5 Verantwortlichkeiten

Bei der Verantwortlichkeit für die Verarbeitung von personenbezogenen Daten im Rahmen von medizinischen Forschungsvorhaben ist zu **unterscheiden** zwischen der datenschutzrechtlichen und der strafrechtlichen Verantwortlichkeit, die insbesondere in § 203 StGB thematisiert wird.[196] Da die strafrechtliche Regelung in § 203 StGB zugleich im Standes- und Medizinrecht relevant ist und Rückwirkungen auf den Datenschutz hat, wird hierauf im Folgenden ausführlich eingegangen. Weiterhin sind diese beiden Formen der Verantwortlichkeit zu unterscheiden von der zivilrechtlichen Verantwortung, also insbesondere für Ansprüche aus Vertrag, auch Behandlungsvertrag (§§ 630a ff. BGB), sowie für Schadenersatzansprüche (§§ 823 ff. BGB sowie Art. 82 DSGVO).[197]

5.1 Verantwortlichkeit

Wer Verantwortlicher i.S.d. DSGVO ist, wird in Art. 4 Nr. 7 definiert. Danach ist

> *„Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung*

196 Auf die Verknüpfung der datenschutzrechtlichen mit der strafrechtlichen Verantwortlichkeit in § 42 BDSG wird hier nicht näher eingegangen.

197 Auf die datenschutzrechtlich begründeten Schadenersatzansprüche nach Art. 82 DSGVO wird hier nur am Rande eingegangen.

durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden."

Im Datenschutzrecht erfolgt eine **juristische Betrachtungsweise** bei der Auslegung des Begriffs.[198] Eine Sonderregelung enthält lediglich § 67 Abs. 4 S. 2 SGB X für den Bereich des Sozialdatenschutzes: Handelt es sich bei einem Sozialleistungsträger um eine Gebietskörperschaft, sind verantwortliche Stelle die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile des SGB **funktional** erfüllen.[199]

Die Mitgliedstaaten haben im Rahmen der Vorgaben der DSGVO die Möglichkeit, die Verantwortlichkeit im **nationalen Recht** zu präzisieren.[200] Solche allgemeinen Regelungen bestehen im deutschen Recht in Bezug auf die Forschung und die medizinische Datenverarbeitung nicht.

Sowohl natürliche wie auch juristische Personen, Behörden oder Einrichtungen können Verantwortliche sein (Art. 4 Nr. 7 DSGVO). Es sind letztlich immer **natürliche Personen**, auf die eine Datenverarbeitung zurückgeht. Diese können dann als Verantwortliche dem Anwendungsbereich der DSGVO unterfallen, wenn sie im Rahmen einer beruflichen oder wirtschaftlichen Tätigkeit personenbezogene Daten verarbeiten.[201] Nutzt eine natürliche Person, die für eine juristische Person handelt, Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle der juristischen Person, so ist die natürliche Person der für die Verarbeitung Verantwortliche, da sie hierüber eigenständig und unabhängig entschieden hat. Der ursprüngliche für die Verarbeitung Verantwortliche kann jedoch auch eine (gemeinsame) Verantwortung tragen, etwa wenn die neue Verarbeitung aufgrund eines Mangels an angemessenen Sicherheitsmaßnahmen erfolgt.[202]

Handelt ein **Mitarbeiter** im Auftrag und im Namen einer Stelle (seines Arbeitgebers), so ist diese Stelle datenschutzrechtlich verantwortlich. Überschreitet der Mitarbeiter seine stelleninternen Kompetenzen, so ist er selbst als Verantwortlicher anzusehen (vgl. Art. 28 Abs. 10 DSGVO).[203] Der Zugehörigkeit zu einer Stelle tut es keinen Abbruch, dass der **Mitarbeiter oder ein Organisationsteil** eine gesetzlich gesicherte Unabhängigkeit genießt oder eigene Verarbeitungsrechte hat bzw. Pflichten unterworfen ist, z.B. als Arzt, Forschungsleiter oder Betriebsarzt. Auf die Belegenheit der Datenverarbeitungsanlage kommt es auch nicht an; so sind z.B. dienstlich genutzte mobile Rechner (Laptop, Notebook) eines Arbeitnehmers dem Arbeitgeber als Verantwortlichem zuzurechnen.[204]

Dies gilt auch für forschende **Professoren**, soweit sie die forschende Datenverarbeitung als Angehörige ihrer Forschungseinrichtung oder Hochschule durchführen.

198 Jung/Hansch ZD 2019, 146; a.A. noch Weichert in Kilian/Heussen, Computerrechts-Handbuch, 1993, 132 Rn. 39ff.
199 Kritisch dazu Dierks in Dierks/Roßnagel, 77ff.
200 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36.
201 Schwartmann/Mühlenbeck in SJTK, Art. 4 Rn. 108–110; ausgeschlossen ist die Anwendbarkeit bei ausschließlich persönlicher oder familiärer Tätigkeit, Art. 2 Abs. 2 lit. c DSGVO.
202 Artikel 29-Datenschutzgruppe, WP 160 v. 16.02.2010, 20.
203 Jung/Hansch, ZD 2019, 146.
204 LAG Schleswig-Holstein, DuD 2001, 235 = RDV 2001, 107.

Zwar ist für die Feststellung der Verantwortlichkeit die autonome Entscheidungskompetenz von Bedeutung[205], die Professoren auch im Rahmen ihrer „abhängigen Beschäftigung" im Rahmen von Forschungsvorhaben zukommt. Dies ändert aber nichts daran, dass auf sie eine direkte Einflussmöglichkeit auch in diesem Bereich durch die beschäftigende Stelle besteht, wenn sie für diese und nicht für sich tätig sind. Handeln sie als privat Forschende, so sind sie persönlich als Verantwortliche anzusehen. Ausschlaggebend ist, ob sie eigenständig und nicht als Teil der sie beschäftigenden Stelle tätig sind.[206] Relevant ist dabei, wie der Professor gegenüber anderen Stellen und insbesondere gegenüber den Betroffenen auftritt, etwa durch die Verwendung eines persönlichen statt eines dienstlichen Briefkopfs.

Ist ein **Betriebsarzt** (§§ 2–4, 8–10 ASiG) Mitarbeiter des Arbeitgebers (interner Betriebsarzt), so ist er rechtlich Teil des vom Arbeitgeber geführten Betriebs und somit nicht datenschutzrechtlich Verantwortlicher.[207] Verantwortlicher ist der Arbeitgeber. Dieser ist i.d.R. auch im sachenrechtlichen Sinn über die betriebsärztliche Dokumentation verfügungsbefugt. Dass dem Arbeitgeber wegen der ärztlichen Schweigepflicht (§ 8 Abs. 1 S. 3 ASiG) keine Zugriffsrechte auf die Daten zustehen, spielt für die datenschutzrechtliche Bewertung keine Rolle. Der externe Betriebsarzt, egal ob er als Einzelperson handelt oder als betriebsärztlicher Dienst, ist als eigenständige, vom Arbeitgeber rechtlich getrennte Person nicht dem Arbeitgeber zuzuordnen. Der externe Betriebsarzt bzw. der betriebsärztliche Dienst ist also im Sinne des Datenschutzrechts selbst Verantwortlicher. Dies schließt nicht aus, dass er die Räumlichkeiten, Einrichtungen und Geräte des Arbeitgebers in Anspruch nimmt und dass der Arbeitgeber deren Eigentümer ist. Es kommt darauf an, dass der externe Betriebsarzt als natürliche oder juristische Person vertraglich mit dem Arbeitgeber hierüber eine Vereinbarung trifft und so über Mittel und Zwecke der Verarbeitung bestimmt. Möglich ist auch, dass sich die Mittel der ärztlichen Dokumentation im Eigentum des externen Betriebsarztes befinden.[208]

Die Ausführungen zum internen Betriebsarzt sind auf **verbeamtete oder angestellte Ärzte**, die für eine private oder eine öffentliche Stelle tätig sind, übertragbar. Dabei spielt es keine Rolle, ob das Beschäftigungsverhältnis mit einem Krankenhaus[209], einem medizinischen Versorgungszentrum, einer Gemeinschaftspraxis oder in einer ambulanten Arztpraxis besteht. Demgegenüber sind Ärzte in einer Praxisgemeinschaft jeweils selbstständig Verantwortliche, auch wenn sie gemeinsames Praxispersonal beschäftigen.[210]

Im Datenschutzrecht wird unabhängig vom Wissen über die Daten bei der Feststellung der Verantwortlichkeit darauf abgestellt, wer objektiv über die Verarbeitung der Daten bestimmen kann, wer die Entscheidungsgewalt über „Ob" und „Wie" zu **Zweck**

205 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36.
206 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 12; zur Chefarztabrechnung Kühling/Seidel in Kühling/Kingreen, 89.
207 Weichert RDV 2007, 191; zu undifferenziert Washausen in Kingreen/Kühling, 420.
208 Weichert DANA 2020, 5.
209 Nicht jedoch der Klinik-Konzern, Dochow, 641.
210 Kühling/Seidel in Kühling/Kingreen, 89; zur Unterscheidung Deckenbrock in Prütting, § 705 BGB Rn. 4–19, 27–29.

und Mittel der Datenverarbeitung hat.[211] Dabei kommt es nicht darauf an, ob die Stelle über die Daten tatsächlich Besitz und Herrschaft hat.[212]

Bei vernetzten, mobilen oder sonstigen **komplexen Verarbeitungsverfahren** liegt die Verantwortlichkeit zuweilen bei unterschiedlichen Stellen. Sie kann teilweise auch beim Betroffenen bzw. Nutzenden selbst liegen.[213] Entscheidend ist, wer einen wesentlichen Teil des Datenverarbeitungsprozesses tatsächlich beherrscht.[214] Dabei kann es Schwierigkeiten der Zuordnung geben. Bei einem mobilen Datenträger, der vom Betroffenen mitgeführt wird, liegt die Verantwortlichkeit jeweils bei den Stellen, die die Herrschaft über den jeweiligen Verarbeitungsvorgang ausüben. Dies können der Betroffene, ein Plattformanbieter, ein App-Anbieter sowie der Hardware-Hersteller zugleich sein (s.u. Kap. 5.2).

Befinden sich Daten in **Verbunddateien** und sind mehrere Stellen selbstständig zur Veränderung der Datensätze berechtigt, liegt die Verantwortlichkeit kumulativ bei sämtlichen derart berechtigten Stellen. Ist z.B. ein Verbundteilnehmer zu einer Löschung oder Berichtigung verpflichtet, müssen die anderen Teilnehmer dies auch gegen sich gelten lassen. Erfolgt ein (automatisierter) Abruf eines Verbundteilnehmers von einem Datum, für das nur eine andere Stelle verantwortlich ist, liegt hierin eine Offenlegung.[215]

Teilweise wurde die Ansicht vertreten, dass bei arbeitsteiliger Datenverarbeitung eine Verantwortung nur bei **Vorliegen eines Vertragsverhältnisses** besteht und wenn die Stelle positive Kenntnis von den Tatsachen hat, welche der (möglicherweise rechtswidrigen) Verarbeitung der beteiligten anderen Stelle zu Grunde liegen.[216] Diese Ansichten haben sich mit der DSGVO und der neuen Rechtsprechung des EuGHs zur gemeinsamen datenschutzrechtlichen Verantwortlichkeit erledigt.[217]

5.2 Gemeinsame Verantwortlichkeit

Die DSGVO enthält in Art. 26 erstmals eine ausführliche Regelung zur **gemeinsamen Verantwortlichkeit.**

> *„(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der*

211 EDPS 2019, 9f.; Weichert DuD 2009, 10; Jotzo MMR 2009, 233.
212 Dammann in Simitis, § 3 Rn. 225; Weichert, ZD 2014, 605; ders., ZD 2014, 1; a.A. OVG Schleswig, ZD 2014, 643 = DuD 2014, 869 = K&R 2014, 831; VG Schleswig, ZD 2014, 51 mit Anm. Karg; offenhaltend noch die Vorlage beim EuGH durch BVerwG 25.2.2016 – 1 C 28.14, K&R 2016, 437; dazu Marosi, K&R 2016, 389; jetzt ständige Rspr. des EuGH, s.u. Kap. 5.2).
213 Von dem Bussche DB 2018, 1782; Goland K&R 2019, 535; Weichert DANA 2019, 6.
214 Art.-29-Datenschutzgruppe, Arbeitsdokument Datenschutz und RFID-Technologie v. 18.01.2005, WP 105; Kesten, RDV 2008, 100.
215 VGH Kassel, CR 1992, 693.
216 Petri ZD 2015, 103.
217 Ausführlich Monreal ZD 2019, 797ff.

Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.“

Der EU-Gesetzgeber wollte mit der neuen Regelung eine klare Zuordnung der Verantwortungsbereiche schaffen und der komplexen Realität von verschachtelten informationstechnischen Vorgängen gerecht werden. Die Verantwortlichen sollen ihre DSGVO-Pflichten klar und transparent verteilen.[218] Die gemeinsame Verantwortlichkeit ist zwar als rechtliche Konstruktion seit langem bekannt (vgl. § 6 Abs. 2 BDSGaF), spielte aber bisher in der Praxis in Deutschland keine wesentliche Rolle. Dies änderte sich mit **Entscheidungen des Europäischen Gerichtshofes** (EuGH) seit Juni 2018, in denen das oberste europäische Gericht klarstellte, dass eine solche Rechtsbeziehung unter Verantwortlichen öfter besteht, als bisher von den Daten verarbeitenden Stellen, der Datenschutzaufsicht und den Gerichten angenommen wurde.[219]

Gemeinsame Verantwortlichkeit ist gegeben, wenn eine Verarbeitung **selbstständige Entscheidungen verschiedener Stellen voraussetzen**, d.h., wenn eine Verarbeitung ohne die aktive Beteiligung jeder Stelle nicht denkbar ist, also ein kumulatives Zusammenwirken erfolgt.[220] Eine zeitgleiche und gemeinsam abgestimmte Entscheidung über Zwecke und Mittel ist nicht nötig.[221] So kann die gemeinsame Verantwortung dadurch entstehen, dass im Voraus von einem Anbieter festlegte Zwecke und Mittel von einem Nutzer akzeptiert werden, indem er diese für sich in Anspruch nimmt.[222] Beteiligt sein können zwei, aber auch viele Stellen. Für die Feststellung der gemeinsamen Verantwortlichkeit kommt es auf die objektiven tatsächlichen Umstände an, ein schriftlicher Vertrag ist nicht begriffsnotwendig.[223]

Wurde eine Vereinbarung nach Art. 26 DSGVO geschlossen, ohne dass hierfür die tatsächlichen Voraussetzungen vorliegen, so besteht keine gemeinsame Verantwortung. Eine **Bezeichnung als „Vereinbarung“** nach Art. 26 ist allenfalls ein Indiz.[224] Die in Art. 26 Abs. 1 S. 2 DSGVO geforderte Vereinbarung ist Rechtsfolge und Rechtmäßig-

218 Specht-Riemenschneider/Schneider MMR 2019, 504; Albrecht/Jotzo, 61.

219 EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = NZA 2018, 919 = ZD 2018, 357 = NVwZ 2018, 1386 = EuZW 2018, 534 = MMR 2018, 591 = BB 2018, 1480 = DuD 2018, 518; zur Prozessgeschichte Weichert DANA 2019, 4ff.; Nebel RDV 2019, 9ff.; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; kritisch dazu Thüsing/Rombey, NZA 2019, 6ff.; EuGH 29.07.2019 – C-40/17 (Fashion ID), zuvor EU-Generalanwalt Bobek, EWS 2019, 55f.

220 Weichert DANA 2019, 5.

221 Doench/Sommerfeld in Kipker/Voskamp, 113 m.w.N., a.A. Kremer CR 2019, 227; Bertermann in Ehmann/Selmayr, Art. 26 Rn. 10.

222 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.

223 EuGH 10.7.2018 – C-25/17 (Zeugen Jehovas), Rn. 67, NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; Martini in Paal/Pauly, Art. 26 Rn. 18.

224 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.

keitsvoraussetzung, aber nicht begründend für das Vorliegen einer gemeinsamen Verantwortlichkeit.[225]

Für eine gemeinsame Verantwortlichkeit ist es nicht erforderlich, dass jeder der für dieselbe Verarbeitung Verantwortlichen Zugang zu den betreffenden Daten hat.[226] Relevant ist, dass jede Stelle aus Eigeninteresse Einfluss auf die Verarbeitung nimmt und damit an der Festlegung über Zwecke und Mittel dieser Verarbeitung **faktisch mitwirkt**. Dies kann ausdrücklich, aber auch stillschweigend erfolgen.[227] Es ist sogar möglich, dass ein Verantwortlicher gar nicht weiß, mit wem er in gemeinsamer Verantwortung steht.[228] Jeder der Verantwortlichen hat eine rechtliche oder tatsächliche Möglichkeit, Zwecke sowie wesentliche Elemente der Mittel der Verarbeitung zu bestimmen.[229] Es muss keine Gleichrangigkeit der Entscheidungsbefugnis gegeben sein, wohl aber muss eine *„kooperative Determinierung des Zielzustands"* erfolgen.[230] Die Entscheidungen der gemeinsam Verantwortlichen müssen in der Form erfolgen, dass sie sich zum Zeitpunkt der Datenverarbeitung gegenseitig ergänzen, nacheinander erfolgende Entscheidungen in Bezug auf konkrete Verarbeitungsschritte sind nicht gemeinsam.[231] Die Einflussnahme eines Verantwortlichen kann sich auf die Organisation bzw. Koordinierung der Datenverarbeitung beschränken.[232] Selbst ein Abhängigkeitsverhältnis kann die Grundlage für eine gemeinsame Verantwortung sein, wenn in dem organisatorischen Zusammenhang dem untergeordneten Beteiligten eine wesentliche Bestimmungs- und Einflussmöglichkeit über die Verarbeitung verbleibt. Dies kann etwa bei der Tätigkeit eines privat Forschenden (z.B. eines Professors, s.o. Kap. 5.1) und der Einrichtung, bei der dieser beschäftigt ist, gegeben sein. Gleiche Augenhöhe ist nicht nötig.[233]

Eine **Entscheidung** bzgl. der Datenverarbeitung liegt vor, wenn diese ohne den direktiven, bestimmte Modalitäten der Datenverarbeitung regelnden Input einer Stelle potenziell anders ausfallen würde.[234] „Entscheiden" bedeutet, dass eine Frage endgültig geklärt wird.[235] Fehlt es an der Bestimmungsmöglichkeit, so ist i.d.R. eine Auftragsverarbeitung (Art. 28 DSGVO) gegeben. Dass und ob gemeinsam verarbeitete (erhobene) Daten von einer Stelle wieder an einen der Verantwortlichen nach einer Aufbereitung (etwa einer statistischen oder wissenschaftlichen Auswertung) zur alleinigen Nutzung zurückgespielt werden[236], spielt für die Frage der vorangehenden gemeinsamen Verantwortlichkeit keine Rolle.

225 Monreal ZD 2019, 806 Rn. 57; Kremer DB 2019, 1433; Golland K&R 2019, 533, mit weiteren Nachweisen in Fn. 8.
226 EuGH 05.06.2018 – C-210/16 (Facebook Fanpage), Rn. 38.
227 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 68, 80.
228 Monreal 2019, 804 Rn. 42.
229 EDPS 2019, 23.
230 Thüsing/Rombey NZA 2019, 10; Martini in Paal/Pauly, Art. 26 Rn. 21.
231 EDPS (2019), 23; Specht-Riemenschneider/Schneider MMR 2019, 504; Thomale in Auernhammer, Art. 26 Rn. 9; DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.
232 EuGH 10.7.2018 – C-25/17 Rn. 70; Thüsing/Rombey NZA 2019, 10; Specht-Riemenschneider/Schneider MMR 2019, 504.
233 EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), Rn. 70, 75, NJW 2019, 290; Thüsing/Rombey, NZA 2019, 10; von dem Bussche DB 2018, 1782; Golland ZD 2019, 381; Jung/Hansch ZD 2019, 144.
234 EDPS 2019, 7; Specht-Riemenschneider/Schneider MMR 2019, 504; Ingold in Sydow-DSGVO, Art. 26 Rn. 4.
235 Monreal ZD 2019, 802, Rn. 28.
236 So wie dies bei den Facebook-Fanpages mit Facebook Insights der Fall ist.

Welches **Eigeninteresse** von den Verantwortlichen verfolgt wird, ist unbedeutend. Dieses kann ökonomischer oder altruistischer Art sein, es kann in einem Erkenntnisinteresse liegen oder in Bequemlichkeit bzw. dem Interesse an einer unaufwändigen Abwicklung eines Vorgangs. Einzige faktische Voraussetzung ist, dass sich die verfolgten Zwecke, die sich unterscheiden können, praktisch gegenseitig ergänzen.[237] Die Zwecke müssen nicht übereinstimmen.[238] Die Zwecke müssen auch nicht in einem positiven wirtschaftlichen Bedingungszusammenhang stehen.[239]

Jeder der gemeinsam Verantwortlichen muss für sich die Verarbeitung auf eine **Rechtsgrundlage** stützen können, wobei diese Rechtsgrundlagen nicht zwingend identisch sein müssen.[240] So ist es möglich, dass der eine sich auf eine Einwilligung beruft, der andere auf die Wahrnehmung berechtigter Interessen.

Bei einer Forschungsdatenverarbeitung müssen in jedem Fall bei allen Beteiligten reine Forschungs- und Erkenntnisinteressen im Vordergrund stehen, um **rechtlich privilegiert** sein zu können (Kap. 3.4 u. Kap. 8.1). Dies trifft auch für Treuhänder zu, soweit sie für Forschende tätig sind. Diese Forschungsinteressen der Beteiligten können sich im Rahmen einer gemeinsam verantworteten Datenverarbeitung aber unterscheiden.[241]

Bei der Feststellung der gemeinsamen Verantwortlichkeit muss auf den jeweiligen konkreten Verarbeitungsvorgang Bezug genommen werden. Dies kann zur Folge haben, dass ein technisch einheitlicher Prozess in verschiedene **Prozessschritte** bzw. Verarbeitungsphasen aufzuteilen ist.[242] Art. 4 Nr. 2 DSGVO umschreibt solche verschiedenen Abschnitte einer „Vorgangsreihe". Für die Differenzierung bei der Verantwortlichkeit besonders relevant sind die Schritte „Erhebung", „Speicherung", „Auswertung" und „Übermittlung".[243] Sind einzelne Prozessschritte denklogisch, nicht technisch, miteinander verbunden, so besteht insofern eine einheitliche Verantwortungszuordnung. Die Artikel 29-Datenschutzgruppe führt als Beispiel hierfür klinische Arzneimittelstudien an, in denen das Pharmaunternehmen (der Sponsor) die jeweiligen Studienprotokolle und Weisungen hinsichtlich der Datenverarbeitung vorgibt und evtl. kontrolliert, ohne selbst die Daten zu verarbeiten. Die Verarbeitung kann vollständig bei den Studienzentren liegt, die auch die konkrete Umsetzung der Vorgaben festlegen.[244]

Bei der Differenzierung der Verarbeitungsschritte wird zwischen der **Mikro- und der Makroebene** unterschieden: Bei der Mikroebene wird auf den jeweiligen Verarbeitungsschritt i.S.d. Art. 4 Nr. 2 DSGVO abgestellt, bei der Makroebene auf die Sicht der Betroffenen. Relevant für die Feststellung der gemeinsamen Verantwortung ist die Mikroebene, also die Entscheidung über den tatsächlich erfolgenden Verarbeitungsschritt. Um deshalb keine falsche Wahrnehmung der Betroffenen auszulösen, soll für diese über Art. 26 DSGVO Transparenz und Rechtsschutz gesichert werden.[245]

237 Golland ZD 2019, 382.
238 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2; a.A. Kremer CR 2019, 227.
239 Hanloser ZD 2019, 123; dagegen richtig Golland K&R 2019, 535.
240 Petri in SHS, Art. 26 Rn. 1; Monreal ZD 2019, 805 Rn. 50.
241 Weichert DANA 2019, 6
242 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74; DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2f.; Piltz DB 2019, 239.
243 Golland K&R 2019, 534.
244 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36f.
245 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 8.

Eine gemeinsame Verantwortlichkeit bedingt **keine gleichwertige Verantwortlichkeit** der Akteure. Diese können in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein, sodass der Grund der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.[246] Spätestens mit Kenntniserlangung über die Datenverarbeitung der anderen gemeinsam Verantwortlichen können alle einem Verantwortlichen zuzurechnenden Pflichten, auch die Umsetzung der Betroffenenrechte, abverlangt werden.[247] Der unterschiedliche Grad der Verantwortlichkeit hat keinen Einfluss auf die materielle Rechtmäßigkeit des jeweiligen Verarbeitungsschritts. Wohl aber können innerhalb der Gemeinschaft der Verantwortlichen durch eine Vereinbarung Aufgaben konzentriert werden, z.B. in Bezug auf die Umsetzung von Betroffenenrechten. Der Grad der Verantwortlichkeit kann daran gemessen werden, wie groß das Interesse an den Daten und der Einfluss auf die Datenverarbeitung ist. Damit wird dem Grundsatz der Verhältnismäßigkeit entsprochen.[248] Dieser Grad, der nicht von den Beteiligten frei bestimmt werden kann, sondern von den objektiven Umständen abhängt, sollte maßgeblich in der Vereinbarung nach Art. 26 DSGVO abgebildet und aus dieser abgeleitet werden können.[249] Er ist z.B. im Rahmen der Bemessung von Bußgeldern nach Art. 83 DSGVO oder bei Maßnahmen der Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO von Bedeutung.

Für die Frage, welchen der gemeinsamen Verantwortlichen eine **Aufsichtsbehörde** in Anspruch nimmt, kommt es auf den unterschiedlichen Grad der Verantwortung nicht an. Festlegungen in einer Vereinbarung nach Art. 26 DSGVO sind für die Aufsichtsbehörden nicht verbindlich; sie können aber eine Anregung dafür geben, welche Aufsichtsbehörde bei einer Prüfung die Federführung übernimmt. Eine explizite Regelung zur Federführung bei gemeinsamer Verantwortlichkeit enthält die DSGVO nicht. Erfolgt eine gemeinsame Verarbeitung unter der Verantwortlichkeit einer Behörde oder einer privaten Stelle auf der Grundlage von Art. 6 Abs. 1 lit. c oder lit. e DSGVO, so ist die Aufsichtsbehörde in jedem Fall zuständig, ohne dass es insofern eine Federführung gibt (Art. 55 Abs. 2 DSGVO). Die Aufsichtsbehörde kann sich an jeden Verantwortlichen wenden.[250] Eine geforderte Abhilfemaßnahme ist nur dann nicht ermessensfehlerfrei, wenn die konkrete Aufsichtsbehörde durch Inanspruchnahme eines anderen gemeinsam Verantwortlichen effektiver den Anlass des Einschreitens beseitigen könnte.[251]

Von der Verantwortlichkeit nicht mehr mit umfasst werden vor- und nachgelagerte Vorgänge einer **Verarbeitungskette**, für die weder Zwecke noch Mittel gemeinsam festgelegt werden.[252] So besteht z.B. für das Erheben und Übermitteln von Daten über ein Webseiten-Social-Plugin wie den „Gefällt mir"-Button von Facebook eine gemeinsame Verantwortlichkeit von Webseiten- und Plattformbetreiber, nicht mehr aber

246 EuGH 05.06.2018 – C-210/16 (Facebook Fanpage), Rn. 43; Härting/Gössling NJW 2018, 2524f.; Weichert DANA 2019, 5.
247 Weichert ZD 2014, 1; Weichert in Breiter/Wind (Hrsg.), Informationstechnik und ihre Organisationslücken, 2011, 301ff.; Weichert, DANA 2012, 18ff.
248 Petri EuZW 2018, 541; Härting/Gössling NJW 2018, 2524.
249 Schreiber ZD 2019, 58.
250 BVerwG 11.09.2019 – 6 C 15.18 Rn. 25, NJW 2020, 414.
251 BVerwG 11.09.2019 – 6 C 15.18 Rn. 35ff.
252 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74.

für die weitere Verarbeitung durch den Plattformbetreiber.[253] Übermitteln Krankenkassen Daten an eine wissenschaftliche Stelle, um aus den Ergebnissen Erkenntnisse für sich zu erlangen, so haben die Kassen keinen Einfluss auf die Datenauswertung und tragen deshalb hierfür auch keine Verantwortung.[254] Keine gemeinsame Verantwortlichkeit besteht mit einer Stelle, wenn die Voraussetzungen einer Auftragsverarbeitung gemäß Art. 28 DSGVO vorliegen. Auch eine parallele, technisch nebeneinander erfolgende Datenverarbeitung ist nicht automatisch eine gemeinsame, auch wenn diese in gleichartigen Prozessschritten erfolgt.[255]

Unbedeutend für die Feststellung der gemeinsamen Verantwortlichkeit ist es, in wessen **Eigentum oder Herrschaftssphäre** sich die technischen Anlagen zur Datenverarbeitung befinden.[256]

5.3 Verantwortung bei Forschungsprojekten

Die Entscheidungen des EuGH zur gemeinsamen Verantwortlichkeit hatten eine intensive Fachdebatte zur Folge. Schon aus den ersten drei Urteilen war erkennbar, dass dem bisher selten angewendeten Rechtsinstitut der gemeinsamen Verantwortlichkeit künftig eine hohe praktische Relevanz zukommt. Dies gilt nicht nur für die Arbeitsteilung bei einer Internet-Datenverarbeitung, etwa dem Betreiben von Webseiten oder dem Implementieren von Plug-ins, sondern findet auch Anwendung auf sonstige digitale und analoge **arbeitsteilige Verarbeitungsprozesse**. Es ist naheliegend, dass gerade in der oft komplexen und arbeitsteiligen Datenverarbeitung im Bereich der Medizin gemeinsame Verantwortlichkeiten gegeben sind. So liegt bei der elektronischen Patientenakte, bei der ein Krankenversicherer, ein Dienstleister, medizinische Leistungserbringer und evtl. der Betroffene selbst über Zweck und Mittel der Verarbeitung bestimmen, zumindest für einzelne Verarbeitungsschritte gemeinsame Verantwortlichkeiten vor.[257]

Gemeinsame Verantwortlichkeit im Bereich der nach der DSGVO privilegierten Forschung setzt voraus, dass sämtliche Verantwortlichen die **Anforderungen an unabhängige Forschung** erfüllen (s.o. Kap. 3.3).[258] Nicht nötig ist, dass alle Verantwortlichen den gleichen spezifischen Zweck verfolgen und sich auf die gleiche Rechtsgrundlage stützen können. So kann die Tätigkeit eines Treuhänders in Forschungsprojekten einem sehr spezifischen Zweck dienen, während die Durchführenden der Projekte einen umfassenderen Zweck verfolgen. Voraussetzung für die rechtmäßige Datenverarbeitung ist aber bei allen beteiligten Verantwortlichen, dass bei ihnen die Privilegierungsvoraussetzungen vorliegen. Fehlt es bei einem der Verantwortlichen an den Voraussetzungen hierfür, so kann der gesamte gemeinsam verantwortete Verarbeitungsprozess eine Privilegierung für sich nicht mehr in Anspruch nehmen, da dann die Verarbeitung *„gleichzeitig einem anderen Zweck"* dient (Art. 89 Abs. 4 DSGVO).

253 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 77.
254 Doench/Sommerfeld in Kipker/Voskamp, 115.
255 Kremer CR 2019, 228.
256 Specht-Riemenschneider/Schneider MMR 2019, 505; Härting/Gössling NJW 2018, 2525.
257 Kremer CR 2019, 233f.
258 Golland K&R 2019, 534.

Gemeinsame Verantwortlichkeit ist immer gegeben, wenn in einem Forschungsprozess mehrere Stellen zeitgleich **aufeinander abgestimmt agieren**, ohne dass hierbei eine reine Verarbeitungsfolge vorliegt, bei der die nachfolgenden Verantwortlichen selbstständig über die weitere Verarbeitung entscheiden. Die Entscheidungen der Stellen müssen nicht zeitgleich erfolgen. Ein aufeinander abgestimmtes Vorgehen kann z.B. bei Arzneimittelstudien gegeben sein, wenn Sponsor, Studienzentren und Ärzte zusammenwirken.[259] Voraussetzung für die Mitverantwortlichkeit des Sponsors ist, dass dieser auf die Verarbeitungsprozesse einen (mit-)bestimmenden Einfluss nimmt (s.o.). Dies ist nicht der Fall, wenn die Festlegungen für die Datenverarbeitung ausschließlich von dem Prüfer vorgenommen werden.

Stellen **Webseitenbetreiber** ihre Seiten für ein Forschungsprojekt zur Verfügung und werden hierüber personenbezogene Daten erhoben, so sind der Projektbetreiber und die Webseitenbetreiber hinsichtlich des Erhebungsvorgangs gemeinsam Verantwortliche.

Werden in einem **Verbundprojekt** von verschiedenen Stellen medizinische Daten erhoben und dann in einer gemeinsamen Datenbank zusammengeführt, die von jedem der Projektpartner zur Auswertung genutzt wird, so besteht bzgl. der Datenerhebung jeweils eine individuelle Verantwortlichkeit, hinsichtlich der Speicherung und Nutzung jedoch eine gemeinsame Verantwortlichkeit.[260] Bedarf es in einer gemeinsam betriebenen Datenbank mit Mandantentrennung für den Abruf und die Nutzung eines Datensatzes durch eine andere als die erhebende Stelle der Freischaltung durch diese, so besteht bzgl. der Erhebung und der Speicherung eine individuelle Verantwortlichkeit, für die Nutzung dagegen eine gemeinsame Verantwortung.

Bei einem **Krankheits- oder sonstigen medizinisch relevanten Register**[261] kommt es darauf an, ob die Datenanlieferungen, die Datenspeicherungen sowie die Datenabfragen und -nutzungen in getrennten Schritten mit jeweils eigenständigen Entscheidungen erfolgen. In diesem Fall besteht für jedes Verfahrensstadium eine individuelle Verantwortlichkeit. Für die Speicherung und Übermittlung zum Zweck der Nutzung ist die Registerstelle verantwortlich. Dabei spielt es keine Rolle, ob das Register auf einer gesetzlichen oder einer vertraglichen Grundlage betrieben wird. Erfolgt dagegen die Datenanlieferung oder die Datenabfrage ohne individuelle Prüfung, so liegt eine gemeinsame Verantwortung bzgl. der Speicherung und der Übermittlung vor. Besteht für ein Krankheitsregister eine Vertrauens- und eine Registerstelle, so sind diese regelmäßig gemeinsam verantwortlich. Dies ist z.B. – auf gesetzlicher Grundlage – bei den gesetzlichen Krebsregistern[262], beim Implantateregister[263] und beim GKV-Datentransparenzregister mit seinem Forschungsdatenzentrum[264] der Fall.

259 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 4; Bischoff/Wiencke ZD 2019, 8f.

260 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3; zu gemeinsamen Datenpools von Stellen in der Schweiz und der EU Mausbach ZD 2019, 453.

261 Zenker/Krawczak/Semler in TMF, 34ff.

262 § 65 Abs. 1 S. 1Nr. 8 SGB V.

263 Implantateregister-Errichtungsgesetz (EIRD) v. 12.12.2019, BGBl. I S. 2494, dort §§ 7–19 EIRD, dazu Kuketz DANA 2020, 35; Gode/Niemeck in Kipker/Voskamp, 540.

264 §§ 303a ff. SGB V, dazu BVerfG 19.03.2020 – 1 BvQ 1/20, JZ 2020, 1012f.; Weichert DANA 2020, 20; Schäfer in Kipker/Voskamp, 353ff.; Schulz SGb 09.20, 540f.; Platzer NZS 2020, 289ff.; Bretthauer/Spiecker, JZ 2020, 990ff.; Weichert MedR 2020, 539ff.; Kühling/Schildbach NZS 2020, 41ff.; Kühling, 49ff.; Graf von Kielmansegg in TMF, 111; Schrahe/Städter DuD 2020, 714ff.; Dierks 2020, 11ff.

Keine gemeinsame Verantwortlichkeit bei einem Verbundprojekt oder einem Register besteht, wenn die Anlieferung in der Weise erfolgt, dass für den Übermittler **keine weitere Bestimmungsmöglichkeit** über die angelieferten Daten besteht. Entscheidet eine Registerstelle oder ein Verbundpartner allein über die weitere Verarbeitung, so liegt eine aufeinander folgende getrennte Verantwortlichkeit vor.

Ein Anwendungsfall für eine alleinige Verantwortlichkeit ist es, wenn an eine zentrale Stelle oder Plattform **Sozialdaten** für Forschungszwecke angeliefert werden, wenn diese zentrale Stelle nicht selbst ein Sozialleistungsträger ist. Die spezifischen Regelungen des SGB zur Zweckbindung (Sozialgeheimnis) und zur (funktionalen) Verantwortlichkeit (s.o. Kap. 5.1) erlauben es nicht, dass Sozialleistungsträger und andere gemeinsam datenschutzrechtlich verantwortlich sind. Auch keine gemeinsame Verantwortlichkeit besteht bei dem Datentransparenzregister nach §§ 303a ff. SGB V zwischen den Daten anliefernden Krankenkassen und den Stellen des Transparenzregisters. Zwischen diesen – der Vertrauensstelle nach § 303c SGB V und dem Forschungsdatenzentrum[265] nach § 303d SGB V – bestehen in Bezug auf einzelne Verarbeitungsschritte der Datenanlieferung und der Datenspeicherung gemeinsame Verantwortlichkeiten auf gesetzlicher Grundlage. Diese gesetzliche Grundlage ersetzt, soweit sie ausreichende Regelungen enthält, die in Art. 26 DSGVO genannte Vereinbarung.

5.4 Anforderungen bei gemeinsamer Verantwortlichkeit

Art. 26 DSGVO verlangt eine **Vereinbarung**, ein „Joint Controller Agreement". Für die gemeinsame Festlegung von Zweck und Mitteln der Datenverarbeitung ist keine gemeinsame Entscheidungsfindung der Akteure erforderlich, doch zwingt sie diese dazu, sich hierüber zumindest informell zu verständigen.[266] Die Vereinbarung kann von einer Seite vorgegeben werden, der dann die anderen Verantwortlichen beitreten.[267] Nicht möglich ist es, allein mit der formalen Vereinbarung eine faktisch gegebene gemeinsame Verantwortlichkeit entgegen den objektiven Gegebenheiten auf einen der Verantwortlichen zu übertragen.[268] Wohl ist es aber möglich, hinsichtlich der tatsächlichen Wahrnehmung der Verantwortung zwischen den Beteiligten eine Arbeitsteilung auszuhandeln.

Bzgl. der **Form der Vereinbarung** gibt es keine Vorgaben. Da die Inhalte der Vereinbarung festgelegt und für die Betroffenen transparent sein müssen, ist eine konkludente – lediglich durch schlüssiges Verhalten begründete – Vereinbarung praktisch ausgeschlossen.[269] Möglich ist, dass die Vereinbarung mit anderen Absprachen verbunden wird, sofern hierdurch die Qualität der Information nicht leidet.[270]

Eine Vereinbarung ist nicht nötig, wenn und soweit die Aufgabenverteilung durch **verbindliches Recht der Union oder eines Mitgliedsstaates** festgelegt wird (Art. 26 Abs. 1 S. 2 DSGVO: begrenzte Öffnungsklausel). Derartige Festlegungen können bei

265 Zuvor Datenaufbereitungsstelle.
266 Hanloser BB 34.2019, I; Härting/Gössling NJW 2018, 2525.
267 Von dem Bussche DB 2018, 1782.
268 Im Sinne eines „Single-Controllership-Agreements", Golland ZD 2019, 381.
269 Weichert DANA 2019, 6; a.A. Schantz in Schantz/Wolff, Rn. 371.
270 Petri in SHS, Art. 26 Rn. 21.

Verarbeitungen im öffentlichen Interesse eine Rolle spielen.[271] So ist es für die nationalen Gesetzgeber möglich, für spezifische Formen der Verarbeitung von (medizinischen) Daten für Forschungszwecke Festlegungen nach Art. 26 DSGVO z.B. in Bezug auf Krankheitsregister vorzunehmen. Soweit solche normativen Festlegungen fehlen, sind sie durch eine Vereinbarung zu ergänzen.

Durch die jeweilige Vereinbarung kann das durch die DSGVO oder durch sonstiges staatlich **vorgegebenes Recht nicht modifiziert** werden. Die Rechte und Pflichten gemäß der DSGVO sowie sonstiger Datenschutzgesetze gelten für jeden der Verantwortlichen gleichermaßen.

Ein **wesentlicher Inhalt der Vereinbarung** muss sein, dass sich die gemeinsam Verantwortlichen verständigen, „wer von ihnen welche Verpflichtung" gemäß der DSGVO erfüllt. Gegenstände der Arbeitsteilung können sein: das Einholen einer Einwilligung (Art. 7 DSGVO); die Information über die Verarbeitung (Art. 12–14 DSGVO), die Bearbeitung von Betroffenenanträgen, etwa auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Verarbeitungseinschränkung (Art. 18 DSGVO)[272]. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen der Beteiligten widerspiegeln (Art. 26 Abs. 2 S. 1 DSGVO).[273]

Unerlässlich ist insofern die spezifische Erfassung der **tatsächlichen logistischen Infrastruktur**, also der Anwendungsprogramme, ihrer Schnittstellen und der ihnen zu Grunde liegenden physischen Infrastruktur.[274] Nicht nur die interne Aufgabenteilung sollte die Vereinbarung enthalten, sondern auch Aussagen über die interne Haftung, wenn einer der Verantwortlichen in Anspruch genommen wird.[275]

Der wesentliche Inhalt muss den **Betroffenen zur Verfügung** gestellt werden (Art. 26 Abs. 2 S. 2 DSGVO). Zur-Verfügung-Stellen bedeutet nicht, dass den Betroffenen der Text der Vereinbarung bzw. deren wesentlicher Inhalt[276] direkt mitgeteilt wird; es genügt, dass die Betroffenen vor Beginn der Verarbeitung einen Hinweis erhalten, wo oder wie sie den Text einsehen können.[277] Die Art und Weise der Information ist nicht festgelegt. Es ist möglich, dass mehrere Verantwortliche ihre Informationspflicht über eine einheitliche, in der Vereinbarung zu vereinbarende Stelle erfüllen.[278] Die Information kann z.B. über eine Webseite erfolgen, auf welche die Betroffenen zugreifen können.[279] Dies bietet sich bei großen, einrichtungsübergreifenden Projekten sowie bei Studien ohne direkten Betroffenenkontakt an. Möglich ist auch, dass den Probanden, z.B. im Rahmen einer Klinik- oder Arzneimittelstudie, ein Hinweisblatt oder eine Mitteilung auf einem umfassenderen Informationsblatt zur Verfügung gestellt wird. Eine mündliche Information genügt nicht.[280]

271 Petri in SHS, Art. 26 Rn. 22.
272 EDPS 2019, 27–29; Petri in SHS, Art. 26 Rn. 17.
273 Petri in SHS, Art. 26 Rn. 14.
274 Petri in SHS, Art. 26 Rn. 16.
275 Härting/Gössling NJW 2018, 2526; Jung/Hansch ZD 2019, 146; Grages CR 2020, 232ff.
276 Mindestens die Aufteilung der Pflichten und die Informationen nach Art. 13, 14 DSGVO, vgl. Martini in Paal/Pauly, Art. 26 Rn. 32, Kremer in SJTK, Art. 26 Rn. 42; Hartung in Kühling/Buchner, Art. 26 Rn. 26.
277 Däubler in DWWS, Art. 26 Rn. 12; a.A. Piltz in Gola, Art. 26 Rn. 21, der eine spätere Bereitstellung und dies erst auf Antrag des Betroffenen für ausreichend ansieht.
278 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 13.
279 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 4; Martini in Paal/Pauly, Art. 26 Rn. 34.
280 Hornung in SHS, Art. 26 Rn. 27.

Bei einer **wesentlichen Inhaltsänderung** einer Vereinbarung nach Art. 26 DSGVO, etwa hinsichtlich der Verantwortlichen oder einer Änderung der Zuständigkeit unter den Verantwortlichen, muss auch diese Information zur Verfügung gestellt werden. Bei einem Verweis auf einen Webauftritt oder eine sonstige Informationsquelle genügt eine dortige Änderung der jeweiligen Informationen. Einen besonderen Hinweis gegenüber den Betroffenen auf den Umstand der Änderung fordert Art. 26 Abs. 2 S. 2 DSGVO nicht.

Um die gemeinsame Verantwortlichkeit wahrnehmen zu können, müssen sämtliche Verantwortlichen eine im Wesentlichen klare Vorstellung davon haben, wie die gemeinsam verarbeiteten Daten erlangt werden und wie diese weiterverarbeitet werden. Die gemeinsam Verantwortlichen müssen, um die **Rechtmäßigkeit** der gemeinsam verantworteten Verarbeitung beurteilen zu können, sich deshalb über die hierfür relevanten Informationen austauschen.[281]

Verarbeitet einer der gemeinsam Verantwortlichen gemeinsam erhobene Daten weiter, so müssen die anderen Verantwortlichen eine Vorstellung davon entwickeln können, ob die weitere Verarbeitung rechtmäßig ist. Dies setzt voraus, dass über die Weiterarbeitung soweit Transparenz hergestellt wird, dass eine Beurteilung der **mitverantworteten Datenübermittlung** bzw. Offenlegung an den (mit verantwortlichen) Empfänger möglich wird. Erweist sich (im Nachhinein) die Beurteilung als falsch, so besteht eine verstärkte (weitere) Verantwortlichkeit für weitere Übermittlungen. In einem gemeinsam verantworteten Register muss z.B. erkennbar sein, für welche Zwecke die abgerufenen Daten verwendet werden dürfen. Ist einer der gemeinsam Verantwortlichen z.B. für die Speicherung und Verwaltung der sog. Metadaten[282] zuständig, so ist klarzustellen, für welche Zwecke dieser Verantwortliche diese weiternutzen darf.

Werden Daten aus unterschiedlichen Quellen in gemeinsamer Verantwortung zusammengeführt, so tragen sämtliche Nutzer der gemeinsamen Datenbank auch für die **Rechtmäßigkeit der Datenanlieferung und -speicherung** die gemeinsame Verantwortung. Um diese Rechtmäßigkeit zu gewährleisten, ist es sinnvoll, die Anforderungen an die Anlieferung mit den Übermittlern festzulegen. Dies kann in der Vereinbarung nach Art. 26 DSGVO erfolgen, die den Übermittlern bereitgestellt wird, oder in separaten Absprachen mit den Übermittlern.

Hinsichtlich der datenschutzrechtlich relevanten Vertragsinhalte nach Art. 26 DSGVO kann auf Art. 28 DSGVO zur **Auftragsverarbeitung** und dort insbesondere auf Abs. 3 zurückgegriffen werden. Die darin genannten Mindestinhalte ermöglichen es jedem der Verantwortlichen, eine überschlägige Rechtmäßigkeitsprüfung durchzuführen.[283] Bei den notwendigen Regelungspunkten kann insofern eine Anleihe gemacht werden, wobei aber die anders gelagerte Beziehung zwischen den Vertragspartnern berücksichtigt werden muss: Während beim Auftrag zumindest formal ein Über-/Unterordnungsverhältnis besteht, besteht hier – auch zumindest formal – eine gleichrangige Beziehung. Bei der Auftragsdatenverarbeitung hat der Auftraggeber die vorrangige materiell-rechtliche Verantwortung; bei der gemeinsamen Verantwortung

281 Datenschutzkonferenz (DSK) 05.09.2018, Beschluss zu Facebook-Fanpages; Weichert DANA 2019, 7.

282 Also der Nutzungs- bzw. Protokolldaten.

283 Specht-Riemenschneider/Schneider MMR 2019, 505, Hartung in Kühling/Buchner, Art. 26 Rn. 25; Weichert DANA 2019, 7; Schreiber ZD 2019, 57.

liegt diese uneingeschränkt bei jedem Verantwortlichen. Entsprechendes gilt für die Voreinstellungen (Privacy by Default) gemäß Art. 25 Abs. 2 DSGVO.

Hinsichtlich der sonstigen **technisch-organisatorischen Vorkehrungen** nach Art. 32 DSGVO, die bei der Auftragsverarbeitung voll dem Auftragsverarbeiter zugeordnet werden können, lassen sich auch bei einer gemeinsamen Verantwortlichkeit bei einzelnen Stellen Abstriche machen, wenn jeweils Verantwortliche arbeitsteilig die „Verantwortung" übernehmen. Anders als beim materiellen Recht und beim Privacy by Default gibt es hier nicht nur richtige oder falsche Lösungen. Vielmehr kann ein ganzer Instrumentenkasten zum Einsatz kommen, bei dem es auch kurzfristig Änderungen bzw. Änderungsnotwendigkeiten gibt, die nicht in jedem Fall den anderen Verantwortlichen kommuniziert werden können und müssen. Aus Sicherheitsgründen und zur Wahrung von Betriebs- und Geschäftsgeheimnissen können die jeweiligen Verantwortlichen u.U. Vertraulichkeit für sich beanspruchen. Entsprechendes kann gelten, wenn einer der Verantwortlichen für seine Verarbeitung Auftragsverarbeiter in Anspruch nimmt. Die Kategorien der Auftragnehmer sind aber zumindest zu benennen (Art. 15 Abs. 1 lit. c DSGVO). Bestehen bzgl. technisch-organisatorischer Maßnahmen oder einer Auftragsverarbeitung konkret begründete Zweifel an der Rechtmäßigkeit, so besteht auch insofern ein Informationsbedarf und Auskunftsanspruch der anderen Verantwortlichen.

Folgende Aspekte sind **für die Vereinbarung wesentlich**:

- die beteiligten Stellen mit Angaben zu Sitz/Niederlassung sowie Funktion bzw. Beziehung zu den Betroffenen,
- die verfolgten Zwecke jedes einzelnen Verantwortlichen in Bezug auf jede Datenart, also z.B. Namen, Identifizierungsdaten, IP-Adressen, Standortdaten, Kommunikationsdaten zu Zeit, Dienst, Partner, (Kommunikations-)Inhaltsdaten, insbesondere Diagnose- und Behandlungsdaten, evtl. differenziert nach Vertraulichkeitsstellung der Nutzenden,
- umfassende und abschließende Darstellung der gesamten gemeinsam verantworteten Datenverarbeitung (beispielhafte Beschreibung genügt nicht),
- Differenzierung nach Datenverarbeitung auf Einwilligungsbasis, auf Vertragsbasis, auf Abwägungsbasis bei (Plattform-)Mitgliedern, auf Abwägungsbasis bei Drittnutzenden,
- Differenzierung nach Sensitivität (Art. 9 DSGVO) sowie bei Kinderdatenverarbeitung (vgl. Art. 8 DSGVO),
- Übermittlung an dritte Stellen,
- insbesondere Drittlandtransfers (Art. 15 Abs. 1 lit. c DSGVO),
- Anonymisierung und Löschfristen,

involvierte Logik beim Profiling oder bei sonstigen automatisierten Entscheidungsverfahren (Art. 15 Abs. 1 lit. h, Art. 22 DSGVO).[284]

Hinsichtlich der Wahrnehmung der **Betroffenenrechte** können Absprachen zwischen den gemeinsam Verantwortlichen vorgenommen werden. Dazu gehört insbesondere die Information der Betroffenen nach den Art. 13, 14 DSGVO. Bzgl. der Bearbeitung von Ansprüchen aus den Art. 15–18, 21 DSGVO können zentrale Anlaufstel-

284 Ähnlich Specht-Riemenschneider/Schneider MMR 2019, 505f.

len etabliert werden (Art. 26 Abs. 1 S. 3 DSGVO). Für die Umsetzung von Betroffenenrechten ist eine gegenseitige Mitteilung vorzusehen (Art. 19 DSGVO).[285]

Auch bezüglich **sonstiger Verpflichtungen** (z.B. Führen des Verarbeitungsverzeichnisses, Durchführung der Datenschutz-Folgenabschätzung, Benennung eines Datenschutzbeauftragten, Protokollierungen) kann eine Arbeitsteilung verabredet werden. Eine Ausnahme stellt die Meldung bzw. die Benachrichtigung im Fall einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde bzw. an die Betroffenen (sog. „Breach Notification", Art. 33, 34 DSGVO) dar, da wegen der Kurzfristigkeit der Reaktionspflicht, die an die Kenntniserlangung jedes einzelnen Verantwortlichen anknüpft, kein Verweis auf einen anderen Verantwortlichen möglich ist.

Eine gemeinsame Verantwortlichkeit begründet denklogisch auch jenseits der Verpflichtung zum Abschluss einer Vereinbarung **Kooperationspflichten**, soweit die gemeinsame Verarbeitung tangiert ist.[286] Dies kann immer dann relevant werden, wenn Fragen der Rechtmäßigkeit einer Verarbeitung, die von der gemeinsamen Verantwortlichkeit erfasst wird, im Raum stehen.

5.5 Rechtliche Formen der gemeinsamen Verantwortung

Die rechtliche **Ausgestaltung des Binnenverhältnisses** zwischen den gemeinsam Verantwortlichen ist von der DSGVO nicht vorgegeben.[287] Dabei sind verschiedene Vertrags- und Gesellschaftsformen möglich, auch eine Gesellschaft bürgerlichen Rechts. Selbst die Organisationsform eines Vereins ist denkbar. Bei gesellschaftsrechtlichen Lösungen ist zu klären, ob die Gesellschaft selbst datenschutzrechtlich verantwortlich ist oder ob dies für die Gesellschafter gilt. Ist die Gesellschaft oder ein sonstiger rechtlicher Zusammenschluss selbst verantwortlich, dann ist zu prüfen, ob eine alleinige Verantwortlichkeit vorliegt, sodass es für eine Datenoffenlegung gegenüber den Gesellschaftern/Mitgliedern einer eigenständigen Rechtsgrundlage bedarf oder ob eine gemeinsame Verantwortlichkeit mit den Gesellschaftern besteht.

Für die Vereinbarung nach Art. 26 DSGVO bestehen keine Formvorgaben. Daher ist es möglich, eine separate Vereinbarung zu treffen, aber auch deren Inhalt in einen anderen (Gesellschafts-)Vertrag oder in eine andere Vereinbarung, etwa eine Vereins- oder Genossenschaftssatzung zu **integrieren**.

Erfolgt keine förmliche Festlegung in der Vereinbarung nach Art. 26 DSGVO, so stellt sich die Frage, ob dadurch automatisch eine **Gesellschaft bürgerlichen Rechts** (GbR) entsteht, die in § 705 BGB geregelt ist:

> *„Durch den Gesellschaftsvertrag verpflichten sich die Gesellschafter gegenseitig, die Erreichung eines gemeinsamen Zweckes in der durch den Vertrag bestimmten Weise zu fördern, insbesondere die vereinbarten Beiträge zu leisten."*

285 EDPS 2019, 30; vgl. Hartung in Kühling/Buchner, Art. 26 Rn. 25; zum oben Stehenden vgl. Weichert DANA 2019, 7f.; Schreiber ZD 2019, 57.
286 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 1 Rn. 61.
287 DWWS-Däubler, Art. 26 Rn. 9; Petri in SHS, Art. 26 Rn. 18.

Wie oben (Kap. 5.2) ausgeführt, knüpft die Annahme einer gemeinsamen Verantwortung an objektive tatsächliche Verhältnisse an, nicht an einen gemeinsamen Willensakt. Voraussetzung ist nicht ein gemeinsamer Zweck i.S.d. Datenschutzrechts, sondern eine gemeinsame Verarbeitung, bei der jeder der Verantwortlichen einen eigenen Zweck verfolgen kann, die sich aber faktisch gegenseitig ergänzen. Die sich hieraus ergebenden Förderpflichten ergeben sich aus Art. 26 DSGVO, nicht aus einem Vertrag i.S.v. § 705 BGB. Eine gemeinsame datenschutzrechtliche Verantwortlichkeit kann also auf einer GbR beruhen; diese muss aber **nicht zwangsläufig** gegeben sein.[288]

Liegt keine andere Rechtsgrundlage für die Kooperation der gemeinsam Verantwortlichen als die Vereinbarung nach Art. 26 DSGVO vor und wird von den gemeinsam Verantwortlichen ein **gemeinsamer Zweck** verfolgt, so wird mit der Vereinbarung eine GbR begründet. Dies wird im Forschungsbereich oft der Fall sein, etwa wenn ein unabhängiger Treuhänder eingebunden wird oder wenn eine Vielzahl von Forschungseinrichtungen eine gemeinsame Datenbank betreibt. Ein gemeinsamer übergeordneter Zweck besteht darin, ein gemeinsames Forschungsprojekt durchzuführen, auch wenn die Beteiligten hierbei unterschiedliche Beiträge leisten. Ein gemeinsamer Zweck kann auch im gemeinsamen Betrieb einer Forschungsdatenbank liegen, auf welche die Beteiligten für eigene separate Forschungsprojekte zugreifen können. Bei der Annahme einer GbR handelt es sich im Fall einer gemeinsamen Verantwortlichkeit immer um eine Außengesellschaft, da sämtliche Verantwortlichen gegenüber Betroffenen eine Rechtsbeziehung haben. Die Annahme einer GbR nach § 705 BGB hat zur Folge, dass die §§ 706ff. BGB anwendbar sind.

Erfolgt die Entscheidung über Zwecke und Mittel einheitlich durch die GbR und nicht durch einzelne Gesellschafter, so ist die **GbR Verantwortliche als Gesamtgesellschaft**; es liegt dann insoweit keine gemeinsame Verantwortlichkeit der Gesellschafter vor.

5.6 Rechtsfolgen bei gemeinsamer Verantwortlichkeit

Die gemeinsame Verantwortlichkeit für konkrete Verarbeitungsprozesse hat zur Folge, dass sämtlichen Verantwortlichen **sämtliche datenschutzrechtlichen Verpflichtungen**, wie sie insbesondere in der DSGVO festgehalten sind, obliegen. Dies gilt u.a. für die Einhaltung der Grundprinzipien des Art. 5 Abs. 1 DSGVO, also insbesondere für die Rechtmäßigkeit der Verarbeitung (lit. a). Jeden trifft die Dokumentationspflicht (Art. 5 Abs. 2 DSGVO). Jedem Verantwortlichen obliegt weiterhin die Wahrung der Betroffenenrechte (Art. 12ff. DSGVO), insbesondere, dass die erforderlichen Informationen erteilt werden (Art. 12–14 DSGVO), die Beachtung der formellen Anforderungen, insbes. das Erstellen des Verarbeitungsverzeichnisses und die Durchführung einer Folgeabschätzung (Art. 30, 35 DSGVO). Jeder der Verantwortlichen muss dafür sorgen, dass Privacy by Default sowie im Grundsatz Privacy by Design umgesetzt werden einschließlich der erforderlichen technisch-organisatorischen Sicherungsmaßnahmen (Art. 25, 32 DSGVO). Um diesen Pflichten entsprechen zu können, sind in die Vereinbarung gem. Art. 26 DSGVO Regelungen aufzunehmen,

288 Kremer CR 2019, 232; Hartung in Kühling/Buchner, Art. 26 Rn. 30.

die hierzu Aussagen enthalten; Verabredungen zur Arbeitsteilung sind möglich (s.o. Kap. 5.4).

Kann ein Verantwortlicher seinen datenschutzrechtlichen Pflichten ohne die Unterstützung oder Beteiligen eines anderen Verantwortlichen nicht nachkommen, so ergibt sich allein schon aus dem Umstand des objektiven Vorliegens einer gemeinsamen Verantwortlichkeit eine **gegenseitige Kooperationspflicht**, soweit die Kooperationsmaßnahme für die Umsetzung der Datenschutzpflichten nötig ist. Diese Kooperationspflicht ergibt sich gemäß Art. 26 DSGVO als eine direkte Rechtsfolge aus dem objektiven Vorliegen einer gemeinsamen Verantwortlichkeit.[289] Ein Beispiel hierfür ist die Tätigkeit einer treuhänderischen Vertrauensstelle, die für die Pseudonymisierung und die Verwaltung der Pseudonyme in einer Forschungsdatenbank verantwortlich ist. Wendet sich ein Betroffener an eine mitverantwortliche Forschungseinrichtung, die Daten pseudonymisiert verarbeitet, so ist die Vertrauensstelle verpflichtet, die für die Zuordnung des Pseudonyms notwendige Unterstützung zu leisten.[290] Die gemeinsam Verantwortlichen haben aus Art. 26 DSGVO gegeneinander nicht nur einen Anspruch auf Abschluss einer Vereinbarung, sondern auch auf Auskunft oder im Fall einer Verweigerung einen Schadenersatzanspruch (Art. 82 DSGVO).[291]

Teilweise wird erörtert, ob es für den **Datenaustausch zwischen den gemeinsam Verantwortlichen** einer eigenständigen Rechtsgrundlage bedarf oder ob insofern, vergleichbar mit der Auftragsverarbeitung, eine „Privilegierung" (s.u. Kap. 5.7) besteht, die insbesondere auch sensitive Daten, etwa Gesundheitsdaten, mit einschließt.[292] Diese Frage ist jedoch rein akademischer Natur, da eine gemeinsame Verantwortlichkeit nur in Bezug auf einheitliche Verarbeitungsprozesse bestehen kann, für die jeder der Verantwortlichen einer Rechtsgrundlage bedarf.[293] Es kommt also nicht zu einer Übermittlung.[294] Es erfolgt allenfalls eine Offenlegung i.S.v. Art. 4 Nr. 2 DSGVO.[295] Wohl kann, da ein Verantwortlicher keinen Zugriff auf den zu verantwortenden Datenprozess haben muss, ein Zugriff eingeräumt werden. Hierfür muss eine rechtliche Grundlage bestehen; anderenfalls ist die gemeinsame Verarbeitung unzulässig.[296]

Durch die Vereinbarung von Zuständigkeiten für die Wahrnehmung spezifischer Datenschutzaufgaben können sich die intern nicht für zuständig deklarierten Verantwortlichen extern gegenüber den Betroffenen, der Datenschutzaufsicht oder den Gerichten nicht entlasten.[297] Vielmehr besteht für jeden der gemeinsam Verantwortlichen **im Außenverhältnis** eine individuelle Verpflichtung.[298]

289 Weichert, DANA 2019, 8.
290 Graf von Kielmansegg in TMF, 113.
291 Specht-Riemenschneider/Schneider, MMR 2019, 506f.
292 Golland ZD 2019, 382; ausführlich Kremer CR 2019, 230f.
293 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 11.
294 A.A. Martini in Paal/Pauly, Art. 26 Rn. 3a, der annimmt, die Datenweitergabe sei privilegiert.
295 Kremer CR 2019, 231.
296 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 1.
297 DWWS-Däubler, Art. 26 Rn. 14; Petri in SHS, Art. 26 Rn. 24.
298 Schreiber ZD 2019, 58; zur Gerichtszuständigkeit im Außenverhältnis Specht-Riemenschneider/Schneider MMR 2019, 508.

Dies gilt auch für Schadenersatzansprüche aus Art. 82 DSGVO, für die Art. 82 Abs. 4 DSGVO eine gesamtschuldnerische **Haftung** festlegt.[299] Nach Art. 82 Abs. 5 DSGVO kann der haftbar gemachte Verantwortliche die anderen Verantwortlichen in Regress nehmen. Fehlt es an einer Vereinbarung nach Art. 26 DSVGO oder an wesentlichen Inhalten, so liegt hierin in Verbindung mit den jeweiligen Regelungspflichten gemäß DSGVO ein Rechtsverstoß gemäß Art. 5 Abs. 2 DSGVO.[300] Die Aufsichtsbehörden haben die in Art. 58 DSGVO genannten Untersuchungs- und Abhilfebefugnisse.[301] Der Verstoß gegen Art. 26 DSGVO ist zudem gemäß Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt.[302]

Die gemeinsame Verantwortlichkeit ist gemäß Art. 30 Abs. 1 S. 2 lit. d DSGVO in das **Verarbeitungsverzeichnis** aufzunehmen. Verantwortlich sind sämtliche Empfänger gemäß Art. 4 Nr. 9 DSGVO, abgesehen von Auftragsverarbeitern nach Art. 28 DSGVO, gegenüber denen die personenbezogenen Daten offengelegt werden. Auch Verantwortliche, die keinen direkten Zugang zu den Daten haben, sind dann gemeinsam verantwortlich und im Verarbeitungsverzeichnis zu dokumentieren. Dies ergibt sich aus dem Sinn und dem Zweck des Art. 30 DSGVO ungeachtet der Verwendung des Singulars in der Regelung.[303]

Ist eine gemeinsame Verantwortlichkeit tatsächlich begründet und **weigert sich einer der Verantwortlichen**, eine angemessene Vereinbarung zu schließen, so liegt wegen der gemeinsamen Festlegung von Mitteln und Zwecken einer Dritte betreffenden Datenverarbeitung eine vertragsähnliche faktische Beziehung vor, die ein gesetzliches Schuldverhältnis und einen Anspruch gegen die weigernde Stelle auf Abschluss der Vereinbarung nach Art. 26 DSGVO begründet.[304] Zur Schaffung der faktischen Grundlagen für den Abschluss der Vereinbarung sowie zwecks Wahrnehmung der Pflichten als (gemeinsame) Verantwortliche können von der sich weigernden Stelle die nötigen o.g. Informationen gerichtlich eingefordert werden. Zumindest eine entsprechende Klage ist in Bezug auf Facebook inzwischen anhängig.[305] Der Abschluss der Vereinbarung bzw. die Bereitstellung der dafür nötigen Informationen sind nicht vertretbare Handlungen der sich weigernden Stelle, die mit Zwangsgeld nach § 888 Abs. 1 ZPO erzwungen werden können.

Die gerichtliche Durchsetzung dieser Ansprüche erfolgt gemäß Art. 79 Abs. 2 S. 1 DSGVO vor dem Gericht des Mitgliedsstaates, in dem der sich weigernde Verantwortliche eine Niederlassung hat.[306] Diese Regelung gilt nicht nur für Betroffene i.S.v. Art. 79 Abs. 1 DSGVO, sondern auch für verantwortliche Stellen untereinander. Offenkundig ist dies, wenn, was bei Social Media regelmäßig der Fall ist, der Betroffene zugleich Verantwortlicher in Bezug auf die Verarbeitung von Daten über Dritte ist (s.o. Kap. 5.1). Dies gilt aber auch in den sonstigen Fällen. Gemäß ErwGr 147 DSGVO zielt die DSGVO darauf ab, vorrangige **einheitliche Gerichtsstände** festzulegen. Für

299 Specht-Riemenschneider/Schneider MMR 2019, 507; Hanloser BB 34.2019, I.
300 Petri in SHS, Art. 26 Rn. 30.
301 Petri in SHS, Art. 26 Rn. 31; Schreiber ZD 2019, 58ff.
302 Petri in SHS, Art. 26 Rn. 32; Schreiber ZD 2019, 60.
303 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 14; Kremer CR 2019, 226, 232.
304 Specht-Riemenschneider/Schneider MMR 2019, 506f.
305 BT-Fraktion Bündnis 90/Die Grünen, PM 02.10.2018, Klage gegen Facebook, https://www.gruene-bundestag.de/netzpolitik/klage-gegen-facebook.html.
306 Bergt in Kühling/Buchner (Fn. 26) Art. 79 Rn. 16; Specht-Riemenschneider/Schneider MMR 2019, 508.

den Innenausgleich zwischen zwei Verantwortlichen sollen die Gerichte zuständig sein, die auch für die Klage eines Betroffenen wegen des Rückgriffs auf einen Verantwortlichen zuständig sind.[307]

5.7 Auftragsverarbeiter

Der „Auftragsverarbeiter" wird in Art. 4 Nr. 8 DSGVO definiert. Danach ist

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

Für die Auftragsverarbeitung genügt es, dass eine Stelle personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet. Er übernimmt eine spezifische Aufgabe oder mehrere Aufgaben im Interesse des Verantwortlichen.[308] An die Art oder die Form des Auftrags werden nur geringe Anforderungen gestellt, wohl aber an den Inhalt. Die rechtliche Zulässigkeit ist in Art. 28 DSGVO geregelt:

> *„(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.*
>
> *(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.*
>
> *(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter*
>
> *a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;*

307 Vgl. EuGH 15.06.2017 – C-249/16 (Kareda), Rn. 31; NJW 2018, 845; ZIP 2017, 1734.
308 EDPS 2019, 16f.

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vor-

liegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher."

Liegen die in **Art. 28 DSGVO genannten Voraussetzungen** vor, so ist der Auftragsverarbeiter nicht Dritter i.S.v. Art. 4 Nr. 10 DSGVO und die Verarbeitung durch ihn ist datenschutzrechtlich zulässig. Fehlt es an den Voraussetzungen des Art. 28 DSGVO, so gilt der Auftragsverarbeiter als Verantwortlicher (Art. 28 Abs. 10). Fehlt es für die Datenweitergabe an diesen Verantwortlichen, der im Auftrag einer anderen Stelle Daten verarbeitet, ohne dass die Anforderungen des Art. 28 DSGVO erfüllt sind, an einer sonstigen Rechtsgrundlage, so ist diese Datenweitergabe bzw. Übermittlung unzulässig.

Während das frühere deutsche Recht davon ausging, dass der Auftragsverarbeiter (Auftragnehmer) dem Verantwortlichen (Auftraggeber) zuzurechnen ist mit der Folge, dass die Datenweitergabe zwischen dem Auftraggeber und dem Auftragnehmer keine Übermittlung darstellt, wird bei der DSGVO nun weitgehend angenommen, dass dem Auftragsverarbeiter eine Eigenständigkeit zukommt und die Datenweitergabe zwischen diesem und dem Verantwortlichen eine „**Offenlegung durch Übermittlung**", also ein legitimationsbedürftige Datenverarbeitung, darstellt (Art. 4 Nr. 2 u. Nr. 8 DSGVO).[309] Der Auftragsverarbeiter ist „Empfänger" (Art. 4 Nr. 9 DSGVO, nicht Dritter, vgl. Art. 4 Rn. 10 DSGVO). Nach dieser Ansicht bedarf diese Offenlegung einer eigenständigen Rechtsgrundlage, etwa in Art. 6, 9 oder 10 DSGVO.[310] Für die Offenlegung und für die Verarbeitung durch den Auftragsverarbeiter wird bei nicht sensitiven Daten Art. 6 Abs. 1 UAbs. 1 DSGVO zur Anwendung gebracht.

Demgegenüber ist eine sehr weit verbreitete Meinung, die von den deutschen Aufsichtsbehörden geteilt wird, dass Art. 28 DSGVO weiterhin eine **Privilegierungswirkung** zur Folge hat. Rechtsgrundlage für eine Verarbeitung durch einen Auftragsverarbeiter sei die des Verantwortlichen i.V.m. Art. 28 DSGVO. Der Auftragsverarbeiter

309 Wedde in DWWS, Art. 28 Rn. 5–11; Bertermann in Ehmann/Selmayr, Art. 28 Rn. 4–8; Hofmann in Roßnagel 2017, § 3 Rn. 251; LNK § 6 Rn. 6; Ingold in Sydow, Art. 28 Rn. 29; Dovas ZD 2016, 516; Piltz K&R 2016, 712; Eckhardt/Kramer DuD 2016, 145f.; wohl auch Petri in SHS Art. 28 Rn. 10.

310 Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 18.

sei weiterhin nicht Dritter, sondern Teil des Verantwortlichen.[311] Für die erstgenannte Ansicht spricht, dass dem Auftragsverarbeiter in der DSGVO eine eigenständige Verantwortung zugewiesen wird, auch wenn diese von den Vorgaben des Verantwortlichen abhängig ist. Dies ändert aber nichts daran, dass für die Zweckfestlegung und damit für die materielle Zulässigkeit der Datenverarbeitung ausschließlich der Verantwortliche zuständig ist. In der Praxis hat der Streit jedoch keine wesentlichen Auswirkungen. Diese beschränken sich darauf, dass auf unterschiedliche Rechtsgrundlagen zurückgegriffen wird, die im Rahmen von Transparenzpflichten, etwa gegenüber den Betroffenen, benannt werden müssen. In Umsetzung der Informationspflichten ist der Betroffene über die „Empfänger oder Kategorien von Empfängern", wozu die Auftragsverarbeiter gehören (Art. 4 Nr. 9 DSGVO)[312], zu informieren (Art. 13 und 14, jeweils Abs. 1 lit. e DSGVO). So kann ein Betroffener oder auch ein sonstiger Beteiligter erkennen, auf welche Rechtsgründe sich die Verarbeiter beziehen. Dass eine Auftragsverarbeitung, auch bei sensitiven Daten, grundsätzlich erlaubt ist, ist nach beiden Meinungen anerkannt.[313]

Die Auftragsverarbeitung definiert das Verhältnis einer datenschutzrechtlich verantwortlichen Stelle (Auftraggeber) zu einer Stelle (Auftragsverarbeiter bzw. Auftragnehmer), die den Verantwortlichen als **Hilfsunternehmen bei der Verarbeitung** unterstützt. Beim Verantwortlichen müssen alle datenschutzrechtlichen Voraussetzungen (Einwilligung oder gesetzliche Gestattung) für eine Verarbeitung vorliegen.

Der **Verlauf der Trennlinie** zwischen Auftragsverarbeitung und eigenständiger Verantwortlichkeit, die aus rechtlicher Sicht zu ziehen ist, war schon nach altem Recht umstritten.[314] Hieran hat sich nichts geändert. Die Bezeichnung „Auftragsverarbeitung" und „gemeinsame Verantwortlichkeit" in einem Vertrag bzw. einer Vereinbarung kann insofern nur ein Indiz dafür sein, was von den Partnern beabsichtigt ist. Ob eine reine Hilfstätigkeit vorliegt oder ob ein Partner wesentliche Entscheidungen zur Verarbeitung beiträgt, hängt von der konkreten Ausgestaltung des Vertrags bzw. der Vereinbarung und den tatsächlichen Gegebenheiten ab.[315] Letztentscheidend ist, wer die Entscheidungshoheit über die Zwecke und Mittel der Verarbeitung ausübt.[316] Auch dem Auftragsverarbeiter kann hinsichtlich seiner Entscheidungskompetenz ein gewisser Spielraum eingeräumt sein. Wann dieser Spielraum so groß wird, dass eine Eigenverantwortlichkeit anzunehmen ist, hängt von dem konkreten Kontext, den bestehenden Regelungen und der gelebten Praxis ab. Während für den Auftragsverarbeiter bzgl. der Zwecke und des „Ob" der Datenverarbeitung kein Spielraum besteht, gibt es einen solchen bzgl. der Mittel und des „Wie".[317]

311 DSK, Kurzpapier Nr. 13 v. 17.12.2918, 2; Albrecht/Jotzo, Teil 5 Rn. 22f.; Martini in Paal/Pauly, Art. 28 Rn. 8a–10; BMH, Art. 28 Rn. 15–23; Schmitz/von Dall'Armi ZD 2016, 429, 432; Schmidt/Freund ZD 2017, 14; Krohm/Müller/Peltzer RDV 2016, 307; Cremer CR 2019, 230; Schantz in Schantz/Wolff, Rn. 939; Gola in Gola, Art. 4 Rn. 58: Art. 28 DSGVO als Rechtsgrundlage; ausführlich Hartung in Kühling/Buchner, Art. 28 Rn. 13–23.

312 Weichert in DWWS, Art. 4 Rn. 99.

313 Schantz in Schantz/Wolff, Rn. 379, zu möglichen Konsequenzen beim Widerspruchsrecht Hartung in Kühling/Buchner, Art. 28 Rn. 21.

314 Petri in Simitis, § 11 Rn. 22–24.

315 Petri in SHS, Art. 28 Rn. 21.

316 Petri in SHS, Art. 4 Nr. 7, Rn. 20; Weichert in DWWS, Art. 4 Rn. 87; 96f.; Klabunde in Ehmann/Selmayr, Art. 4 Rn. 36; Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 10.

317 Hartung in Kühling/Buchner, Art. 4 Nr. 7 Rn. 13, Art. 4 Nr. 8 Rn. 7, Art. 28 Rn. 26–30.

Mit der Ablösung des bisherigen Datenschutzrechts durch die DSGVO wurde teilweise die These vertreten, dass die Abgrenzung zwischen Auftragsverarbeitung und Funktionsübertragung obsolet werde, weil die Definition des Art. 4 Nr. 8 DSGVO eigenverantwortliches Handeln des Auftragsverarbeiters nicht ausschließe, es auf Verantwortlichkeiten nicht ankomme.[318] Diese Ansicht übersieht, dass nach Art. 28 Abs. 3 lit. a DSGVO die **Weisungen des verantwortlichen Auftraggebers** konstituierend für das Auftragsverhältnis sind und nach Art. 28 Abs. 10 DSGVO eine eigene Verantwortlichkeit des Auftragsnehmers nur begründet wird, wenn eine Verarbeitung entgegen den Weisungen erfolgt, also wenn der Auftragnehmer und nicht der Auftraggeber *„Zwecke und Mittel der Verarbeitung bestimmt"*.[319] Die durch die DSGVO neu eingeführten Pflichten (Bestellung eines Vertreters, Art. 27 Abs. 1, Führen eines Verarbeitungsverzeichnisses, Art. 30, Meldepflicht bei Datenpannen, Art. 33, 34) sind nicht konstituierend für die Abgrenzung zwischen dem Auftragsverarbeiter und dem Verantwortlichen.

Die **Mittel der Verarbeitung**, also die Art und Weise der Auftragserledigung, kann der Auftragsverarbeiter nach Art. 28 DSGVO selbst bestimmen. Er ist bei der Ausgestaltung der von ihm eingesetzten und verwendeten Hard- und Software sowie der verwendeten technischen und organisatorischen Infrastruktur grundsätzlich weisungsfrei.[320] Dies hindert den Verantwortlichen aber nicht, dem Auftragsverarbeiter für die Abwicklung des Auftrags bestimmte verpflichtende Vorgaben zu machen.[321] Schon nach dem bisherigen Recht bedurfte es für die Annahme einer Datenverarbeitung im Auftrag nach § 11 BDSGaF nicht einer bis ins Detail gehenden Anweisung. Der Auftragsdatenverarbeiter war für die Festlegung der technisch-organisatorischen Maßnahmen nach § 9 BDSGaF (mit) verantwortlich (§ 11 Abs. 4 BDSGaF). Entgegen teilweise vertretener Meinung[322] hat sich insofern rechtlich nichts geändert.[323]

Der Umfang der Entscheidungsspielräume des Auftragsverarbeiters bei der **Wahl der technisch-organisatorischen Maßnahmen** ist für die Annahme einer Auftragsverarbeitung unerheblich. Es entspricht der typischen Aufgabenverteilung, dass sich damit der Auftraggeber nicht im Detail befassen muss.[324] Während Art. 28 Abs. 3 S. 1 DSGVO präzise Vorgaben des Verantwortlichen bzgl. bzgl. der Art und des Zwecks der Verarbeitung verlangt, begnügt sich Art. 28 Abs. 3 S. 2 lit. c DSGVO mit der Verpflichtung, dass der Auftragnehmer *„alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift"*.

Eine Auftragsverarbeitung setzt ein **bipolares Verhältnis** voraus. Ein Auftragsverhältnis kann nur zwischen einem Verantwortlichen und einem Auftragsverarbeiter bestehen. Weitere Stellen können nur als Unterauftragsverarbeiter, also als Auftragnehmer eines Auftragsverarbeiters, eingebunden sein. Ein Auftragsverhältnis nach Art. 28 DSGVO mit mehreren Verantwortlichen ist ausgeschlossen, da dadurch keine

318 Härting, Rn. 579; Dovas ZD 2016, 516f.; Doench/Sommerfeld in Kipker/Voskamp, 120; Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 20f.

319 Petri in SHS Art. 4 Nr. 8 Rn. 6; Härting/Gössling NJW 2018, 2524; zum Verhältnis zwischen altem und neuem Recht ausführlich Thomale in SJTK, Art. 28 Rn. 9–13.

320 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 17; Däubler in DWWS, Art. 28 Rn. 15; Bertermann in Ehmann/Selmayr, Art. 28 Rn. 3.

321 Petri in SHS, Art. 28 Rn. 73; Däubler in DWWS, Art. 28 Rn. 15.

322 Müthlein, RDV 2016, 78f.; Rücker/Kugler, DB 2016, 2768

323 Petri in SHS, Art. 28 Rn. 7, 8; Ingold in Sydow, Art. 28 Rn. 16.

324 Kremer CR 2019, 229; Schreiber ZD 2019, 55.

eindeutige Verantwortlichkeit des jeweiligen Auftraggebers sichergestellt werden kann. Dies gilt auch für gemeinsam Verantwortliche: Zwar kann hier eine einheitliche Verarbeitung gegeben sein, doch auch hier ist es möglich, dass Weisungen und Entscheidungen der Verantwortlichen voneinander abweichen. Beauftragten mehrere Verantwortliche einen Auftragnehmer, so handelt es sich bei jedem Verhältnis um je eine Auftragsverarbeitung. Eine Vermischung der Daten beim Auftragnehmer ist unzulässig. Der Auftragnehmer ist zur Mandantentrennung verpflichtet.[325]

5.8 Datenempfänger

Der **Begriff** „Empfänger" wird in Art. 4 Nr. 9 S. 1 DSGVO definiert:

> *„[...] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht."*

Empfänger ist der Dritte als Übermittlungsempfänger und der Auftragsverarbeiter (s.o. Kap. 5.7). Der Begriff setzt eine rechtliche Eigenständigkeit gegenüber der die Daten weitergebenden Stelle voraus.[326] Nicht dazu zu zählen sind Organisationseinheiten innerhalb einer verantwortlichen Stelle, da die Regelung eine weitergehende rechtliche Eigenständigkeit verlangt.[327] Auch der Betroffene selbst ist kein Empfänger. Relevant ist der Empfängerbegriff in der DSGVO im Rahmen der Informationspflichten (Art 14), der Auskunftsrechte (Art. 15), der Mitteilungspflichten (Art. 19) und bei der Verzeichniserstellung (Art. 30).

Der Begriff der **Funktionsübertragung**, der nach dem alten Datenschutzrecht als Datenverarbeitung im Auftrag einer anderen Stelle in eigener Verantwortung verwendet wurde[328], wird heute von vielen als nicht mehr nützlich angesehen.[329] Der Begriff fand sich schon in der Vergangenheit und findet sich auch heute in keinem Datenschutzgesetz. Er wurde und wird weiterhin in der Literatur und in der Wissenschaft verwendet. Mit diesem Begriff wird in Abgrenzung von der Auftragsverarbeitung ein Dienstleistungsverhältnis verstanden, bei dem der Dienstleister einen eigenen Beurteilungs-, Ermessens- und Entscheidungsspielraum in Bezug auf konkrete Verarbeitungsinhalte hat.[330]

Dadurch begründet sich eine **eigenständige datenschutzrechtliche Verantwortlichkeit** des Empfängers der übertragenen Daten. Diese besteht z.B. bei einem externen Treuhänder (s.u. Kap. 5.9) wie auch in anderen Fällen, in denen gemeinsam Verantwortliche einen gemeinsamen Zweck verfolgen (s.o. Kap. 5.2). Für die dadurch nöti-

325 Datenschutzkonferenz (DSK), Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit, Version 1.0 v. 11.10.2012.

326 Unsicher insofern Ernst in Paal/Pauly, Art. 4 Rn. 57.

327 A.A. Kühling/Buchner, Art. 4 Nr. 9 Rn. 5; Gola/Schomerus, § 3 Rn. 51; Gola, RDV 2011, 66.

328 Krasemann in Jandt/Steidle, B. II Rn. 148, 185.

329 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2; Kremer CR 2019, 228f.; Kremer in SJTK, Art. 28 Rn. 48, Hartung in Kühling/Buchner, Art. 28 Rn. 44; Thomale in Auernhammer, Art. 28 Rn. 19ff.; Müthlein, RDV 2016, 84f.; Mantz/Marosi in Specht/Mantz, § 3 Rn. 145.

330 Petri in SHS, Art. 28 Rn. 11, Härting, Rn. 575.

ge Datenoffenlegung bedarf es einer eigenständigen Rechtsgrundlage, also einer Rechtfertigung aufgrund einer Einwilligung oder eines Gesetzes. Der Begriff ist mit der DSGVO nicht überflüssig oder hinfällig geworden[331]; er ist weiterhin zur Abgrenzung von der Auftragsverarbeitung geeignet. Er eignet sich aber nicht, um eine individuelle von einer gemeinsamen Verantwortlichkeit abzugrenzen.

Werden personenbezogene Daten an Dritte weitergegeben, damit diese damit ausschließlich eigene Zwecke verfolgen, so liegt eine **Datenübermittlung** an allein verantwortliche Dritte vor. Ein Beispiel hierfür ist die Weitergabe von Daten, die im Rahmen der Aufgabenerfüllung einer Stelle entstanden sind, an eine andere Stelle für Forschungszwecke. Auch die Weitergabe von Forschungsdaten an eine andere Forschungseinrichtung mit einer eigenständigen wissenschaftlichen Zielrichtung ist eine Datenübermittlung.

5.9 Datentreuhänder

Treuhänderschaft ist ein im Zivilrecht anerkanntes Rechtsinstitut. Treuhänderaufgaben gehören z.B. zum Kernbereich notarieller oder sind ein Bestandteil anwaltlicher Tätigkeit. Möglich ist eine mehrseitige Treuhand, bei der eine Vertrauenstätigkeit gegenüber mehreren Personen oder Stellen mit möglicherweise entgegengesetzten Interessen erfolgt. Bei der treuhänderischen Tätigkeit wird dem Treuhänder eine **Rechtsmacht übertragen**, die er gemäß einer Treuhandanweisung einzusetzen hat. Besteht ein Interessenkonflikt, so bestehen regelmäßig besondere Benachrichtigungs- oder Transparenzpflichten.[332] Datentreuhänderschaft kann so organisiert sein, dass sie insbesondere Betroffeneninteressen wahrnimmt, dies möglicherweise auch im Interessengegensatz zu verarbeitenden Stellen[333], oder dass sie eher dem Bereich dieser Stellen zugeordnet werden, etwa zum Zweck der Datenminimierung (s.u. Kap. 10.4). Die unabhängige Stellung eines Treuhänders soll regelmäßig beiden Seiten dienlich sein.[334]

In der medizinischen Forschung ist der Einsatz eines Treuhänders oft Bestandteil eines umfassenden Datenschutzkonzepts (s.u. Kap. 11.4). Mit dessen Einsatz soll der Schutz der Daten gewährleistet und der Eingriff in die Betroffenenrechte minimiert werden, ohne dass der Informationsumfang für die Forschung beeinträchtigt wird. Er nimmt die Funktion eines rechtlich (teil-)selbstständigen bzw. unabhängigen **vertrauenswürdigen Dritten** wahr, der zwischen den speichernden und den forschenden Stellen sowie den Betroffenen seine Aufgabe wahrnimmt. Er sollte weisungsunabhängig sein und sich im Interesse des Vertraulichkeitsschutzes auf ein Aussageverweigerungsrecht und ein entsprechendes Verbot der Dokumentenbeschlagnahme

331 Ingold in Sydow, Art. 28 Rn. 15ff.; Schwartmann/Hermann in SJTK, Art. 4 Rn. 135; Spittka in Specht/Mantz, § 12 Rn. 68; Petri in SHS, Art. 4 Nr. 8 Rn. 6, Art. 28 Rn. 21.

332 ULD, 38.

333 Zur Treuhänderschaft im Verbraucherinteresse Blankertz, Designing Data Trusts, Why we need to test Consumer Data Trusts now, February[[in der folgenden Fußnote: Februar]] 2020, https://www.stiftung-nv.de/de/publikation/designing-data-trusts-why-we-need-test-consumer-data-trusts-now.

334 Ausführlich zu den Potentialen von Datentreuhändern Blankertz, Designing Data Trust, Why we need to test consumer data trusts now, Februar 2020, https://www.stiftung-nv.de/de/publikation/designing-data-trusts-why-we-need-test-consumer-data-trusts-now.

stützen können.[335] Dies ist der Fall, wenn ein Forschungsprojekt in einen ärztlich geleiteten Behandlungszusammenhang integriert ist und der Treuhänder als Mitwirkender nach § 203 Abs. 3, 4 StGB verpflichtet wird (s.u. Kap. 6.6). Die Vertrauenswürdigkeit eines Datentreuhänders sollte in jedem Fall durch vertragliche Festlegungen, kann aber auch durch öffentlich-rechtliche Bestimmungen abgesichert werden.[336] Sie setzt u.a. voraus, dass der Treuhänder mit den anvertrauten Daten nicht selbst Forschung betreibt.[337]

Typische **Aufgaben von Datentreuhändern** im medizinischen Forschungsbereich sind es, die Anonymisierung oder Pseudonymisierung sowie Aufgaben der Reidentifizierung vorzunehmen. Es geht also zumeist darum, die Verkettbarkeit von Daten zu handhaben und die hierfür nötigen Daten materiell-rechtlich, technisch und organisatorisch zu sichern und diese vorzuhalten. Die Funktion des Datentreuhänders besteht darin, Daten entgegenzunehmen, zu archivieren und bereitzustellen. Über den Treuhänder kann „informationelle Gewaltenteilung" sichergestellt werden.[338] Diese Aufgaben sind insbesondere relevant bei großen Datenbeständen, verschiedenen Datenquellen, komplexen und mehrfachen Datennutzungen und langfristigen Datenspeicherungen.[339] Eine Aufgabe von Treuhändern kann auch darin bestehen, für andere Stellen Transparenz- und Rechenschaftspflichten zu übernehmen, z.B. indem sie gewährleisten, dass Betroffenenrechten entsprochen wird.[340] Der Einsatz von Treuhändern ist somit eine spezifische Maßnahme zur Sicherung der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO, s.u. Kap. 10.3) oder der Wahrung der Betroffenenrechte (Art. 12ff. DSGVO) unter Einsatz technisch-organisatorischer Maßnahmen (Art. 25, 32 DSGVO).

Die Rolle von Treuhändern ist im allgemeinen **Datenschutzrecht** nicht geregelt. Eine solche findet sich vereinzelt in medizinrechtlichen Regelungen. So sieht § 12 Abs. 4 HambKHG vor, dass bei genetischer Forschung zu prüfen ist, *„ob die Sicherheit der betroffenen Personen vor einer unbefugten Zuordnung ihrer Proben und Daten es erfordert, dass die Pseudonymisierung durch eine unabhängige externe Datentreuhänderin oder einen unabhängigen externen Datentreuhänder erfolgt."* Ein Treuhänder wird rechtlich oft „Vertrauensstelle" genannt. Regelungen dazu finden sich in Krebsregistergesetzen der Länder, so etwa in § 5 Hessisches Krebsregistergesetz (HKRG)[341] oder § 6 Krebsregistergesetz Schleswig-Holstein (KRG SH)[342]. Eine Regelung gab es auch in Art. 7 Bayerisches Krebsregistergesetz.[343] Ähnliche Regelungen bestehen im Sozialgesetzbuch V (§§ 303a ff. SGB V)[344], für das Implantateregister (§§ 8, 9 IRegG) sowie zur Gewährleistung der Spenderanonymität im Transplantationsgesetz (§§ 12ff., 15c TPG) und im Transfusionsgesetz (§ 21 TFG).[345]

335 Metschke/Wellbrock, 43; Bizer, 195ff. m.w.N.; zum Beschlagnahmeschutz nach alter Rechtslage Dierks B2 F2.1, F2.2–F2.8.
336 Bizer DuD 1999, 394.
337 Böhm/Wagner, CR 1987, 625.
338 Metschke, 26f.; Dierks 2008, A1.
339 Bizer DuD 1999, 393ff.; Bizer, 196f.
340 TA-Projekt: Biobanken für die humanmedizinische Forschung und Anwendung, BT-Drs. 16/5374, 84, 103.
341 G. v. 17.10.2001, Hess GVBl. I 2001, 582.
342 G. v. 04.11.2015, GVOBl. SH 2015, 372.
343 G. v. 25.07.2000, Bay GVBl. S. 274, außer Kraft getreten am 31.03.2017; zu den Gesetzen auch Dierks 2008, B41ff.
344 Kühling, 52f.
345 ULD, 41ff.

So vielfältig die Aufgaben von Treuhändern sein können, so unterschiedlich können auch die **rechtlichen und organisatorischen Strukturen** sein, in die diese eingebunden sind. Sie können als gemeinnützige, privatwirtschaftliche oder staatliche Stellen eigenständig oder in Kooperation oder als Organisationsteil einer größeren Stelle tätig sein.[346]

Um seine Aufgabe als vertrauenswürdige Stelle wahrnehmen zu können, darf ein Treuhänder bei seiner grundlegenden Tätigkeit nicht an Weisungen gebunden werden. Das Vertrauen in ihn wird durch seine Unabhängigkeit und Neutralität begründet. Zugleich ist es aber für die Vertrauenswürdigkeit erforderlich, dass der Treuhänder **nach klaren vorgegebenen Regeln** agiert und dass die Einhaltung dieser Regeln überwacht wird bzw. das Handeln hinreichend transparent ist.[347] Die Regeln können durch Gesetze oder sonstige hoheitliche oder standesrechtliche Normen festgelegt sein, möglich ist aber auch eine vertragliche Grundlage.[348]

Gemäß den Vorgaben der DSGVO bestehen für eine rechtliche Einordnung von Datenverarbeitern nur die Alternativen einer eigenen Verantwortlichkeit oder der Auftragsverarbeitung. Da Treuhänder bzgl. ihrer Hauptfunktion weisungsunabhängig sein sollen und Weisungsabhängigkeit ein zentrales Wesensmerkmal für die Auftragsverarbeitung darstellt, kommt für den Datentreuhänder eine rechtliche **Einordnung als Verantwortlicher** in Betracht.[349] Handelt es sich bei einem Treuhänder um eine eigenständige juristische oder natürliche Person, so wird mit der Datenverarbeitung eine Verantwortlichkeit nach Art. 24 DSGVO begründet.

Rechtlich nicht ausgeschlossen ist jedoch, dass es sich bei dem Treuhänder um einen **Organisationsteil einer größeren juristischen Person** handelt. In diesem Fall liegt die datenschutzrechtliche Verantwortlichkeit gemäß DSGVO bei der juristischen Person. Die datenschutzrechtliche Letztverantwortung verbleibt bei der jeweiligen Stellenleitung.[350] Die Verantwortlichkeit für die Wahrnehmung der Treuhänderfunktion kann durch Gesetz, durch vertragliche Regelung oder auch durch einen einfachen internen Organisationsakt des Verantwortlichen begründet werden. Eine solche Delegation der Verantwortlichkeit ist dem Datenschutzrecht nicht fremd. Sie besteht in Bezug auf die Wahrung der beruflichen Verschwiegenheit durch Ärzte, also gebunden an eine persönliche Qualifikation eines Mitarbeiters (s.u. Kap. 6), aber auch funktional, etwa bei einem Betriebsarzt (§ 3 ASiG), beim Betriebsrat (§ 37, 78 S. 2 BetrVG)[351], beim (internen) Datenschutzbeauftragten (Art. 37f. DSGVO, §§ 5–7, 38 BDSG) sowie bei anderen Organisationsteilen, denen durch normative Vorgaben hin-

346 TA-Projekt: Biobanken für die humanmedizinische Forschung und Anwendung, BT-Drs. 16/5374, 84.
347 Dierks 2008, B44.
348 Dierks 2008, B45; Bizer, 197.
349 Dierks 2008, B63; Schneider 2015, 290f.
350 Dierks 2008, B46.
351 Bzgl. Betriebsräten ist dies hoch umstritten, wie hier Däubler, Gläserne Belegschaften, Rn. 640g, 850a; Brandt, CuA 11/2018, 30; Zieske, DANA 2018, 89; Hartung in Kühling-Buchner, Art. 4 Nr. 7 Rn. 11; Cumanns, RDV 2018, 55; Specht/Mantz-Ströbel/Wybitul, Teil B § 10 Rn. 77–82; Lücke, NZA 2019, 660; tendenziell Jung/Hansch, ZD 2019, 146f.; zweifelnd Gola in Gola, Art. 4 Rn. 55f.; Kranig/Wybitul, ZD 2019, 1ff.; offen lassend Hamann/Wegmann, BB 2019, 1348f.; a.A. LfDI BW, 34. Tätigkeitsbericht 2018, 1.6.1 (S. 37f.); LAG Sachsen-Anhalt 18.12.2018 – 4 TaBV 19/17, DB 2019, 1156; Kleinebrink, DB 2018, 2567f.; Beilecke, Landesdatenschutzgesetz Schleswig-Holstein, 2. Aufl. 1996, § 3 Rn. 3; zur Eigenverantwortlichkeit des Betriebs- bzw. Personalrats BAG, NJW 1998, 2466 = RDV 1998, 64.

sichtlich der Verarbeitung personenbezogener Daten eine gewisse Unabhängigkeit zugewiesen ist.

Weitgehend offen und deshalb gestaltungsfähig ist das Verhältnis, das sich datenschutzrechtlich durch die Unabhängigkeit des (internen) Treuhänders zwischen diesem und der Leitung der umfassenderen juristischen Person ergibt. Die **Beziehung Treuhänder – Stellenleitung** sollte so gestaltet sein, dass der letztlich verantwortliche Organisationsteil, also die Leitung, seine Verantwortlichkeit gemäß der DSGVO wahrnehmen kann, ohne dass die Unabhängigkeit des Treuhänders beeinträchtigt wird. Dies kann dadurch erfolgen, dass dem (internen) Treuhänder Dokumentations- und Rechenschaftspflichten gegenüber der Stellenleitung auferlegt werden, damit diese den Pflichten nach Art. 5 Abs. 2 DSGVO genügen kann. Die individuelle Bearbeitung der Betroffenenrechte (Art. 15ff. DSGVO) kann weitgehend an den Treuhänder delegiert werden.

Mangels konkreter gesetzlicher Vorgaben obliegt die Sicherstellung der Unabhängigkeit des internen Treuhänders der Organisationshoheit der Stellenleitung. Eine Rechtsform ist nicht vorgegeben. Möglich ist sowohl eine direktive Vorgabe durch die Stellenleitung als auch eine Vereinbarung zwischen Stellenleitung und Treuhänder.[352] Der **Organisationsakt** der Stellenleitung muss aber verbindlich sein, um als Garantie für die Rechte und Freiheiten der Betroffenen i.S.v. Art. 89 Abs. 1 S. 1, 2 DSGVO anerkannt werden zu können. Es ist angezeigt, eine Festschreibung der Prozessabläufe, der organisatorischen und technischen Vorkehrungen und des Entscheidungsspielraums des Treuhänders im Datenschutzkonzept (s.u. Kap. 11.4) vorzunehmen und die wesentlichen Informationen den Betroffenen (z.B. auf einem Hinweisblatt oder einer Webseite) zur Verfügung zu stellen.

Sonstige Aufgaben gemäß der DSGVO, bei denen es auf die konkrete Verarbeitung nicht ankommt, so etwa die Installation von Hard- und Software, die Festlegung und Umsetzung der technisch-organisatorischen Vorkehrungen (Art. 25, 32 DSGVO), die Erstellung der Verarbeitungsverzeichnisse (Art. 30 DSGVO) oder die Durchführung der Datenschutzfolgenabschätzung (Art. 35 DSGVO), obliegt der Stellenleitung, die in Respektierung der Unabhängigkeit des Treuhänders eine kooperative Lösung mit diesem anstreben sollte. Die Leitung der Stelle ist letztlich die Instanz innerhalb des Verantwortlichen, die über „Zweck und Mittel" der Verarbeitung bestimmt.

Bei einem externen Treuhänder ist dieser im Verhältnis zur Daten liefernden oder speichernden Stelle Dritter und erhält die personenbezogenen Daten im Rahmen seiner Aufgabenwahrnehmung in Ausübung der eigenen Verantwortlichkeit und nicht als Auftragsverarbeiter.[353] Die Rolle des Treuhänders als Dritter und als Übermittlungsempfänger hat zur Folge, dass er mit der Datenübermittlung zum **Verantwortlichen** wird. Er bestimmt (mit) über Zweck und Mittel der eigenen Verarbeitung.[354] Die Ausgestaltung einer Datentreuhänderschaft als Auftragsverarbeitung (Art. 28 DSGVO) ist zwar rechtlich nicht ausgeschlossen, aber nicht zu empfehlen. Dadurch würde der Vorteil der Datentreuhänderschaft, der Verweis auf die Vertraulichkeit durch Unabhängigkeit des Treuhänders, verloren gehen, da Auftragsver-

352 Dierks 2008, B44ff. in Bezug auf klinische Prüfungen.

353 Dierks 2008, B64.

354 A.A. hinsichtlich der alten Rechtslage Dierks (2008), B63ff., der für den Treuhänder die Regeln der Auftragsverarbeitung analog anwendete.

arbeitung insbesondere in Bezug auf die materielle Rechtmäßigkeit der Datenverarbeitung eine umfassende Weisungsabhängigkeit bedingt (Art. 28 Abs. 3 lit. a DSGVO). Weitere Vorteile einer Treuhänderschaft, etwa die technisch-organisatorische Trennung durch File-Trennung und Pseudonymisierung sowie durch die räumliche, organisatorische und personelle Abschottung, sind auch in der Ausgestaltung einer Auftragsverarbeitung erreichbar. Es ist dann aber nicht mehr angebracht, von einer Treuhänderschaft zu sprechen.

Externe Datentreuhänder im medizinischen Bereich sind in der Regel in einen umfassenderen Verarbeitungsprozess eingebunden, der mit der Datenerhebung oder zumindest der Datenübermittlung durch einen medizinischen Leistungserbringer beginnt, bei dem es zu einer Datenspeicherung bei einer weiteren Stelle kommt, über die letztlich Übermittlungen an Empfänger erfolgen, die die Daten auswerten oder anderweitig nutzen. Diese Nutzung kann für medizinische Forschungszwecke erfolgen. Die Einbindung des Treuhänders erfolgt zumeist bei einem Datentransfer zwischen Verantwortlichen. Grundlage solcher Treuhänderprozesse sind regelmäßig gemeinsame Entscheidungen, in die außer dem Treuhänder selbst zumindest die speichernde Stelle eingebunden ist. Auch die anliefernden sowie die auswertenden Stellen können einbezogen sein. Bei derartigen arbeitsteiligen Verarbeitungsprozessen für einen gemeinsamen Zweck gemäß einem verabredeten Verfahren handelt es sich um typische Formen **gemeinsamer Verantwortung** (s.o. Kap. 5.2–5.6). Welche Stellen bei dieser gemeinsamen Verantwortung mit einbezogen sind, hängt von den objektiven tatsächlichen Umständen ab. Relevant ist insbesondere, ob die Übermittlung zum Zweck der Speicherung sowie die Übermittlung zum Zweck der Auswertung/Nutzung jeweils auf einer Einzelfallentscheidung beruht oder die Entscheidung hierüber im gemeinsam vorgegebenen Prozessablauf vorweggenommen wird.

Eine **Funktionsübertragung** (s.o. Kap. 5.8) an einen Treuhänder kommt nur dann in Betracht, wenn diesem das ausschließliche Bestimmungsrecht über den Umgang mit treuhänderisch übertragenen Daten zugestanden wird, d.h., wenn dem Datentreuhänder in einer Verarbeitungskette das alleinige Bestimmungsrecht über die durch ihn erfolgende Verarbeitung zugestanden wird. Dies dürfte regelmäßig nicht im Interesse der Daten anliefernden noch in dem der Daten nutzenden Stellen liegen. Der Zweck der Treuhänderschaft liegt ja gerade darin, dass vom Treuhänder zwar unabhängig, aber gebunden an spezifische Vorgaben und somit vertrauenswürdig gehandelt wird. Insofern liegt die Ausgestaltung als gemeinsame Verantwortlichkeit nahe. Eine Funktionsübertragung (Kap. 5.8) ist aber nicht ausgeschlossen. Diese kann angenommen werden, wenn dem Treuhänder die ausschließliche Entscheidungshoheit über den treuhänderisch verwalteten Prozess (z.B. über die Reidentifizierung von pseudonymisierten Datensätzen) zugewiesen wird, ohne dass dieser Prozess eine notwendige Bedingung für sonstige Verarbeitungsprozesse ist. Eine solche notwendige Bedingung der Kooperation von Treuhändern mit weiteren Verantwortlichen ist z.B. bei der Behandlung von Betroffenenansprüchen bei einem pseudonym geführten Krankheitsregister gegeben.

An die Stelle einer gemeinsamen Entscheidung der Verantwortlichen in einer Form, die Eingang in eine Vereinbarung nach Art. 26 DSGVO findet, kann eine vollständig oder teilweise normativ, etwa durch den **Gesetzgeber**, vorgegebene Regelung treten (Art. 26 Abs. 1 S. 2 DSGVO).

Für die Beteiligung eines Treuhänders in einem Forschungsvorhaben bedarf es einer rechtlichen Einbindung. Fehlen gesetzliche oder sonstige übergeordnete rechtliche Vorgaben, so kommt als rechtlicher Rahmen eine **vertragliche Regelung** in Betracht. Bei der Festlegung der wesentlichen Vertragsinhalte sind die Anforderungen an eine gemeinsame Verantwortung zu beachten; dabei ist eine Orientierung an den rechtlichen Vorgaben für die Auftragsverarbeitung angesagt (s.o. Kap. 5.4).[355]

Inhalt der vertraglichen Regelung sollte u.a. eine spezifische **Vertraulichkeitsvereinbarung** sein.[356] Die rechtliche Absicherung der Vertraulichkeit kann darin bestehen, dass die Person, die mit der Treuhänderfunktion beauftragt wird, als Mitwirkende einer beruflichen Vertraulichkeitsverpflichtung unterliegt (s.u. Kap. 6.6). Notare, Rechtsanwälte oder auch Ärzte sind nicht allein wegen ihres Berufes schweigepflichtig, sondern auch wenn sie unabhängig von ihrer ursprünglichen Berufstätigkeit eine Treuhänderaufgabe wahrnehmen.[357] Es ist darauf zu achten, dass der Treuhänder nicht mit weiteren Aufgaben betraut wird, die zu Interessenkonflikten führen können.

Angesichts der technischen Möglichkeiten der digitalen Verkettung besteht die Notwendigkeit, die Datenbestände des Datentreuhänders so von den Forschungsmerkmalsdaten oder auch von sonstigen Datenbeständen abzuschotten, dass nur eine kontrollierte Zusammenführung, etwa zu Identifizierungszwecken, erfolgen kann.[358] Eine Absicherung der Vertraulichkeit kann durch die vertragliche Gewährleistung einer personellen, organisatorischen und räumlichen **Trennung der Wahrnehmung der Treuhändertätigkeit** von sonstigen Aufgaben erfolgen. Eine solche Trennung ist bei Forschungsprojekten insbesondere gegenüber wissenschaftlichen Datenauswertungen geboten.[359]

Um das Vertrauen der Betroffenen als Datengeber wie auch der Forschenden als Datennutzer zu rechtfertigen, sollte das Verfahren beim Datentreuhänder transparent sein in Bezug auf Datenquellen, Datenherausgaben und die dazwischen erfolgenden Prozesse. Das **Transparenzerfordernis** erstreckt sich damit auch auf das Verfahren, die Entscheidungsprozesse wie die Maßnahmen der Datensicherheit. Vertrauensfördernd sind Zertifizierungen und Auditierungen sowie die Umsetzung von Kontroll- und Berichtspflichten während des laufenden Betriebs.[360]

355 Ebenso Dierks 2008, B64.
356 Dierks 2008, B65.
357 Dierks 2008, B80.
358 Umfassend ULD, 50f.
359 Dierks 2008, B65; Dierks in Dierks/Roßnagel, 34; vgl. § 303a SGB V gemäß BT-Drs. 19/14867.
360 Martini/Hohmann NJW 2020, 3574.