13 Auslandskooperationen

Angesichts von **globalen Herausforderungen**, auch im Gesundheitsbereich, ist eine weltweite Kooperation von Forschenden zur Erlangung neuer Erkenntnisse oft unabdingbar. Tatsächlich findet medizinische Forschung immer mehr grenzüberschreitend, gesamteuropäisch und international statt.[864] Dies setzt in vielen Fällen einen Austausch personenbeziehbarer Daten voraus. Das Regelungsregime für die Forschung unterscheidet sich in den Rechtsordnungen teilweise stark, insbesondere wenn es um die Anerkennung und den Schutz des Grundrechts auf Datenschutz geht. Es ist aus verfassungsrechtlicher Sicht nicht möglich, aber auch aus praktischer Sicht nicht angebracht, einen in anderen Staaten gepflegten Umgang mit Gesundheitsdaten für Forschungszwecke, der nicht europäischen Standards entspricht, zum Vorbild zu nehmen.[865] Datenschutz darf und soll zugleich aber auch sinnvolle grenzüberschreitende Forschungsprojekte nicht verhindern.

Unterschiedliche Konzepte beim Datenschutz in verschiedenen Staaten müssen respektiert werden.[866] Dies darf jedoch nicht dazu führen, dass die grundlegenden Verfassungsrechte der Betroffenen und der Schutz von deren informationeller Selbstbestimmung aufgegeben werden. Insofern bestehen schon für den Gesundheitsbereich einige wenige grundlegende Regelwerke.[867] Die DSGVO enthält darüber hinausgehend wirksame Lösungsansätze.

---

864 Deutscher Ethikrat, 61; Weichert 2018, Kap. 3.12.

865 So aber Thüsing/Rombey NZS 2019, 203.

866 RfII, 11.

867 Z.B. World Medical Association (WMA), WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, überarbeitet Oktober 2016; Überblick bei Dochow, 279ff.

13.1 Übermittlungen in der EU und im EWR

Die Einbindung ausländischer Beteiligter als Projektpartner oder Dienstleister bei der Verarbeitung personenbezogener Daten richtet sich nach der DSGVO. Soweit hierbei Daten an **Projektpartner mit Sitz in der Europäischen Union** (EU) übermittelt werden sollen, gelten die gleichen Voraussetzungen wie für Übermittlungen innerhalb Deutschlands (Art. 1 Abs. 3 DSGVO).

Entsprechendes gilt für Empfänger in den Mitgliedstaaten des **Europäischen Wirtschaftsraums** (EWR) Norwegen, Liechtenstein und Island.[868] Gemäß Art. 7 lit. a Hauptabkommen über den EWR (EWR-Abkommen) sind alle EWR-Staaten verpflichtet, die DSGVO innerstaatlich zu übernehmen. Um Anwendung zu finden, müssen Rechtsvorschriften vom EWR-Ausschuss überprüft werden und, so sie zur Anwendung kommen sollen, in die Protokolle und Anhänge zum EWR-Abkommen übernommen werden. Dies ist am 06.07.2018 geschehen, sodass die DSGVO seit dem 20.07.2018 dort gilt und unmittelbar anwendbar ist.

Das Verhältnis zwischen der EU und Großbritannien ist noch nicht endgültig geklärt. Gemäß dem Brexit-Abkommen wurde der Übergangszeitraum der Zulassung von Datentransfers zunächst bis zum 31.07.2021 verlängert. Danach ist das Land als Drittland zu behandeln (s.u. Kap. 13.2). Die EU-Kommission hat am 28.06.2021 einen Angemessenheitsbeschluss gemäß Art. 45 DSGVO angenommen. Datenübermittlungen in das Vereinigte Königreich benötigen also keiner besonderen Genehmigung. Diese Entscheidung steht aber unter einem Prüfungsvorbehalt, da die britische Regierung angekündigt hat, ihr Datenschutzrecht zu entbürokratisieren. Zu den Punkten, die weitere Klarstellungen beziehungsweise eine spezielle Kontrolle erforderten, zählt zudem die im Vereinigten Königreich praktizierte Massenüberwachung. Ob das Datenschutzniveau in Großbritannien von der EU-Kommission langfristig als angemessen anerkannt werden wird, hängt davon ab, ob und inwieweit das Land die bisherigen Datenschutzregeln ändert.[869]

13.2 Übermittlungen an Drittstaaten

Ansonsten, also bei Datenübermittlungen an Empfänger aus Drittländern außerhalb der EU und des EWR, gelten die Art. 44ff. DSGVO, wonach beim Empfänger nicht ein gleichwertiges, wohl aber ein angemessenes Datenschutzniveau gewährleistet sein muss. Generell ist Art. 44 DSGVO anzuwenden:

> *„Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestim-*

868 Art. 217, 288 Abs. 2 AEUV, vgl. zu Großbritannien Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 106.
869 Mühlauer, Großbritannien: Goodbye, verhasste Cookie-Banner, www.sueddeutsche.de 26.08.2021.

mungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."

Hat die Kommission der EU beschlossen, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet, dann bedarf es für die jeweiligen Datenübermittlungen keiner besonderen Genehmigung (Art. 45 Abs. 1 DSGVO). Solche umfassenden **Genehmigungen für Übermittlungen** gibt es noch nach den Regelungen des Art. 25 Abs. 6 UAbs. 1 EG-DSRl, die auch unter der DSGVO weiterhin gültig sind, für folgende Staaten: Andorra, Argentinien, Guernsey, Faröer-Inseln, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz[870], Uruguay.[871] Die für die EG-DSRl geltenden Angemessenheitsbeschlüsse wurden durch den Durchführungsbeschluss (EU) 2016/2295 an die Anforderungen angepasst, die der EuGH durch sein Safe-Harbor-Urteil vom 06.10.2015 (Schrems I) aufgestellt hatte.[872] Die Anforderungen wurden vom EuGH in seinem Urteil zum Privacy Shield vom 16.07.2020 (Schrems II) bekräftigt und präzisiert.[873]

Am 23.01.2019 wurde von der EU-Kommission ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO in Bezug auf **Japan** gefällt.[874]

Das in den **USA** geltende Datenschutzniveau wird vom EuGH als nicht angemessen bewertet.[875] Das oberste europäische Gericht hat deshalb die Angemessenheitsbeschlüsse der EU-Kommission aus dem Jahr 2000 und aus dem Jahr 2016 aufgehoben. Diese Angemessenheitsbeschlüsse beruhten jeweils auf einem umfangreichen Rechtsrahmen, der beim EU-US-Privacy-Shield in seinen wesentlichen Grundstrukturen von Safe-Harbor übernommen worden war.

Die fehlende Angemessenheit des Datenschutzniveaus hat seinen Grund in gesetzlichen Regelungen in den USA, die es Behörden mit den Argumenten der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates erlaubt, in massenhaftem Umfang auf personenbezogene Daten zuzugreifen. Hiergegen bestehen **keine wirksamen Rechtsschutzmöglichkeiten** für die Betroffenen. Außerdem fehlt es an einer unabhängigen Datenschutzkontrolle.

Zwecks Kompensation dieser Defizite bedarf es bei einem Datenexport in die USA „geeigneter Garantien". Diese können sich aus von der Kommission erarbeiteten Standarddatenschutzklauseln ergeben (s.u.). Die bisher geltenden Klauseln sind aber nicht ausreichend. Vielmehr sind **ergänzende Vertragsregelungen** nötig. Diese können darin bestehen, dass dem Datenimporteur in den USA Informationspflichten gegenüber dem europäischen Exporteur auferlegt werden, wenn die importierten Daten einer zweckwidrigen Nutzung zugeführt werden sowie wenn von den Betrof-

870 Mausbach ZD 2019, 450.

871 Schantz in SHS, Art. 45 Rn. 28.

872 EuGH 06.10.2015 – C-362/14 (Safe Harbor), NJW 2015, 3151 = JZ 2016, 360 = DuD 2015, 823 = NVwZ 2016, 43 = WM 2015, 2383 = MMR 2015, 753 = K&R 2015, 710 = DÖV 2015, 1070.

873 EuGH 16.07.2020 – C-311/18 (Privacy Shield), NJW 2020, 2613 = DuD 2020, 685 = WM 2020, 1495 = EuZW 2020, 941 = MMR 2020, 597; dazu Botta CR 2020, 505ff.; Golland NJW 2020, 2593ff.; Schröder DB 2020, 1945ff.; Voigt CR 2020, 513ff.; Frenz DVBl 2020, 1270ff.

874 Siehe https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en m.w.N. zu den Angemessenheitsbeschlüssen.

875 EuGH 06.10.2015 – C-362/14 (Safe Harbor, Schrems I), EuGH 16.07.2020 – C-311/18 (Privacy Shield Schrems II).

fenen, von europäischen Gerichten oder von europäischen Aufsichtsbehörden begründete Informationsersuchen vorliegen. Ein angemessener Rechtsschutz kann den Betroffenen gegenüber dem europäischen Datenexporteur zugesichert werden.[876]

Bei Nichtbestehen eines Angemessenheitsbeschlusses zu einem Empfängerland und Vorliegen geeigneter Garantien bedarf es der Genehmigung des Datentransfers. Dies ist insbesondere möglich über zuvor von der EU-Kommission genehmigte Standarddatenschutzklauseln (Art. 46 Abs. 2 DSGVO) oder über verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, Art. 47 DSGVO). Letztgenannte müssen von den **Aufsichtsbehörden genehmigt** werden. Möglich und auch zu empfehlen ist der separate Abschluss eines – auch zu genehmigenden – Export-Import-Vertrags, in dem Vertragspartner die Geltung und die Durchsetzbarkeit eines angemessenen Datenschutzniveaus verabreden.[877]

Als Legitimation von Datenübermittlungen ins Drittausland im Forschungsbereich bieten sich **Standarddatenschutzklauseln** (früher Standardvertragsklauseln) gemäß Art. 46 Abs. 2 lit. c, d DSGVO an, an denen sich alle Beteiligten eines möglicherweise umfangreichen Forschungsprojektes beteiligen. Bisher gibt es keine von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der EU-Kommission gemäß Art. 93 Abs. 2 DSGVO genehmigt wurden (Art. 46 Abs. 2 lit. d DSGVO). Notwendig ist aber eine Ergänzung bei den genehmigten Klauseln, wenn im konkreten Fall die Garantien nicht ausreichen.[878] Gemäß Art. 46 Abs. 5 DSGVO bleiben aber auf der Grundlage der Richtlinie 95/46/EG (EG-DSRl) genehmigte Standardvertragsklauseln gültig, bis sie geändert, ersetzt oder aufgehoben wurden. Die EU-Kommission hat bisher folgende Klauseln genehmigt: Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vom 15.06.2001 (Set 1)[879], alternative Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vom 27.12.2004 (Set 2)[880] und Standardvertragsklauseln über die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer vom 05.02.2010.[881]

Als Grundlage für eine Datenübermittlung ins Drittausland kommen weiterhin genehmigte **Verhaltensregeln** nach Art. 40 Abs. 3 DSGVO in Betracht (Art. 46 Abs. 2 lit. e DSGVO). Derartige Verhaltensregeln (Codes of Conduct – CoC) werden von Verbänden oder Vereinigungen aufgestellt und dienen der Spezifizierung der Vorgaben der DSGVO in bestimmten Branchen (vgl. Art. 40 Abs. 2 DSGVO). Sie müssen geeignete Garantien für Übermittlungen in Drittländer vorsehen und von einer Aufsichtsbehörde genehmigt worden sein. Derartige Verhaltensregeln können für den Forschungsbereich oder spezifische für den medizinischen Forschungsbereich von den einschlägigen Forschungsverbänden in Deutschland erarbeitet und von den jeweils zuständigen Aufsichtsbehörden genehmigt werden.[882]

876 EuGH 16.07.2020 – C-311/18 Rn. 105; LfDI Baden-Württemberg, Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer? 07.09.2020; so schon Weichert/Schuler, DuD 2016, 386ff.

877 Weichert/Schuler DuD 2016, 386ff.

878 EuGH 16.07.2020 – C-311/18, Rn. 132f; Kociok/Hofmann K&R 2020, 594f.

879 2001/497/EG, ABl. L 181 v. 04.07.2001, 19–31, Aktenzeichen K(2001) 1539, konsolidierte Fassung v. 17.12.2016.

880 2004/915/EG, ABl. L 385/74 v. 19.12.2004, Aktenzeichen K(2004) 5271.

881 2010/87/EU, ABl. L 39/5 v. 12.02.2010, Aktenzeichen K(2010) 593, alle Klauseln sind abgedruckt in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2015, Anlagen 4–6.

882 Ausführlich dazu die Kommentierung von Weichert in DWWS, Art. 40, 41.

13.3 Einwilligung und weitere bestimmte Ausnahmen

Fehlt es an einem Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO, an verbindlichen internen Datenschutzvorschriften nach Art. 47 sowie an sonstigen geeigneten Garantien für eine Datenübermittlung ins Drittausland oder an eine internationale Organisation, so erlaubt Art. 49 Abs. 1 UAbs. 1 DSGVO Datenübermittlungen unter folgenden **Bedingungen**:

> *„a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde, […]*
>
> *d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig, […]*
>
> *g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind."*

Art. 49 DSGVO ist als **Ausnahmevorschrift** konzipiert. Sie eignet sich nicht für Verarbeitungen, die massenhaft, wiederholt und routinemäßig erfolgen.[883] Bevor eine Übermittlung nach Art. 49 DSGVO erlaubt wird, ist zu prüfen, ob dies nicht durch Art. 48 DSGVO ausgeschlossen wird, der eine internationale Übereinkunft oder ein Rechtshilfeabkommen voraussetzt.[884]

Gemäß Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO kann eine **Einwilligung** Übermittlungen ins unsichere Drittausland legitimieren. Hierfür müssen zunächst sämtliche Voraussetzungen für eine wirksame Einwilligung nach der DSGVO vorliegen (Art. 4 Nr. 11, 6 Abs. 1 UAbs. 1 lit. a, 7, 9 Abs. 2 lit. a), wozu insbesondere die Freiwilligkeit, die Bestimmtheit und der Hinweis auf die Widerruflichkeit gehören. Die Einwilligung muss „ausdrücklich" sein. Entsprechend Art. 9 Abs. 2 lit. a DSGVO, wonach sich die ausdrückliche Erklärung auf die Verarbeitung sensitiver Daten beziehen muss, muss hier ausdrücklich auf die Verarbeitung im unsicheren Drittausland Bezug genommen werden. Zudem muss auf die bestehenden Risiken hingewiesen worden sein. Diese Unterrichtung kann allgemeiner Art sein, sollte aber so konkret wie möglich auf die beim Empfänger bestehenden Risiken eingehen. Der Betroffene ist darüber zu informieren, welche Daten an welchen Empfänger und welchen Zielort übermittelt werden und welche Verarbeitungen dort geplant sind. Als Risiko ist zu benennen, dass möglicherweise Betroffenenrechte nicht adäquat durchgesetzt werden können. Liegen konkrete Erkenntnisse über die Verarbeitungspraxis vor, so ist darauf hinzuweisen.[885] Ändern

883 Zerdick in Ehmann/Selmayr, Art. 49 Rn. 4.

884 EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 v. 25.05.2018, 5; Schantz in SHS, Art. 49 Rn. 36; Schröder in Kühling/Buchner, Art. 49 Rn. 24.

885 EDPB, Guidelines 2/2018 v. 25.05.2018, 7f.; Ambrock/Karg ZD 2017, 157; Däubler in DWWS, Art. 49 Rn. 5; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 6; vgl. das Beispiel der Gendatenübermittlung nach Hongkong, Netzwerk Datenschutzexpertise, 20.03.2020, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_eluthia_previatest_final.pdf.

sich Bedingungen bei der Datenverarbeitung und dem Risiko, so ist zumindest eine Information an den Betroffenen, bei wesentlichen Änderungen eine erneute Einwilligung nötig.[886]

Wegen der verschärften Anforderungen gegenüber dem alten Recht kann nicht davon ausgegangen werden, dass (wirksame) **alte Einwilligungen** in den Drittlandstransfer[887] ab Mai 2018 weiterhin wirksam sind. Es bedarf vielmehr einer Feststellung im konkreten Fall, dass die Voraussetzungen des Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO vorliegen.[888]

Die Ausnahmevorschrift des Art. 49 Abs. 1 UAbs. 1 lit. d DSGVO, die Übermittlungen ins unsichere Drittausland aus Gründen des **öffentlichen Interesses** erlaubt, zielt auf öffentliche Stellen ab. Private als Empfänger sind aber nicht völlig ausgeschlossen.[889] Solche Gründe können in den Bereichen der Steuerverwaltung, der sozialen Sicherung oder der öffentlichen Gesundheit liegen. Ausdrücklich als Beispiele genannt werden die *„Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport"* (ErwGr 112 S. 1). Ein öffentliches Interesse des Empfängerstaates soll nicht genügen; es bedarf eines solchen Interesses der Union oder eines Mitgliedstaats. Für die Übermittlung muss im konkreten Fall ein wichtiger Grund vorliegen. Der wichtige Grund muss nach Art. 49 Abs. 4 DSGVO im Unionsrecht oder im Recht eines Mitgliedsstaats anerkannt sein.[890] Weiterhin ist zu prüfen, ob geeignete Garantien gemäß Art. 46 Abs. 2 lit. a DSGVO oder in Form völkerrechtlicher Zusicherungen bestehen.[891] Für Forschungszwecke kommt eine Übermittlung z.B. zur Erkundung der Ursachen und der Bekämpfung einer aktuellen Pandemie in Frage.

Eine **Registerübermittlung** nach Art. 49 Abs. 1 UAbs. 1 lit. g DSGVO betrifft öffentliche Register, die nicht notwendigerweise von einer Behörde geführt sein müssen. Private Datensammlungen werden aber nicht erfasst. Als Beispiele werden das Grundbuch, das Handelsregister, das Vereinsregister, das Bundeszentralregister sowie sonstige „Transparenzregister" genannt. Die Register müssen für jedermann frei zugänglich sein. Eine Übermittlung ist nur zulässig an Personen oder Stellen, die ein berechtigtes Interesse haben und selbst in das Register Einblick nehmen dürften.[892] Besondere Relevanz erlangt die Regelung für internetgestützte Register.[893] Es ist nicht erkennbar, dass der Unionsgesetzgeber von der Vorschrift auch Forschungsregister erfasst sehen wollte. Sind aber die rechtlichen Voraussetzungen gegeben, so können über diese Ausnahmeregelungen Übermittlungen gerechtfertigt sein.

886 Klein/Pieper in SJTK, Art. 49 Rn. 6.
887 Hierzu Artikel 29-Datenschutzgruppe, WP 114 v. 25.11.205, 12–14.
888 EDPD, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 v. 25.05.2018, 4f.; Ambrock/Karg ZD 2017, 157f.; vgl. ErgGr 111.
889 EDPB, Guidelines 2/2018 v. 25.05.2018, 11.
890 EDPB, Guidelines 2/2018 v. 25.05.2018, 10f.; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 14; Hladjik in Auernhammer, Art. 49 Rn. 6.
891 Schantz in SHS, Art. 49 Rn. 38 mit Verweis auf die Rechtsprechung von EuGH und BVerfG.
892 EDPB, Guidelines 2/2018 v. 25.05.2018, 13f.; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 17; Däubler in DWWS, Art. 49 Rn. 16; Schantz in SHS, Art. 49 Rn. 49.
893 Zerdick in Ehmann/Selmayr, Art. 49 Rn. 17.

13.4 Übermittlungen von Sozialdaten

Wegen der Öffnungsklauseln in der DSGVO und des abschließenden Charakters der Verarbeitungsregeln in den SGB richtet sich die grenzüberschreitende Übermittlung von Sozialdaten, **auch für Forschungszwecke**, nicht direkt nach den Regeln der DSGVO, sondern ist im SGB selbst geregelt. § 77 Abs. 1 SGB X dient als Rechtsgrundlage für die Übermittlung in andere Staaten der EU bzw. des EWR. § 77 Abs. 2 SGB X ist Rechtsgrundlage für Übermittlungen in Länder außerhalb der EU mit Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO). Liegt kein Angemessenheitsbeschluss vor, so ist in Anwendung von § 77 Abs. 3 SGB X eine Datenübermittlung erlaubt auf der Grundlage *„zwischenstaatlicher Übereinkommen auf dem Gebiet der sozialen Sicherheit"* (Nr. 1) oder soweit die Voraussetzungen von § 69 Abs. 1 Nr. 1 u 2 oder § 70 SGB X vorliegen und dem keine schutzwürdigen Interessen der Betroffenen entgegenstehen.[894] Da die §§ 69, 70 SGB X auf die Erfüllung sozialer Aufgaben sowie des Arbeitsschutzes abzielen, können Sozialdaten für Forschungszwecke in das aus Datenschutzsicht unsichere Drittausland nur auf der Grundlage zwischenstaatlicher Übereinkommen übermittelt werden.

13.5 Übermittlung von Berufsgeheimnissen

Keine Rechtsklarheit besteht, inwieweit **Berufsgeheimnisse** ins Ausland transferiert werden dürfen. Eine Vermutung hierfür besteht, wenn datenschutzrechtlich die Angemessenheit des Schutzniveaus im Ausland festgestellt wurde. Art. 9 Abs. 3 DSGVO erlaubt ergänzend, dass sensitive Daten für die in Art. 9 Abs. 2 lit. h DSGVO genannten Zwecke verarbeitet werden, *„wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedsstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt."*

Hintergrund dieser Regelung ist, dass die EU-Mitgliedstaaten ihre Regelungen zu Berufsgeheimnissen mit der DSGVO nicht aufgeben wollten.[895] Die Regelung ist dahingehend zu verstehen, dass national oder europarechtlich zusätzliche Verarbeitungsvoraussetzungen geregelt werden können, aber nicht müssen. Art. 9 Abs. 3 DSGVO erlaubt dem deutschen Gesetzgeber die Aufrechterhaltung des für Berufsgeheimnisse geltenden Zwei-Schranken-Prinzips (s.o. Kap. 6.3).

Irritierend ist aber, dass die Öffnungsklausel des Art. 9 Abs. 3 DSGVO auf Verarbeitungszwecke nach Abs. 2 lit. h beschränkt ist. Die dort genannten *„Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich"*

schließen **medizinische Forschung** nicht generell mit ein. Diese findet als „wissenschaftliche Forschung" in Art. 9 Abs. 2 lit. j DSGVO ausdrücklich Erwähnung.

Bei der Verwendung von **Gesundheitsdaten** für Forschungszwecke kann auf die lit. h oder i zurückgegriffen werden, wenn diese „im öffentlichen Interesse" „gesundheits-

894 Bieresborn NZS 2017, 931f.
895 Albrecht/Jotzo, Teil 3 Rn. 58.

bezogenen Zwecken" dient (ErwGr 53 S. 159). Damit kommt keine skeptische Haltung des Verordnungsgebers gegenüber medizinischer Forschung und Entwicklung zum Ausdruck.[896] Es wird lediglich klargestellt, dass rein kommerziell ausgerichtete Forschung etwa von Pharmaunternehmen oder Unternehmen im Bereich der Biotechnik die Privilegierungen von Art. 9 Abs. 2 DSGVO nicht in Anspruch nehmen können.[897] Die Alternativen in Art. 9 Abs. 2 DSGVO können sich teilweise überschneiden. Die nicht anwendungsorientierte medizinische Forschung ist aber ausschließlich in lit. j und nicht in lit. h geregelt. Aus Art. 9 Abs. 3 DSGVO kann also nicht geschlossen werden, dass und inwieweit mit der Geltung der DSGVO Berufsgeheimnisse ein Hindernis für einen grenzüberschreitenden Datentransfer sind.

Auch aus den sonstigen Regelungen ergeben sich keine klaren Hinweise darauf, ob grenzüberschreitende Übermittlungen von Berufsgeheimnissen für Forschungszwecke erlaubt oder untersagt sein sollen. Klar ist, dass insofern Öffnungsklauseln zur Anwendung kommen, die insbesondere in Art. 9 Abs. 2 lit. j und Art. 89 Abs. 2 DSGVO geregelt sind. Die deutschen Gesetzgeber sahen es offenbar bisher nicht für notwendig an, die internationale Forschungskommunikation mit Berufsgeheimnissen zu regeln. Es ist deshalb naheliegend, insofern eine **grundrechtsbasierte Abwägung** vorzunehmen. Dabei kann die Erwägung eine Rolle spielen, inwieweit angesichts der spezifischen Situation der Auslandsverarbeitung und angesichts der bestehenden konkreten Risiken ein gleichartiger Schutz im Interesse der Schutzziele des Berufsgeheimnisses nötig ist.[898] Angesichts der restriktiven Regeln in Art. 49 Abs. 1 S. 1 lit. a DSGVO kann eine Einwilligung als Offenbarungsbefugnis zu Berufsgeheimnissen gegenüber Empfängern im unsicheren Drittausland im Ausnahmefall wirksam sein. Auch bei sonstigen Offenbarungen in ein Drittland muss eine wirksame Schweigepflichtentbindung als Mindestvoraussetzung vorliegen.

Bei einer **Verarbeitung für Forschungszwecke** kommt es – den Grunderwägungen der Privilegierung dieser Zwecke in der DSGVO folgend – weniger auf den Schutz des individuellen Vertrauensverhältnisses an als auf eine strenge Zweckbindung und Abschottung der Forschung gegen operative Zwecke (s.o. Kap. 8). Von materiell-rechtlicher Relevanz ist der Umstand, dass Dienstleister, die durch § 203 Abs. 3, 4 StGB gebunden sind und dadurch zu Berufsgeheimnisträgern werden, vor deutschen Gerichten gemäß § 5 Nr. 7 StGB zur Verantwortung gezogen werden können, selbst wenn der Geheimnisverrat nach ausländischem Recht nicht strafbar ist.[899] Umgekehrt kann von Bedeutung sein, wenn, anders als nach deutschem Recht, wo mitwirkende Personen durch ein Zeugnisverweigerungsrecht geschützt sind (§ 53a StPO)[900], ein entsprechender Schutz im Ausland nicht besteht.[901] Kein Berufungsfall kann es dagegen sein, dass mit bestimmten Auslandsübermittlungen ein bestehendes Vollzugsdefizit nur vertieft wird.[902]

896 So aber Härting, Rn. 549.
897 Weichert in Kühling/Buchner, Art. 9 Rn. 150.
898 Grosskopf/Momsen CCZ 2018, 103.
899 Pohle/Ghaffari CR 2017, 493.
900 Zu dieser Notwendigkeit Momsen/Savić, KriPoZ 2017, 303f.
901 Grosskopf/Momsen CCZ 2018, 105.
902 Ebenso Grosskopf/Momsen CCZ 2018, 103f.

Für einige Berufsgeheimnisträger ist die Mitwirkung von ausländischen Dienstleistern ausdrücklich geregelt, etwa für Rechtsanwälte (§ 43e Abs. 4 BRAO), Steuerberater oder Wirtschaftsprüfer:

„Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet."[903]

Eine entsprechende **explizite Regelung** für medizinische Berufsgeheimnisträger gibt es nicht. In der Gesetzesbegründung zu den genannten Regelungen wird ausgeführt, dass für die anderen Mitgliedstaaten der EU *„in der Regel von einem solchen Schutz ausgegangen werden"* kann. Bei anderen Staaten sei im Einzelfall zu prüfen, ob der erforderliche Schutz gewährleistet ist.[904] Aus den bereichsspezifischen Regelungen wird teilweise geschlossen, dass in Bezug auf die nicht spezifisch geregelten Berufsgruppen, zu denen auch die Heilberufe gehören, keine weiteren Einschränkungen bestehen.[905] Ein mit dem Inland vergleichbares Schutzniveau wird aber generell im Datenschutzrecht gefordert (Art. 44ff. DSGVO). Es ist nicht erkennbar, dass mit den Übermittlungsregelungen der DSGVO der berufsspezifische Geheimschutz umgangen werden sollte, soweit keine spezifischen Regelungen zur Auslandsübermittlung bestehen.

13.6 Anonymität bei Datenbeschaffung aus einem Drittland

Auf eine Datenübermittlung aus dem Drittland folgt eine Datenerhebung in der EU. Die Übermittlung für Forschungszwecke von Daten aus dem Ausland ist nach dem jeweiligen Recht des Staates zu bewerten, aus dem die Daten übermittelt werden. Werden nach dem **Recht des übermittelnden Staates** Daten als anonym eingestuft, sodass sie nicht unter das dortige Datenschutzrecht fallen und deshalb übermittelt werden dürfen, so hat dies jedoch keine Indizwirkung für die Bewertung der Erhebung dieser Daten und deren weitere Verarbeitung nach europäischem Recht.

Eine **Erhebung in der EU** stellt gemäß Art. 4 Nr. 1 DSGVO eine Form der Datenverarbeitung dar, soweit nach der DSGVO die Daten als personenbezogen zu bewerten sind. Alleiniger Beurteilungsrahmen sind hierbei die Vorgaben zum Personenbezug nach Art. 4 Nr. 1 DSGVO. Gemäß dem hierbei anzulegenden objektiven Maßstab kommt es darauf an, ob die übermittelten Proben oder Datensätze *„nach allgemeinem Ermessen genutzt werden [können], um die natürliche Person direkt oder indirekt zu identifizieren […]"* (ErwGr 26, S. 3). Bei dieser Feststellung sollen *„alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."* (ErwGr 26, S. 4).

903 So § 43e Abs. 4 BRAO, ebenso § 62a Abs. 4 Steuerberatungsgesetz, § 50a Abs. 4 Wirtschaftsprüferordnung.

904 BT-Drs. 18/11936, 35; dazu ausführlich mit Ausführungen zum Beschlagnahmeschutz in verschiedenen Ländern der EU Dierlamm/Ihwas BB 2017, 1097ff.

905 Eisele JR 2018, 85.

Maßgeblich ist also auch, wie wahrscheinlich es ist, dass im Drittausland vorliegende Information innerhalb der EU zur Reidentifizierung von Datensätzen verfügbar gemacht werden können.

Es kommt also darauf an, ob das zur Identifizierung erforderliche Zusatzwissen für die Verantwortlichen, also hier für Forschende in der EU, verfügbar gemacht werden kann. Ein hierfür relevanter Aspekt ist gemäß der Rechtsprechung des EuGHs, ob das **Zusatzwissen rechtmäßig beschafft** werden kann.[906] Dabei geht der EuGH davon aus, dass die unzulässige Beschaffung von Zusatzwissen unwahrscheinlich sei. Hiervon kann aber selbst im EU-Binnenmarkt nicht ausgegangen werden. Besteht bzgl. der Verhinderung der Beschaffung des Zusatzwissens ein Vollzugsdefizit, so muss ein Personenbezug angenommen werden, wenn eine illegale Datenbeschaffung vorstellbar ist.[907] Ist das Zusatzwissen nur in einem Drittstaat verfügbar und besteht auch dort ein Vollzugsdefizit im Bereich des Datenschutzes, so ist die Unzulässigkeit der Beschaffung ebenso wenig ein Hinderungsgrund für die Beschaffung und das Nutzen des Zusatzwissens. Dies gilt erst recht, wenn, wie etwa in den USA, kein wirksamer Rechtsschutz gegen Datenschutzverstöße gewährt wird.[908] So zeigte sich z.B., dass in den USA die Fa. Clearview – rechtlich bisher unbeanstandet – eine Datenbank zur automatisierten biometrischen Gesichtserkennung weltweit bereitgestellt hat, die mithilfe von Scraper-Software im Internet mehr als 3 Mrd. Fotos abgesaugt hat, mit denen global Gesichter Identitäten zugeordnet werden können.[909] Ist dagegen das Zusatzwissen im Drittstaat für den Verantwortlichen in der EU faktisch nicht zugänglich, so kann sich hieraus ergeben, dass ein konkreter Datensatz als anonym anzusehen ist.

906 EuGH 19.10.2016, C-582/14 (Breyer), Rn. 46, NJW 2016, 3579 = NVwZ 2017, 213 = EuZW 2016, 909 = BB 2016, 2830 = K&R 2016, 811.

907 Karg in SHS, Art. 4 Nr. 1 Rn. 64; Weichert in DWWS, Art. 4 Rn. 25; Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 28f.

908 In Bezug auf Gesundheitsdaten Solove/Schwartz, Privacy Law Fundamentals, 2011, 71ff.; generell EuGH 06.110.2015 – C-362/14 Rn. 84–98; EDPS, Stellungnahme 4/2016 zu EU-US-Datenschutzschild v. 30.05.2016, 11f.; Article 29 Data Protection Working Party, WP 255, EU-U.S. Privacy Shield – First annual Joint Review, v. 28.11.2017, 18; dies., WP 238, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, v. 13.04.2016, 25ff., 51f.; Schantz in SHS, Art. 45 Rn. 42f.; 69; Weichert, ZD 2016, 213f.; Weichert RDV 2012, 113ff.

909 Beuth/Horchert, Anonym? War gestern! Der Spiegel Nr. 5 v. 25.01.2020, 43; Hurtz, Eine Technologie und ihre Gefahren; Schmieder, Modus Tarnkappe, SZ 23.01.2020, 18; Brühl/Hurtz, Ich kann dich sehen, SZ 21.01.2020, 18.