechen, etwa sofern sie eine gesetzliche Aufbewahrungspflicht trifft.

§ 9

Die Parteien informieren sich gegenseitig unverzüglich und vollständig, wenn sie bei der Prüfung der Verarbeitungstätigkeiten Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellen.

§ 10

Die Parteien verpflichten sich, den wesentlichen Inhalt der Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit den betroffenen Personen zur Verfügung zu stellen (§ 29 Abs. 2 DSG-EKD).

§ 11

Beiden Parteien obliegen die aus den §§ 32, 33 DSG-EKD resultierenden Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen. Die Parteien stimmen Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemeinsam ab. Die Meldungen an die Aufsichtsbehörde werden nach Abstimmung in gemeinsamer Verantwortlichkeit an die Aufsichtsbehörde übermittelt:

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland, Hr. Michael Jacob, Böttcherstr. 7, 30419 Hannover, Tel.: 0511 76 81 28-0, Fax: 0511 76 81 28-20, E-Mail: michael.jacob@datenschutz.ekd.de

§ 12

Dokumentationen im Sinne von § 5 Abs. 2 DSG-EKD, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, werden durch jede Partei entsprechend den rechtlichen Befugnissen und Verpflichtungen über das Vertragsende hinaus aufbewahrt.

§ 13

(1) Die Parteien stellen innerhalb ihres Wirkbereiches sicher, dass alle mit der Datenverarbeitung befassten Mitarbeitenden gemäß § 26 DSG-EKD auf das Datengeheimnis verpflichtet sind sowie in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen werden.

(2) Die Parteien haben eigenständig dafür Sorge zu tragen, dass sie sämtliche in Bezug auf die Daten bestehenden gesetzlichen Aufbewahrungspflichten einhalten. Sie haben hierzu angemessene Datensicherheitsvorkehrungen (§ 27 DSG-EKD, § 26 KDG) zu treffen. Dies gilt insbesondere im Falle der Beendigung der Zusammenarbeit.

(3) Die Implementierung, Voreinstellung und der Betrieb der Systeme sind unter Beachtung der Vorgaben der DSG-EKD, KDG und anderer Regelungswerke, insbesondere unter Beachtung der Grundsätze des Datenschutzes durch Design und datenschutzfreundliche Voreinstellungen (privacy by design and privacy by default) sowie unter Verwendung von dem Stand der Technik entsprechenden geeigneten technischen und organisatorischen Maßnahmen durchzuführen.

(4) Die im Zuge der Abwicklung der Leistungen zu verarbeitenden personenbezogenen Daten werden auf besonders geschützten Servern gespeichert. Die eingesetzten Server sind gem. DIN ISO/IEC 27001 zertifiziert.

§ 14

(1) Die Parteien verpflichten sich beim Einsatz von Auftragsverarbeiterinnen im Anwendungsbereich dieser Vereinbarung (siehe § 1), einen Vertrag nach § 30 DSG-EKD abzuschließen und die schriftliche Zustimmung der anderen Vertragspartei vor Abschluss des Vertrages einzuholen.

(2) Die Parteien informieren sich gegenseitig rechtzeitig über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von als Subunternehmer eingesetzten Auftragsverarbeiterin und beauftragen nur solche Subunternehmer, die die Anforderungen des Datenschutzrechts und die Festlegungen dieses Vertrages erfüllen. Nicht als Leistungen von Subunternehmern im Sinne dieser Regelung gelten Dienstleistungen, die die Vertragsparteien bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nehmen, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Die Parteien sind jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Es werden nur Auftragsverarbeiterinnen in Zusammenhang mit diesem Vertrag eingesetzt, die der gesetzlichen Pflicht zur Bestellung eines Datenschutzbeauftragten unterliegen.

(4) Der Datenschutzbeauftragte des Portals wird die Einhaltung des Vertrages datenschutzrechtlich betreuen und bei Verdacht auch Verletzungen oder bei datenschutzrechtlichen Fragen die Vertragsparteien beraten.

§ 15

Die Parteien erstellen ein Verzeichnis von Verarbeitungstätigkeiten gem. § 31 DSG-EKD, auch und insbesondere mit einem Vermerk zur gemeinsamen Verantwortung.

§ 16

(1) Unbeschadet der Regelungen dieses Vertrages haften die Parteien für den Schaden, der durch eine nicht dem DSG-EKD entsprechende Verarbeitung verursacht wird, im Außenverhältnis gemeinsam gegenüber den betroffenen Personen.

(2) Im Innenverhältnis haften die Parteien, unbeschadet der Regelungen dieses Vertrages, nur für Schäden, die innerhalb ihres jeweiligen Wirkbereiches entstanden sind.

§ 17

Sollte eine der Regelungen des AVV oder einer mit Bezug hierauf geschlossenen weiteren Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden oder der AVV eine nach übereinstimmender Auffassung der Parteien regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Anstelle der unwirksamen Regelung oder in Ausfüllung der Lücke gelten die gesetzlichen Bestimmungen.